Author:
Hall, Emily V

Title:
Almost elusive permutation groups

Almost elusive permutation groups

Emily Hall

School of Mathematics
University of Bristol

A dissertation submitted to the University of Bristol in accordance with the requirements of the degree of Doctor of Philosophy in the Faculty of Science.

July 2023

ABSTRACT

Let G be a transitive permutation group on a finite set Ω with $|\Omega| \geqslant 2$. An element of G is said to be a derangement if it has no fixed points on Ω. As an easy consequence of the orbit counting lemma, G always contains such an element. In fact, by a theorem of Fein, Kantor and Schacher, G contains a derangement of prime power order. However, there do exist groups with no derangements of prime order; we call such groups elusive. As a natural extension, we say that G is almost elusive if it contains a unique conjugacy class of prime order derangements. In this thesis, we classify the quasiprimitive almost elusive groups.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my supervisor, Tim Burness. Your expertise, guidance and continuous encouragement have been invaluable to me over the past four years. Thank you for your constant patience and meticulous attention to detail. I am truly fortunate to have had the opportunity to work with you.

I would also like to thank the Heilbronn Institute for Mathematical Research for providing the funding for this research to happen.

I'm extremely grateful to the mathematics PhD students who have contributed to making my experience in Bristol so enjoyable. In particular, thank you to Ayesha, Andrei, Alex and Harry for providing the perfect combination of support and distraction. Thank you for engaging in some very juvenile banter at times and for all the fun over the last few years. I would also like to thank Jenny. Thank you for singing with me (even though we guessed most of the lyrics) and making my summers so much fun. You really are my platonic life partner.

I would like to express my deepest gratitude to my family for their continual support and unhesitating belief in my abilities. Thank you to my parents Alison and Alan for always encouraging me to do what I love, and to my brothers Ben and Eddie for always being there to provide the comic relief. You all mean the world to me.

Finally, I would like to thank my wonderful husband Max. Your unwavering love, support and understanding throughout my entire PhD journey means more to me than words can express. Thank you for believing in me when I didn't believe in myself and for

being my biggest cheerleader. None of this would have been possible without you, and I am so grateful to have you as my partner in life.

AUTHOR'S DECLARATION

I declare that the work in this dissertation was carried out in accordance with the requirements of the University's Regulations and Code of Practice for Research Degree Programmes and that it has not been submitted for any other academic award. Except where indicated by specific reference in the text, the work is the candidate's own work. Work done in collaboration with, or with the assistance of, others, is indicated as such. Any views expressed in the dissertation are those of the author.

SIGNED: Emily Hall DATE: 2nd July 2023

CONTENTS

NOTATION

Let A and B be finite groups, let $g \in A$ and $h \in B$, and let n, a and b be positive integers. Throughout this thesis we write

$\delta_{a,b}$ for the Kronecker delta (i.e. $\delta_{a,b} = 1$ if $a = b$, and $\delta_{a,b} = 0$ otherwise)

(a, b) for the greatest common divisor of a and b

$(a)_b$ for the greatest power of b dividing a

$\pi(A)$ and $\pi(a)$ for the number of distinct prime divisors of $|A|$ and a, respectively

$\omega(A)$ and $\omega(a)$ for the total number of prime divisors of $|A|$ and a, respectively

$\alpha(A)$ and $\alpha(a)$ for the set of distinct prime divisors of $|A|$ and a, respectively

$\mathbb{F}_q$ for a field of size q

C_n (or simply n) for the cyclic group of order n

D_n for the dihedral group of order n

A_n and S_n for the alternating and symmetric groups of degree n, respectively

$[n]$ for an unspecified soluble group of order n

$A.B$ for an unspecified extension of A by B

$A{:}B$ for an unspecified split extension of A by B

$A \times B$ for the direct product of A and B

A^n for the direct product of n copies of A

$A \wr B$ for the wreath product of A and B, $B \leqslant S_n$

$A \circ B$ for the central product of A and B

$[g, h]$ for the commutator of g and h (i.e $[g, h] = g^{-1}h^{-1}gh$)

$[A, B]$ for the group $\langle \{[g, h] \mid g \in A,\, h \in B\} \rangle$

CHAPTER

1

INTRODUCTION

In 1872, Camille Jordan [50] proved that every nontrivial finite transitive permutation group contains a fixed-point-free element. We call these fixed-point-free elements *derangements*. This result of Jordan has some interesting applications in number theory and topology, as discussed by Serre in [74], and has led to various extensions. For example, the study of the proportion of derangements in finite transitive permutation groups is an area that has been studied extensively in recent years. Here one of the main highlights is the series of papers [[30], [31], [32], [33]] by Fulman and Guralnick, which show that the proportion of derangements in a transitive simple group is bounded below by an absolute constant (this result settles a conjecture of Boston and Shalev from the 1990s).

Another major focus of research in this area concerns the existence of derangements with prescribed properties, which is one of the main focal points of this thesis. For example, an influential result in this direction is established by Fein, Kantor and Schacher in [29]. Here they prove that every nontrivial finite transitive permutation group contains a derangement of prime power order. It is interesting to note that the proof of this result relies heavily on the Classification of Finite Simple Groups, which is in clear contrast to the elementary group theoretic concepts, such as the orbit counting lemma, required to prove the existence of derangements.

Although the existence of prime power order derangements is guaranteed, the existence

of prime order derangements is not. For example, the sporadic group M_{11} with its primitive action on 12 points (that is, its action on the right cosets of a maximal subgroup $\mathrm{L}_2(11)$) does not contain a derangement of prime order (it does however contain derangements of order 4 and 8). Following [18], we call a transitive permutation group *elusive* if it does not contain a derangement of prime order. These groups have been the subject of several papers in recent years (for example [18], [36], [37], [38], [39], [83]) and although a complete classification of the elusive groups remains out of reach, an important step in this direction was achieved by Giudici in [37]. His main theorem states that if G is an elusive group with a transitive minimal normal subgroup, then $G = \mathrm{M}_{11} \wr K$ with its product action on Δ^k, where $|\Delta| = 12$, $k \geqslant 1$ and $K \leqslant S_k$ is transitive.

In this thesis, we are also interested in the number of conjugacy classes of derangements. Take $G \leqslant \mathrm{Sym}(\Omega)$ to be a nontrivial finite transitive permutation group with point stabiliser H and notice that the set of derangements in G, denoted $\Delta(G)$, is a normal subset. Thus $\Delta(G)$ is a union of conjugacy classes. Therefore, it is very natural to consider the number of conjugacy classes of derangements. In [15], Burness and Tong-Viet show that a primitive permutation group G has a unique conjugacy 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 of G), or $(G, H) = (A_5, D_{10})$ or $(\mathrm{L}_2(8){:}3, D_{18}{:}3)$. This result was extended by Guralnick in [41], where he shows that the same conclusion holds for all transitive groups.

Motivated by the work of Burness, Tong-Viet and Guralnick, in this thesis we study the following natural extension of elusivity.

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 the natural action of the symmetric group S_n on n points is almost elusive (to see this, note that every derangement of prime order is a product of n/p disjoint p-cycles, which form a single conjugacy class). This shows that there are infinitely many almost simple primitive groups with this property, which is in stark contrast to the situation for elusive groups, where M_{11} on 12 points is the only example.

A finite permutation group is said to be *quasiprimitive* if every nontrivial normal subgroup is transitive. In [71], 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 result we prove the following theorem (see Section 2.2).

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

The goal of this thesis is to classify the almost elusive quasiprimitive groups.

Our first main result is Theorem 1 below, which classifies the primitive almost elusive groups. Here we use the notation $\mathcal{P}(n,i)$ to denote the i^{th} primitive group of degree n in the *Database of Primitive Groups* in Magma [5]. We direct the reader to Chapter 8 for the relevant tables and Section 8.1 for detailed remarks regarding the tables.

Theorem 1. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group with point stabiliser H. Then G is almost elusive if and only if one of the following holds:*

(i) *G is almost simple and (G,H) is contained in Table P1 or P2.*

(ii) *$G = V{:}H$ is a 2-transitive affine group such that $|V| = n = p^d$, where p is a prime, $d \geqslant 1$ and one of the following holds:*

  (a) *$H \leqslant \Gamma\mathrm{L}_1(p^d)$.*

  (b) *$\mathrm{SL}_2(q) \trianglelefteqslant H \leqslant \Gamma\mathrm{L}_2(q)$, where $p = 2$, d is even and $q = 2^{d/2}$.*

  (c) *$G = \mathcal{P}(n,i)$, where (n,i) is recorded in Table P3.*

Next we extend our analysis from the primitive to the quasiprimitive setting, which completes the classification of the almost elusive quasiprimitive groups. In view of the above theorem in order to do this, we determine the pairs (G,H) such that G is an almost simple group, H is a core-free non-maximal subgroup of G with $G = G_0H$ (where G_0 is the socle of G) and (G,H) is almost elusive, which is a convenient way to say that the natural action of G on the cosets of H is almost elusive. In fact, we can assume that $H < M$, where M is a core-free maximal subgroup of G and (G,M) is almost elusive (see Lemmas 2.1.28 and 2.1.30). In particular, we can assume that (G,M) is contained in Table P1 or P2.

Theorem 2. *Let G be an almost simple group with socle G_0 and let H be a core-free non-maximal subgroup of G such that $G = G_0H$. Then (G,H) is almost elusive only if one of the following holds:*

(i) $G_0 = \mathrm{U}_n(q)$ *and* H *stabilises a 1-dimensional non-degenerate subspace of the natural module, where* q *is even and* $n \geqslant 5$ *is a prime divisor of* $q+1$.

(ii) $G_0 = \mathrm{L}_2(p)$, $p \geqslant 5$ *is a prime and* (G, H) *is recorded in Table Q1.*

(iii) (G, H) *is recorded in Table Q2.*

Remark 1. Here we provide some remarks on Theorem 2.

(a) Suppose that (G, H) is as in Case (i) of Theorem 2 and write $H < M$, where M is the stabiliser of a 1-dimensional non-degenerate subspace of the natural module. Then (G, M) arises in Case 1 of Table P1, with the relevant conditions on n and q recorded in Remark 8.2(a). As discussed in Remark 4.2.43 we anticipate that no genuine almost elusive examples arise in this case (that is, we expect there are no examples satisfying all the number-theoretic constraints), which would allow us to remove case (i) in Theorem 2.

(b) For part (ii), if (G, H) is a case recorded in Table Q1, then (G, K) is almost elusive for any subgroup K of G isomorphic to H. See Proposition 4.3.8 for more details.

(c) Let (G, H) be any of the cases recorded in Table Q2. Then G has a subgroup K with $H \cong K$ such that (G, K) is almost elusive. In the table, we record the total number of G-classes of subgroups isomorphic to H such that $G = G_0H$, together with the number of these G-classes that give almost elusive examples. We note that all of these groups can easily be constructed with the aid of Magma [5]. Additionally, we note that in each case G_0 is isomorphic to a classical group, except in a couple of cases with $G_0 = A_9$. See Remark 8.3 for more information on Table Q2.

The majority of the work in this thesis goes in to proving Theorem 1, particularly for the classical groups. These groups are challenging for a variety of reasons. In particular, several difficult number-theoretic problems arise in the analysis.

Take $G \leqslant \mathrm{Sym}(\Omega)$ to be a primitive almost simple permutation group with point stabiliser H and socle G_0. In Theorem 2.2.1 we classify the pairs (G_0, H) such that $\pi(G_0) - \pi(H_0) \leqslant 1$, where G_0 is a simple group of Lie type, $H_0 = H \cap G_0$ and $\pi(X)$ denotes the number of distinct prime divisors of $|X|$. It is easy to see that G is almost elusive only if $\pi(G_0) - \pi(H_0) \leqslant 1$, so this result significantly reduces the number of cases we need to consider in the proof of Theorem 1. The cases in which G is a classical group and H is a subspace subgroup (those in the $\mathcal{C}_1$ Aschbacher collection, see Theorem 2.3.6) prove

to be the trickiest to deal with. In particular, the stabilisers of a non-degenerate 1-space require special attention. In fact it is precisely a subgroup of this type for $G_0 = \mathrm{U}_n(q)$ that leads to the special case recorded as Case 1 in Table P1 and part (i) of Theorem 2, for which we do not expect any almost elusive examples (see Proposition 4.2.42 and Remarks 4.2.43 and 4.3.3 for more details on this case).

Take $G \leqslant \mathrm{Sym}(\Omega)$ to be a quasiprimitive permutation group with point stabiliser H. Assume that G is almost simple with socle G_0, an alternating or sporadic group, such that G is not elusive (that is $(G, |\Omega|) \neq (\mathrm{M}_{11}, 12)$). Let r denote the largest prime divisor of $|\Omega|$. In [11, Corollary 1.2], Burness, Giudici and Wilson prove that if G is primitive then G contains a derangement of order r. By inspecting the cases that arise in Theorems 1 and 2, we can establish the following extension. As in Theorem 2, the case where $G_0 = \mathrm{U}_n(q)$ and H stabilises a 1-dimensional non-degenerate subspace of the natural module arises as a special case in Corollary 3.

Corollary 3. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a quasiprimitive almost elusive permutation group with socle G_0 and point stabiliser H. Assume G has derangements of prime order s. Then either s is the largest prime divisor of $|\Omega|$, or one of the following holds:*

(i) *G is primitive, $(s, r) = (2, 3)$ and $(G, H) = ({}^2F_4(2)', \mathrm{L}_2(25))$ or $({}^2F_4(2), \mathrm{L}_2(25).2_3)$.*

(ii) *G is imprimitive and one of the following holds:*

  (a) *$G_0 = \mathrm{U}_n(q)$ and H is properly contained in the stabiliser of a 1-dimensional non-degenerate subspace of the natural module, where q is even and $n \geqslant 5$ is a prime divisor of $q + 1$.*

  (b) *$s = 2$ and (G, H) is as in Case II or III of Table* Q1*.*

  (c) *$s = 3$ and $(G, H) = (\mathrm{L}_2(p), C_p{:}C_d)$ is as in Case IV of Table* Q1*, where $(p-1)/d$ is divisible by an odd prime.*

Let G be an almost simple group with socle G_0 and let H be a core-free subgroup of G such that $G = G_0H$ and (G, H) is almost elusive. We define the *depth of H*, denoted $d_G(H)$, to be the longest possible chain of subgroups

$$G > L_1 > \cdots > L_{\ell-1} > L_\ell = H, \tag{1.1}$$

such that (G, L_i) is almost elusive for all $1 \leqslant i \leqslant \ell$. Here we refer to ℓ as the length of the chain in (1.1). We define the *almost elusive depth* of G to be

$$D_G = \max d_G(H)$$

where we take the maximum over all core-free subgroups H of G such that $G = G_0H$ and (G, H) is almost elusive.

In the following corollary, we let $\omega(n)$ and $\pi(n)$ denote the total number of prime divisors and the number of distinct prime divisors of a positive integer n, respectively.

Corollary 4. *Let G be an almost simple group with socle G_0 and set $k = |G : G_0|$. If $D_G \geqslant 2$ then one of the following holds:*

(i) $G_0 = \mathrm{U}_n(q)$, *where q is even and $n \geqslant 5$ is a prime divisor of $q + 1$.*

(ii) $D_G = \omega(k(p-1)/2) - \pi(k(p-1)/2) + 1$ *and* $G_0 = \mathrm{L}_2(p)$, *where $p = 2^a - 1$ is a prime.*

(iii) $D_G = \omega((p-1)/2) - \pi((p-1)/2) + 1$ *and* $G = \mathrm{L}_2(p)$, *where $p = 2.3^a - 1$ is a prime with $a \geqslant 2$.*

(iv) $D_G = \omega(p+1) - \pi(p+1) + 1$ *and* $G = \mathrm{PGL}_2(p)$ *where $p = 2^a + 1$ is a prime.*

(v) $D_G = 2$ *and* $G = \mathrm{M}_{10}$, A_9, S_9, $\mathrm{L}_2(8).3$, $\mathrm{U}_5(2).2$ *or* $\mathrm{PSp}_6(2)$.

(vi) $D_G = 3$ *and* $G = \mathrm{L}_2(49).2_3$.

(vii) $D_G = 4$ *and* $G = \mathrm{U}_4(2)$, $\mathrm{U}_4(2).2$ *or* $\mathrm{U}_3(3).2$.

Remark 2. Here we provide some remarks on Corollary 4.

(a) In (i), we have $D_G \geqslant 1$ only if G is as in Case 1 of Table P1. That is, $G = G_0.[2f]$, where $q = 2^f$ and all the relevant number-theoretic conditions are satisfied. As highlighted above, we do not anticipate any genuine examples to arise in this case (see for example Remark 4.2.43).

(b) We do not know if D_G can be arbitrarily large, which seems to depend on some very difficult open problems in number theory. But we have checked computationally that if $G_0 = \mathrm{L}_2(p)$ and $p < 2^{1020}$ is a prime of the required form, then $D_G \leqslant 10$.

To conclude the introduction, let us briefly describe the layout of this thesis. In Chapter 2 we introduce some preliminary results and set up most of the notation we will use throughout the remainder of the thesis. We begin the proofs of Theorems 1 and 2 in Chapter 3, where we handle the almost simple groups with alternating and sporadic socle. We then move on to the classical groups in Chapter 4, before completing the proofs for the almost simple groups by handling the exceptional groups of Lie type in Chapter 5.

Finally in Chapter 6 we complete the proofs of Theorems 1 and 2 by handling the affine groups. In our penultimate chapter (Chapter 7) we prove Corollaries 3 and 4, and we briefly discuss some future research directions. Finally in Chapter 8, we present the main tables referenced throughout this thesis.

The content of this thesis is made up largely of the work within the author's papers [13], [44] and [45], the first of which is coauthored with Professor Tim Burness.

CHAPTER

2

PRELIMINARIES

In this chapter, we will introduce some of the background material that we require for the proofs of our main results.

2.1 Permutation groups

We begin by providing a brief introduction to permutation group theory. We refer the reader to the books by Cameron [17] and Dixon and Mortimer [26] for a thorough introduction to the subject.

2.1.1 Basic concepts

For a set Ω, the *symmetric group*, denoted as $\mathrm{Sym}(\Omega)$, is the group of all permutations of Ω.

Definition 2.1.1. Any subgroup S of $\mathrm{Sym}(\Omega)$ is called a *permutation group* on Ω.

We say that a permutation group S is finite if the order of S is finite and we refer to the cardinality of Ω as the degree of S.

Unless stated otherwise, for the remainder of this thesis when we write group we mean a finite group.

Let G be a group. An *action* of G on Ω is a homomorphism $\phi : G \to \mathrm{Sym}(\Omega)$, and we say that Ω is a *G-set*. For $x \in G$ and $\alpha \in \Omega$ we write α^x to denote the element $\phi(x)(\alpha) \in \Omega$. The image of ϕ, denoted G^Ω, is a permutation group, and we say that G is *faithful* if $\ker(\phi) = 1$. We note that if the action of G on Ω is faithful then $G \cong G^\Omega$. In fact, every group is isomorphic to a permutation group. For example, take $\Omega := G$ and define an action by right multiplication (i.e $\alpha^x = \alpha x$ with $\alpha \in \Omega$ and $x \in G$). This is faithful and so G is isomorphic to a permutation group. For $\alpha \in \Omega$ we use

$$\alpha^G = \{\alpha^x \mid x \in G\}$$

to denote the *orbit* of α and we use

$$\mathrm{Stab}_G(\alpha) = \{x \in G \mid \alpha^x = \alpha\}$$

to denote the *stabiliser* of α (we will often refer to this as a *point stabiliser* in G). We say that G is *transitive* if there is only one orbit, namely Ω, otherwise G is *intransitive*. In fact, the concept of transitivity can be generalised. Take k to be a positive integer. Then G is said to be *k-transitive* if for any two k-tuples $(a_1, \ldots, a_k)$ and $(b_1, \ldots, b_k)$, each with k distinct elements in Ω, there exists an $x \in G$ such that $a_i^x = b_i$ for all i. For example, the symmetric group S_n with its natural action on $\{1, \ldots, n\}$ is an n-transitive group.

Let G be a group acting transitively on a set Ω, and let H be a point stabiliser. By the Orbit-Stabiliser Theorem, there is a bijection between the G-set Ω and the set G/H of (right) cosets of H in G. Thus we can associate Ω with G/H. Moreover, the action of G on Ω is isomorphic to the natural action of G on G/H by right multiplication ($(Hx)^g = Hxg$). In addition, if K is also a point stabiliser in G, then H and K are conjugate and so the coset spaces G/H and G/K are isomorphic. Thus the transitive G-sets are (up to isomorphism) parameterised by the conjugacy classes of subgroups of G. The kernel of the action of G on the coset space G/H is

$$\mathrm{Core}_G(H) = \bigcap_{x \in G} x^{-1} H x,$$

this is called the *core* of H in G, and it is the largest normal subgroup of G contained in H. Thus given a group G, the faithful transitive G-sets (up to isomorphism) correspond to the conjugacy classes of core-free subgroups. In other words, the transitive permutation groups isomorphic to G are classified by the conjugacy classes of core-free subgroups.

Notation 2.1.2. Let G be a group and let H be a core-free subgroup. For a given property X of a permutation group, we say that the pair (G, H) has property X if G has property

X when viewed as a transitive permutation group on the set G/H. For example, (G, H) is almost elusive if G is almost elusive with respect to the natural action of G on G/H. We extend this terminology to elements as well. For example, we say that (G, H) contains a derangement if G contains a derangement with respect to the natural action of G on G/H.

A *block* is a nonempty subset Δ of Ω such that for any $x \in G$, either $\Delta^x = \Delta$ or $\Delta^x \cap \Delta = \emptyset$. Each translate Δ^x is also a block, and we say that the set $\{\Delta^x \mid x \in G\}$ is a *block system*. The sets Ω and the singletons $\{\alpha\}$ (for all $\alpha \in \Omega$) are blocks, and any other block is said to be nontrivial. For the remainder of Section 2.1.1 let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group and let H be a point stabiliser. We can now define primitive groups, which are a fundamental notion in permutation group theory.

Definition 2.1.3. We say that G is *primitive* (or G acts primitively on Ω) if Ω has no nontrivial blocks. Otherwise, we say that G is *imprimitive*.

A closely related notion to a block system is a G-invariant partition. We say a partition $\Omega = \Delta_1 \cup \cdots \cup \Delta_k$ is G-invariant if $(\Delta_i)^x \in \{\Delta_1, \ldots, \Delta_k\}$, for all i and all $x \in G$. In fact, it is easy to see that G has a nontrivial block system if and only if Ω admits a nontrivial G-invariant partition.

The primitive groups are often referred to as the basic building blocks of all permutation groups and primitivity can be seen as a natural 'irreducibility' condition. In particular, any imprimitive permutation group is isomorphic to a subgroup of an iterated wreath product of primitive groups (see [17, p. 12], for example). We will now state some basic properties of primitive groups (see [17, Theorem 1.7] for the proofs). We will often use the following lemma, which gives an equivalent definition of primitivity.

Lemma 2.1.4. *The group G is primitive if and only if every point stabiliser is a maximal subgroup of G.*

In particular, this tells us that for a given group K the faithful primitive K-sets (up to isomorphism) correspond to the conjugacy classes of core-free maximal subgroups of K.

Lemma 2.1.5. *Assume that G is 2-transitive. Then G is primitive.*

We note that the converse of Lemma 2.1.5 does not hold. For example, take $G = \langle (1, 2, 3, 4, 5) \rangle \cong C_5$ acting naturally on $\{1, \ldots, 5\}$. This is a primitive subgroup of S_5 but is not 2-transitive. The finite 2-transitive groups have been determined and a complete list of these groups can be found in [17, Tables 7.3 and 7.4], for example.

Lemma 2.1.6. *Assume G is primitive. Then every nontrivial normal subgroup is transitive.*

The latter observation motivates the following definition.

Definition 2.1.7. We say that G is *quasiprimitive* if every nontrivial normal subgroup of G is transitive.

Clearly every primitive group is quasiprimitive and so this is a weaker notion than primitivity. For example, take G to be a simple group and let H be non-maximal in G. Since G is transitive by assumption, and the only nontrivial normal subgroup of G is G itself, we conclude that G is quasiprimitive. Additionally, G is not primitive by Lemma 2.1.4. The quasiprimitive groups have applications in graph theory. For example, in the study of the automorphism groups of highly transitive graphs (see [71], for instance). Additionally, one of the most powerful tools for primitive groups (the O'Nan-Scott theorem) has an analogue in the quasiprimitive setting, which we will discuss in Section 2.1.3. This result describes the structure and actions of the *socle* of the group, which we can define for any finite group.

2.1.2 The socle

Let G be a group, and recall that a nontrivial normal subgroup J of G is *minimal* if it contains no nontrivial proper normal subgroup of G.

Definition 2.1.8. The *socle* of G, which we denote by $\mathrm{Soc}(G)$ or G_0, is the subgroup of G generated by its minimal normal subgroups.

We note that if $G \leqslant \mathrm{Sym}(\Omega)$ is a quasiprimitive group with socle G_0 and point stabiliser H. Then $G = G_0H$ since G_0 is transitive. The following results are all well known for primitive groups and are easy to extend to quasiprimitive groups. We refer the reader to [26, Theorems 4.3A and 4.3B] and [81, Section 2.6.1]. First recall that a group G acting on a set Ω is *regular* if G is transitive and $\mathrm{Stab}_G(\alpha) = 1$ for all $\alpha \in \Omega$. Additionally, the centraliser of a subset S of a group G is defined as $C_G(S) = \{g \in G \mid gs = sg \text{ for all } s \in S\}$.

Lemma 2.1.9. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a quasiprimitive permutation group and let J be a minimal normal subgroup of G. Then the following hold:*

(i) *The centraliser $C_G(J)$ is a normal subgroup of G.*

(ii) *If $C_G(J) \neq 1$, then J and $C_G(J)$ are both regular on Ω.*

Proof. (i) Take $c \in C_G(J)$, $g \in G$ and $s \in J$. Then

$$(gcg^{-1})s(gcg^{-1})^{-1} = gc(g^{-1}sg)c^{-1}g^{-1}$$

Since $J \trianglelefteqslant G$ we know that $g^{-1}sg \in J$. Thus

$$gc(g^{-1}sg)c^{-1}g^{-1} = gg^{-1}sgg^{-1} = s.$$

Therefore $gcg^{-1} \in C_G(J)$ and it follows that $C_G(J)$ is normal.

(ii) Assume that $C_G(J) \neq 1$ and note that since G is quasiprimitive, both J and $C_G(J)$ act transitively on Ω. Let $C := C_{\mathrm{Sym}(\Omega)}(C_{\mathrm{Sym}(\Omega)}(J))$ and note that $J \leqslant C$ and so C is also transitive on Ω. Take $\alpha, \beta \in \Omega$ and $g \in \mathrm{Stab}_{C_{\mathrm{Sym}(\Omega)}(J)}(\alpha)$. Since C is transitive, there exists an $h \in C$ such that $\beta = \alpha^h$, so

$$\beta^g = \alpha^{hg} = \alpha^{gh} = (\alpha^g)^h = \alpha^h = \beta.$$

Therefore $g = 1$, which implies that $\mathrm{Stab}_{C_{\mathrm{Sym}(\Omega)}(J)}(\alpha) = 1$. Since $\mathrm{Stab}_{C_G(J)}(\alpha) \leqslant \mathrm{Stab}_{C_{\mathrm{Sym}(\Omega)}(J)}(\alpha)$, it follows that $C_G(J)$ is regular. We can use similar arguments to show that J is also regular. □

Let $G = T_1 \times \cdots \times T_k$, be a direct product of groups T_i. For $1 \leqslant i \leqslant k$, let $\pi_i : G \to T_i$ be the natural projection map. In this thesis we say a subgroup $H \leqslant G$ is a *subdirect product* of G if $\pi_i|_H$ is an onto homomorphism for all i. If each $\pi_i|_H$ is injective, then we say H is a *diagonal subgroup*. Finally if H is both a subdirect product and a diagonal subgroup, then we say H is a *full diagonal subgroup*.

Lemma 2.1.10. *Let $G = T_1 \times \cdots \times T_k$, be a direct product of non-abelian simple groups. Let H be a subgroup of G and let $I := \{1, \ldots, k\}$.*

(i) *If H is a subdirect product of G, then H is a direct product $\prod D_j$, where D_j is a full diagonal subgroup of some subproduct $\prod_{i \in I_j} T_i$ such that I is partitioned by the I_j.*

(ii) *If H is a nontrivial normal subgroup of G, then $H = \prod_{l \in L} T_j$, where L is a nonempty subset of I.*

Proof. The first part of this lemma comes from [73, Lemma p. 328]. The second part can be found in [54, Proposition 5.2.5(i)]. □

The following two lemmas follow from [26, Theorem 4.3A]. Before we state the next lemma, recall that a subgroup H of a group G is *characteristic* if $H^\gamma = H$ for all $\gamma \in$

$\mathrm{Aut}(G)$. Additionally, a group G is *characteristically simple* if it has no proper nontrivial characteristic subgroups. Note that every characteristic subgroup is normal. We remind the reader that for groups A and B, $[A,B] = \langle\{[a,b] \mid a \in A, b \in B\}\rangle$, where $[a,b]$ is the commutator of a and b. The proof of part (ii) in the following lemma was taken from [8, Lemma 2.5].

Lemma 2.1.11. *Let G be a group with socle G_0.*

(i) *Any two distinct minimal normal subgroups commute. In particular, G_0 is a direct product of minimal normal subgroups.*

(ii) *Every minimal normal subgroup J of G is a direct product $J = T_1 \times \cdots \times T_k$, where the T_i are all isomorphic to a fixed simple group T.*

Proof. (i) Let J_1 and J_2 be distinct minimal normal subgroups of G. Then $[J_1, J_2] \leqslant J_1 \cap J_2 \trianglelefteq G$, so $[J_1, J_2] = J_1 \cap J_2 = 1$ by minimality. Since G is finite we can find a set of minimal normal subgroups of G, $\mathcal{J} = \{J_1, \ldots, J_k\}$, which is maximal with respect to the property that the subgroup H generated by $\mathcal{J}$ is a direct product $J_1 \times \cdots \times J_k$. Therefore, in order to show that $H = G_0$ we must show that H contains every minimal normal subgroup of G. Let K be a minimal normal subgroup of G. Then by minimality either $K \leqslant H$ or $K \cap H = 1$. In the latter case $\langle K, H\rangle = K \times H$, since both K and H are normal. However, this is impossible by our choice of $\mathcal{J}$. Thus H contains every minimal normal subgroup of G, so $H = G_0$.

(ii) Let J be a minimal normal subgroup of G. Since J is minimal, it contains no proper nontrivial normal subgroups. In particular, it contains no proper nontrivial characteristic subgroups of G. Thus J is characteristically simple. Let T be a minimal normal subgroup of J and let $\phi \in \mathrm{Aut}(J)$. Then T^ϕ is also a minimal normal subgroup of J. Thus (i) implies that either $T^\phi = T$, or $T^\phi \cap T = 1$ and $TT^\phi = T \times T^\phi$ is a direct product. In fact, the group $\langle T^\phi \mid \phi \in \mathrm{Aut}(J)\rangle$ is a nontrivial characteristic subgroup of J, so must be equal to J. By induction, J is the direct product of a finite number of T^ϕ. In particular, if $1 \neq N \trianglelefteq T$ then $N \trianglelefteq J$. Thus the minimality of T implies that $N = T$, whence T is simple. □

Lemma 2.1.12. *Let G be a group and let J be a minimal normal subgroup of G. Suppose that $J = T_1 \times \cdots \times T_k$, where each T_i is a non-abelian simple group. Then G acts transitively by conjugation on $\{T_1, \ldots, T_k\}$.*

Proof. Take $g \in G$. Since T_i is a normal subgroup of J it follows that $g^{-1}T_ig$ is a normal subgroup of $g^{-1}Jg = J$. Then by Lemma 2.1.10(ii) we have that $g^{-1}T_ig = \prod_{l\in L} T_l$ where L is some nonempty subset of $\{1,\dots,k\}$. However, $g^{-1}T_ig$ is simple and so $g^{-1}T_ig = T_l$ for some $l \in L$. Thus G acts by conjugation on $\{T_1,\dots,T_k\}$. Now suppose that G is not transitive on $\{T_1,\dots,T_k\}$. By relabeling if necessary, we may assume that $\{T_1,\dots,T_m\}$ is an orbit where $m < k$. Then by assumption, for all $g \in G$ and all $i \in \{1,\dots,m\}$ we have $g^{-1}T_ig \in \{T_1,\dots,T_m\}$. Let $M = T_1 \times \cdots \times T_m$. Then $M < J$ is a nontrivial normal subgroup of G, which is a contradiction. □

The following result reveals that the socle of a quasiprimitive group is very restricted. This is an extension of [26, Theorem 4.3B].

Theorem 2.1.13. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a quasiprimitive permutation group with socle G_0. Let J be a minimal normal subgroup of G. Then exactly one of the following holds:*

(i) *J is a regular elementary abelian group of order p^d, for some prime p and integer $d \geqslant 1$. In addition, $G_0 = J = C_G(J)$.*

(ii) *J is a regular non-abelian group, $C_G(J)$ is a minimal normal subgroup of G which is isomorphic to J, and $G_0 = J \times C_G(J)$.*

(iii) *J is non-abelian and $G_0 = J$.*

In particular, $G_0 = T_1 \times \cdots \times T_k$, where each T_i is isomorphic to a fixed simple group T.

Proof. We first prove that G has at most two distinct minimal normal subgroups. Suppose J_1 and J_2 are distinct minimal normal subgroups of G. Note that since G is quasiprimitive, both J_1 and J_2 act transitively on Ω. By Lemma 2.1.11(i) we have $J_1 \leqslant C_G(J_2)$, and by Lemma 2.1.9(ii), $C_G(J_2)$ is regular. Therefore, J_1 is also regular, which implies that $J_1 = C_G(J_2)$. Similarly $J_2 = C_G(J_1)$. Thus G has at most two minimal normal subgroups.

Suppose first that $C_G(J) = 1$, so J is non-abelian. By the previous argument, it follows that J is the unique minimal normal subgroup of G. Hence $G_0 = J$ and J is non-abelian, so (iii) holds.

For the remainder of the proof, we may assume that $C_G(J) \neq 1$. Now by Lemma 2.1.9, we see that $C_G(J)$ is a regular normal subgroup of G. Thus $C_G(J)$ is a minimal normal subgroup of G (if $C_G(J)$ contains a nontrivial subgroup K, which is normal in G, then K is regular and so $K = C_G(J)$). Since G has at most two distinct minimal normal subgroups, Lemma 2.1.11(i) implies that one of the following holds:

(a) $C_G(J) = J$ and $G_0 = J$; or

(b) $C_G(J) \cap J = 1$ and $G_0 = J \times C_G(J)$.

Suppose that (a) holds. Then it is clear that J is abelian and regular, hence J is elementary abelian by Lemma 2.1.11(ii).

Now assume that (b) holds. It is clear that J is regular by Lemma 2.1.9(ii) and it is non-abelian since $C_G(J) \cap J = 1$. Additionally, we note that $C_G(J)$ is regular by Lemma 2.1.9. Fix $\alpha \in \Omega$ and let L be the stabiliser of α in the group $JC_G(J)$. Then $L \cap J = L \cap C_G(J) = 1$ (since J and $C_G(J)$ are both regular). Therefore $LJ = LC_G(J) = JC_G(J)$ and

$$L \cong L/(L \cap J) \cong LJ/J \cong JC_G(J)/J \cong C_G(J).$$

Similarly, $L \cong J$. Therefore (ii) holds and the final assertion follows from Lemma 2.1.11(ii). □

2.1.3 The O'Nan-Scott theorem

We will now discuss one of the most important theorems in permutation group theory. The O'Nan-Scott theorem describes the structure and action of a finite primitive group in terms of the socle of the group. It roughly states that any finite primitive permutation group must belong to one of five infinite families. It is widely considered to be one of the most powerful tools in permutation group theory and it can often be used to reduce a general problem down to the almost simple case, at which point one can utilise the Classification of Finite Simple Groups, and the vast amount of information about simple groups, their maximal subgroups and conjugacy classes. It was stated independently by O'Nan and Scott at the Santa Cruz conference on Finite Groups in 1979 (only Scott's version made it into the final proceedings [73]) and shortly afterwards Aschbacher corrected an error in the statement. A sketch proof of the result can be found in [17, Section 4.5] and a detailed, self-contained proof is given by Liebeck, Praeger and Saxl in [59]. In 1993, Praeger established an analogue of the O'Nan-Scott theorem [71] for quasiprimitive groups.

Theorem 2.1.14 (Praeger)**.** *Let G be a quasiprimitive permutation group. Then G is isomorphic to one of the groups of type I, II or III described below.*

We will now describe the groups arising in Theorem 2.1.14. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a quasiprimitive group with socle G_0. By Theorem 2.1.13 we have $G_0 = T^k$, where $k \geqslant 1$ and T is a simple group.

Type I - Affine groups

Here $T = C_p$ for some prime p and $G_0 = (C_p)^k$ is an elementary abelian p-group. We can associate G_0 with $V = (\mathbb{F}_p)^k$, a k-dimensional vector space over $\mathbb{F}_p$, so we often write V for the socle of G in this case. We now describe the structure of an affine group.

First recall that an *affine transformation* of V is a map $t_{h,v} : V \longrightarrow V$ with $h \in \mathrm{GL}(V)$ and $v \in V$ such that $t_{h,v}(u) := hu+v$. These affine transformations form the *affine general linear group*, which is denoted $\mathrm{AGL}(V)$ or $\mathrm{AGL}_k(p)$, which we can view as a permutation group on V. The socle of $\mathrm{AGL}(V)$ may be identified with the additive group on V and we say G is an *affine group* of V if

$$V \trianglelefteqslant G = V{:}H \leqslant \mathrm{AGL}(V),$$

where $H \leqslant \mathrm{GL}(V)$ is the stabiliser of the zero vector in V. Here G is quasiprimitive if and only if H is irreducible on V, so every quasiprimitive affine group is primitive.

Type II - Almost simple groups

Here $k = 1$ and T is a non-abelian simple group. In particular $G_0 = T$ is the unique minimal normal subgroup of G and we have

$$G_0 \trianglelefteqslant G \leqslant \mathrm{Aut}(G_0).$$

Take H to be a point stabiliser in G. Then H is a core-free subgroup such that $G = G_0H$. In particular, H does not contain G_0. See Section 2.3 for more details on these groups.

Type III

Here $k \geqslant 2$ and T is non-abelian. These groups can be subdivided into three families; simple diagonal type, product type and twisted wreath type. Below we provide an example of one of the product type cases that arises, which is a "blow-up" of an almost simple group (this is labeled as III(b)(i) in [71, Section 2]).

Example 2.1.15. Let $M \leqslant \mathrm{Sym}(\Gamma)$ be a quasiprimitive almost simple group with socle T. Let $k \geqslant 2$ be an integer and consider the wreath product $W = M \wr S_k$. This has a natural product action on the Cartesian product $\Delta = \Gamma^k$, given by

$$(\gamma_1, \ldots, \gamma_k)^{(m_1,\ldots,m_k)\pi^{-1}} = (\gamma_{1^\pi}^{m_{1\pi}}, \ldots, \gamma_{k^\pi}^{m_{k\pi}}).$$

Here the socle of W is T^k and W acts transitively on the k factors. In this case, we say that a quasiprimitive group $G \leqslant \mathrm{Sym}(\Omega)$ is a product type group if $T^k \trianglelefteq G \leqslant W$, G acts transitively on the k factors of T^k and the following conditions hold:

(a) 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 $\mathrm{Stab}_{\mathrm{Soc}(W)}(\delta) = (\mathrm{Stab}_T(\gamma))^k$, and $\mathrm{Stab}_{\mathrm{Soc}(W)}(\alpha)$ is a subdirect product of S^k for some nontrivial normal subgroup S of $\mathrm{Stab}_T(\gamma)$.

In this thesis, we will not need detailed information on the groups of type III (see [71, Section 2] for more details).

2.1.4 Derangements

To conclude this part of the preliminary section, we present some useful results regarding derangements. We recall that unless stated otherwise, throughout this thesis when we write group we mean a finite group. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group with $|\Omega| \geqslant 2$ and point stabiliser H. For an element $x \in G$, we use $\mathrm{Fix}_\Omega(x)$ to denote the number of fixed points of x. That is,

$$\mathrm{Fix}_\Omega(x) = |\{\alpha \in \Omega \mid \alpha^x = \alpha\}|.$$

We begin by recalling the definition of a derangement.

Definition 2.1.16. An element $x \in G$ is a *derangement* if $\mathrm{Fix}_\Omega(x) = 0$. That is, x fixes no points of Ω.

Note that this definition easily extends to both intransitive and infinite groups. We use $\Delta(G)$ to denote the set of derangements in G and note that $\Delta(G)$ is a normal subset of G, so is a union of conjugacy classes.

We now present an equivalent definition for derangements that will be useful throughout the remainder of this thesis.

Lemma 2.1.17. *An element $x \in G$ is a derangement if and only if $x^G \cap H = \emptyset$, where x^G denotes the conjugacy class of x in G.*

Proof. Let $x \in G$ and define $\Lambda = \{(y, \alpha) \in x^G \times \Omega \mid \alpha^y = \alpha\}$. Take $z \in x^G$. Then it is easy to see that there are $\mathrm{Fix}_\Omega(z)$ many elements in Λ of the form (z, α), where $\alpha \in \Omega$. Thus, $|\Lambda| = \sum_{z \in x^G} \mathrm{Fix}_\Omega(z)$. In fact, since $\mathrm{Fix}_\Omega(z) = \mathrm{Fix}_\Omega(x)$ for all $z \in x^G$, we have

$$|\Lambda| = \mathrm{Fix}_\Omega(x)|x^G|.$$

Now for a given $\alpha \in \Omega$ there are precisely $|x^G \cap H|$ many elements in x^G that fix α, so

$$|\Lambda| = |x^G \cap H|\frac{|G|}{|H|},$$

which implies that

$$\mathrm{Fix}_\Omega(x) = \frac{|x^G \cap H||G|}{|x^G||H|}.$$

The result follows. □

The following result is a theorem of Jordan from 1872, [50]. The proof given here differs from Jordan's original proof, and was taken from [9, p. 3].

Theorem 2.1.18 (Jordan's theorem)**.** *There always exists a derangement in G.*

Proof. By the Orbit-Counting Lemma,

$$|G| = \sum_{x \in G} \mathrm{Fix}_\Omega(x).$$

Since $\mathrm{Fix}_\Omega(1) = |\Omega| \geqslant 2$, there must be an element $x \in G$ such that $\mathrm{Fix}_\Omega(x) = 0$. Thus G contains a derangement. □

We note that Jordan's theorem does not extend to intransitive groups, or to transitive infinite groups.

Example 2.1.19.

(a) Let $n \geqslant 3$ and take the subgroup $K = \langle (1, 2) \rangle \leqslant S_n$ acting naturally on $\{1, \ldots, n\}$. Then K is clearly an intransitive group that does not contain any derangements.

(b) Take $K = \mathrm{FSym}(\Omega)$ to be the *finitary symmetric group* on an infinite set Ω. This is the group of permutations of Ω that move only finitely many elements. This group is infinite and transitive, and clearly does not contain any derangements.

In view of Jordan's theorem there are many natural questions to ask. One such question is: Can we find derangements with special properties, such as prescribed order? A noteworthy outcome in this particular direction is the subsequent theorem established by Fein, Kantor, and Schacher [29], which pertains to the existence of prime power order derangements.

Theorem 2.1.20 (Fein, Kantor and Schacher)**.** *There always exists derangements of prime power order in G.*

A brief sketch of the basic strategy of the proof, in particular the reduction to the simple primitive cases, is given in [9, p. 9]. It is interesting to note that this theorem was originally motivated by a difficult number-theoretic problem related to Brauer groups, and that the only known proof of this result requires the Classification of Finite Simple Groups.

While the existence of prime power order derangements in G is guaranteed, the existence of prime order derangements is not. As stated in the introduction, we say a group is *elusive* if it contains no derangements of prime order. A major result towards the classification of the transitive elusive groups is the following result of Giudici [37].

Theorem 2.1.21 (Giudici)**.** *Let G be an elusive permutation group on a finite set Ω which has at least one transitive minimal normal subgroup. Then $G = \mathrm{M}_{11} \wr K$ acting with its product action on $\Omega = \Delta^k$ for some $k \geqslant 1$, where K is a transitive subgroup of S_k and $|\Delta| = 12$.*

A local notion of elusivity was introduced in [11]. Let r be a prime divisor of $|\Omega|$. Then G is said to be *r-elusive* if it does not contain a derangement of order r. The problem of classifying the r-elusive primitive permutation groups was reduced down to the almost simple cases in [11, Theorem 2.1]. The groups with an alternating or sporadic socle were handled in [11] and groups with a classical socle were later handled in [9] and [10]. The exceptional groups of Lie type are still to be handled.

We now turn our attention to the number of conjugacy classes of derangements in G, which we denote by $\mathcal{K}(G)$ (recall that $\Delta(G)$ is a union of conjugacy classes). Jordan's theorem implies that $\mathcal{K}(G) \geqslant 1$, and so it is natural to wonder if we can classify the groups with $\mathcal{K}(G) = 1$.

Theorem 2.1.22. *There is a unique conjugacy class of derangements in G, that is $\mathcal{K}(G) = 1$, if and only if G is sharply 2-transitive or $(G, H) = (A_5, D_{10})$ or $(\mathrm{L}_2(8){:}3, D_{18}{:}3)$.*

In particular, the proof of Theorem 2.1.22 for the primitive groups was handled by Burness and Tong-Viet in [15], and the remaining transitive groups were handled by Guralnick in [41].

As stated in the introduction, this thesis centers around the following concept, which is motivated by the work of Burness, Tong-Viet and Guralnick.

Definition 2.1.23. We say G is *almost elusive* if it contains a unique conjugacy class of derangements of prime order.

The goal of this thesis is to understand the quasiprimitive almost elusive groups. We end this section with some useful observations about derangements and almost elusive groups. We first record the following elementary observation, which is an application of [16, Lemma 2.2]. Recall that $G \leqslant \mathrm{Sym}(\Omega)$ is a transitive permutation group with $|\Omega| \geqslant 2$ and point stabiliser H. Let G_0 be the socle of G and let $H_0 = H \cap G_0$.

Lemma 2.1.24. *Let G be quasiprimitive and let r be a prime divisor of $|\Omega|$. Let a_r denote the number of G_0-classes of elements of order r in G_0, and let b_r denote the number of G_0-classes of elements of order r in H_0. Assume $a_r > b_r$. Then G contains a derangement of order r.*

Proof. Since $a_r > b_r$, there exists an element $y \in G_0$ of order r such that $y^{G_0} \cap H_0 = \emptyset$. Seeking a contradiction, suppose that there are no derangements of order r in G. Then, $y^G \cap H \neq \emptyset$, say $y^g \in H$ for some $g \in G$. Since G is quasiprimitive we have $G = G_0H$, so we may write $g = uh$ where $u \in G_0$ and $h \in H$. Thus $(y^u)^h \in H$, which implies that $y^u \in H^{h^{-1}} = H$. However $y^u \in G_0$, contradicting the fact that $y^{G_0} \cap H_0 = \emptyset$. Thus y is a derangement of order r in G. □

The following is a simple application of Cauchy's Theorem. Recall that $\alpha(X)$ is the set of distinct prime divisors of $|X|$ and $\pi(X) = |\alpha(X)|$.

Lemma 2.1.25. *Let G be quasiprimitive. Suppose there exists a prime $r \in \alpha(G_0) \setminus \alpha(H_0)$. Then every nontrivial element in G_0 of order r is a derangement.*

Corollary 2.1.26. *Let G be quasiprimitive. Then G is almost elusive only if $\pi(G_0) - \pi(H_0) \leqslant 1$.*

This elementary observation allows us to reduce the problem of classifying the almost elusive quasiprimitive groups to a much smaller number of cases. In Section 2.5 we determine the pairs (G_0, H) such that $\pi(G_0) - \pi(H_0) \leqslant 1$ when G_0 is a simple group of Lie type (see Section 2.5 for more details) and H is maximal in G.

To conclude this section we provide some basic observations which will be useful for handling the proof of Theorem 2. For the remainder of this section let G be an almost simple group with socle G_0 and let H be a core-free non-maximal subgroup of G such that $G = G_0H$. Additionally, let M be a maximal subgroup of G such that $H < M$.

Lemma 2.1.27. *Suppose (G, M) is almost elusive with $\pi(G_0) = \pi(M_0) + 1$. Then (G, H) is almost elusive only if $\pi(M_0) = \pi(H_0)$.*

Proof. Assume that G is almost elusive. By Lemma 2.1.25, if r is a prime dividing $|G_0|$, but not $|H_0|$, then every element in G_0 of order r is a derangement. Thus $\pi(G_0) - \pi(H_0) \leqslant 1$, and the result follows since $\pi(M_0) \geqslant \pi(H_0)$. □

Lemma 2.1.28. *Every maximal overgroup of H in G is core-free. In particular, M is core-free.*

Proof. Suppose that M is not core-free. Then $G_0 \leqslant M$ since G_0 is the unique minimal normal subgroup of G. It follows that $G_0 H \leqslant M$. However $G = G_0 H$. This is a contradiction since $M < G$. □

Lemma 2.1.29. *Suppose that (G, H) is not almost elusive and let L be a core-free subgroup of H. Then (G, L) is not almost elusive.*

Proof. Suppose that (G, H) is not almost elusive. Since H is non-maximal, (G, H) is not elusive and so there must exist distinct conjugacy classes x^G and y^G of elements of prime order in G such that $x^G \cap H = \emptyset$ and $y^G \cap H = \emptyset$. Since $L < H$, there are at least two conjugacy classes of derangements of elements of prime order. Thus (G, L) is not almost elusive. □

Lemma 2.1.30. *Suppose that (G, H) is almost elusive. Then (G, M) is almost elusive.*

Proof. First note that M is core-free by Lemma 2.1.28. Suppose (G, M) is neither almost elusive nor elusive. Then there exist distinct conjugacy classes x^G and y^G of elements of prime order in G such that $x^G \cap M = \emptyset$ and $y^G \cap M = \emptyset$. Since $H < M$, there are at least two distinct conjugacy classes of derangements of prime order in G, which is a contradiction. Thus either (G, M) is almost elusive, or (G, M) is elusive and thus $(G, M) = (\mathrm{M}_{11}, \mathrm{L}_2(11))$ by the main theorem of [37]. It is a simple calculation using the GAP Character Table Library [7] to show that there are no almost elusive cases if $(G, M) = (\mathrm{M}_{11}, \mathrm{L}_2(11))$. Assume first that H is maximal in M. We begin by obtaining the character table of G using the `CharacterTable` command. Then we use `OrdersClassRepresentatives` to obtain a list of the orders of the conjugacy class representatives in G from the character table. The maximal subgroups of G (and their character tables) can be accessed using the `Maxes` function, from which we can easily

identify M. From here we use the `Maxes` function again, to obtain the maximal subgroups of M. For each maximal subgroup H we obtain the character table and then use `FusionConjugacyClasses` to return the fusion of H-classes in G. It is now a routine exercise to check that (G, H) has at least two conjugacy classes of prime order derangements. Thus by Lemma 2.1.29 the result follows. □

We note that by Theorem 1 if (G, M) is almost elusive then it is one of the cases in Table P1 or P2.

2.2 A reduction theorem

In this section we prove one of the key results used in the proof of Theorems 1 and 2. Here we use Praeger's version of the O'Nan-Scott theorem for quasiprimitive groups (Theorem 2.1.14) to show that every quasiprimitive almost elusive group is either affine or almost simple. Below we state and prove the theorem as stated in the introduction (see page 3). We note that this result is [13, Theorem 1].

Theorem 2.2.1. *Let G be a quasiprimitive almost elusive permutation group. Then either G is almost simple, or G is a 2-transitive affine group.*

Proof. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a quasiprimitive almost elusive group with point stabiliser H and socle N. By Theorem 2.1.13 we have $N = T_1 \times \cdots \times T_k$, where 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 [71, 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 Theorem 2.1.13). If $C_G(J) \neq 1$ then Lemma 2.1.9 implies that both J and $C_G(J)$ are regular on Ω and thus every nontrivial element in J is a derangement. However, Burnside's $p^a q^b$ Theorem implies that $|T|$ is divisible by at least three distinct primes, which in turn 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 the unique minimal normal subgroup of G. By Lemma 2.1.12, G acts transitively via

conjugation on $\{T_1, \ldots, T_k\}$. In particular, H acts transitively on the set $\{T_1, \ldots, T_k\}$. 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 $H \cap N$ is a subdirect product of N. So by Lemma 2.1.10, $H \cap N = D_1 \times \cdots \times D_l \cong T^l$, where each

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

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 [71, Theorem 1] and it follows that $G \leqslant L \wr S_k$ is a product-type group as in Example 2.1.15, 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, there exists $\alpha \in \Omega$ and $\gamma \in \Gamma$ such that

$$\mathrm{Stab}_N(\alpha) \leqslant (\mathrm{Stab}_T(\gamma))^k < T^k = N.$$

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 [37, Theorem 1.4] we see that $L = T = \mathrm{M}_{11}$ and $U = \mathrm{L}_2(11)$. Since U is simple, the description of the groups of type III(b)(i) in [71, Section 2] (see Example 2.1.15) implies that $\mathrm{Stab}_N(\alpha)$ is a subdirect product of U^k. If $\mathrm{Stab}_N(\alpha) = U^k$ then N is elusive. Since G is quasiprimitive, $G \leqslant \mathrm{M}_{11} \wr S_k$ and $\mathrm{Aut}(\mathrm{M}_{11}) = \mathrm{M}_{11}$ 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 $\mathrm{Stab}_N(\alpha) < U^k = U_1 \times \cdots \times U_k$ and write $\mathrm{Stab}_N(\alpha) = F_1 \times \cdots \times F_c$, 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 2.2.1. □

2.3 Almost simple groups

As seen in Theorem 2.2.1, the problem of classifying the almost elusive quasiprimitive permutation groups is reduced down to the almost simple and 2-transitive affine cases. The vast majority of the work in this thesis involves the almost simple groups, so we provide here a brief discussion on this important family of groups.

First recall that a finite group G is said to be *almost simple* if there exists a non-abelian finite simple group G_0 such that

$$G_0 \trianglelefteq G \leqslant \mathrm{Aut}(G_0),$$

in which case G_0 is the socle of G. In order to discuss the groups that arise here we first recall the Classification of Finite Simple Groups.

Theorem 2.3.1 (The Classification of Finite Simple Groups (CFSG), 1980)**.** *Let T be a finite simple group. Then T is isomorphic to one of the following:*

(i) *C_p for a prime p*

(ii) *A_n for an integer $n \geqslant 5$*

(iii) *A simple group of Lie type (classical or exceptional)*

(iv) *One of 26 sporadic simple groups.*

Here we are interested in the groups with socle G_0 as in cases (ii), (iii) or (iv). For a complete list of the simple sporadic groups (those in case (iv)) and their orders, see [17, Table 7.2] for example. In this thesis, we use the notation for sporadic groups from the Atlas [82](and we regard the Tits group, ${}^2F_4(2)'$, as an exceptional group of Lie type).

Let us set up the notation we use for the groups of Lie type (those in case (iii)). For the classical groups, we adopt the notation of Kleidman and Liebeck [54]. For instance we write

$$\mathrm{PSL}_n(q) = \mathrm{PSL}_n^+(q) = \mathrm{L}_n(q), \;\; \mathrm{PSU}_n(q) = \mathrm{PSL}_n^-(q) = \mathrm{U}_n(q),$$

for the linear and unitary groups. This notation extends naturally to $\mathrm{L}_n^\epsilon(q)$, $\mathrm{PGL}_n^\epsilon(q)$ and $\mathrm{GL}_n^\epsilon(q)$, where $\epsilon = \pm$. If G is a simple orthogonal group, then we write $G = \mathrm{P}\Omega_n^\epsilon(q)$, where $\epsilon = \circ$ if n is odd and $\epsilon = -$ (respectively $+$) if n is even and the underlying quadratic form has Witt defect 1 (respectively 0). When n is odd, we also often write $G = \Omega_n(q)$.

Notation 2.3.2. We say that a group G is a simple *classical group* over $\mathbb{F}_q$ if G is contained in the set $\mathcal{A} = \mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{A}_3 \cup \mathcal{A}_4$, where

$$\begin{aligned}
\mathcal{A}_1 &= \{\mathrm{L}_n(q) \mid n \geqslant 2,\ (n,q) \neq (2,2),(2,3),(2,4),(3,2)\},\\
\mathcal{A}_2 &= \{\mathrm{U}_n(q) \mid n \geqslant 3,\ (n,q) \neq (3,2)\},\\
\mathcal{A}_3 &= \{\mathrm{PSp}_n(q) \mid n \geqslant 4,\ (n,q) \neq (4,2),(4,3)\},\\
\mathcal{A}_4 &= \{\mathrm{P}\Omega^{\epsilon}_n(q) \mid n \geqslant 7\}
\end{aligned}$$

Similarly we say that G is a simple *exceptional group* of Lie type over $\mathbb{F}_q$ if it is contained in $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2 \cup \mathcal{B}_3 \cup \mathcal{B}_4 \cup \{{}^2F_4(2)'\}$, where

$$\begin{aligned}
\mathcal{B}_1 &= \{{}^2B_2(q), {}^2F_4(q) \mid q = 2^{2m+1},\ m \geqslant 1\},\\
\mathcal{B}_2 &= \{{}^2G_2(q) \mid q = 3^{2m+1},\ m \geqslant 1\},\\
\mathcal{B}_3 &= \{G_2(q) \mid q \geqslant 3\},\\
\mathcal{B}_4 &= \{{}^3D_4(q), F_4(q), E_6(q), {}^2E_6(q), E_7(q), E_8(q) \mid q \geqslant 2\}
\end{aligned}$$

The sets $\mathcal{A}$ and $\mathcal{B}$ are defined so that all the groups in $\mathcal{A} \cup \mathcal{B}$ are simple and pairwise non-isomorphic. In particular, the groups $\mathrm{L}_2(2)$, $\mathrm{L}_2(3)$, $\mathrm{U}_3(2)$ and ${}^2B_2(2)$ are not simple, and below we present a complete list of the relevant isomorphisms between simple groups (see [54, Proposition 2.9.1 and Theorem 5.1.1]):

$$\begin{gathered}
\mathrm{L}_2(4) \cong \mathrm{L}_2(5) \cong A_5,\ \mathrm{L}_2(7) \cong \mathrm{L}_3(2),\\
\mathrm{L}_2(9) \cong \mathrm{PSp}_4(2)' \cong A_6,\ \mathrm{L}_4(2) \cong A_8,\ \mathrm{U}_4(2) \cong \mathrm{PSp}_4(3),\\
G_2(2)' \cong \mathrm{U}_3(3),\ {}^2G_2(3)' \cong \mathrm{L}_2(8)
\end{gathered} \tag{2.1}$$

2.3.1 Automorphisms

In this section we briefly discuss the automorphisms of the non-abelian simple groups.

Let G be a non-abelian simple group. The *inner* automorphisms are the maps $\phi_g : x \mapsto g^{-1}xg$ for $g \in G$. These automorphisms form a normal subgroup of $\mathrm{Aut}(G)$, which we denote by $\mathrm{Inn}(G)$, and we note that $\mathrm{Inn}(G) \cong G/Z(G) \cong G$. We define the *outer automorphism group* of G to be $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$.

When G is an alternating group, that is $G = A_n$ with $n \geqslant 5$, we have that $\mathrm{Aut}(A_n) \cong S_n$ for all $n \neq 6$. In particular, $\mathrm{Out}(A_n) \cong C_2$ for $n \neq 6$, and $C_2 \times C_2$ for $n = 6$. In the case

$n = 6$, there exists an exceptional isomorphism which is an isomorphism $S_6 \to S_6$, which does not correspond to a permutation of the underlying set $\{1, \ldots, 6\}$ (see [81, Section 2.4.2] for more information). When G is a sporadic group, it is well known that $\mathrm{Out}(G)$ is either trivial or C_2 (see [54, Table 5.1.C] for example). For groups of Lie type, we follow Gorenstein, Lyons and Solomon [40] for their definitions of the outer automorphisms (i.e the diagonal, field, graph and graph-field automorphisms), see also [9, Chapter 2]. The following is a theorem of Steinberg [77, Theorem 30].

Theorem 2.3.3. *Let G be a simple group of Lie type. Then every automorphism of G is the product of an inner, a diagonal, a field and a graph automorphism of G.*

Detailed information on the non-inner automorphisms of the non-classical simple groups will not be needed in this thesis. But we will need to recall some basic facts on the non-inner automorphisms of the classical groups.

Let G_0 be a simple classical group over $\mathbb{F}_q$, where $q = p^f$ and p is a prime. We will often use $\mathrm{Inndiag}(G_0)$ to denote the group of *inner-diagonal automorphisms*, which is the subgroup of $\mathrm{Aut}(G_0)$ generated by the inner and diagonal automorphisms of G_0. For example, $\mathrm{Inndiag}(\mathrm{L}_n(q)) = \mathrm{PGL}_n(q)$. We remark that in order to prove the main theorems in this thesis (Theorems 1 and 2) in the classic group setting we typically seek derangements in $\mathrm{Inndiag}(G_0)$, and we then appeal to results describing the effect of non-inner automorphisms on the number of conjugacy classes of such elements (see Section 4.1). In order to introduce the relevant notation, we will briefly describe the outer automorphisms in the linear case, noting that similar descriptions can be found in [9, Sections 2.3, 2.4 and 2.5] for the unitary, symplectic and orthogonal groups, respectively.

Take $G_0 = \mathrm{L}_n(q)$ with $n \geqslant 2$. Let V be the natural module of $\mathrm{GL}_n(q)$ and let $\{v_1, \ldots, v_n\}$ be a basis of V. The elements of $\mathrm{PGL}_n(q) \setminus G_0$ are the nontrivial *diagonal automorphisms* of G_0. In particular $\mathrm{Inndiag}(G_0) = \mathrm{PGL}_n(q) = \langle G_0, \delta \rangle$, where $\delta = [\mu, I_{n-1}]Z \in \mathrm{PGL}_n(q)$, μ is a primitive element of $\mathbb{F}_q$ and Z is the centre of $\mathrm{GL}_n(q)$. Here $[\mu, I_{n-1}]$ is a diagonal matrix with entries μ and 1 (where 1 has multiplicity $n-1$). We note that $|\mathrm{PGL}_n(q) : \mathrm{L}_n(q)| = (n, q-1)$.

We can define a map, $\gamma : V \to V$, where

$$\gamma : \sum_i \lambda_i v_i \mapsto \sum_i \lambda_i^p v_i.$$

Then γ induces a field automorphism $\phi : \mathrm{GL}_n(q) \to \mathrm{GL}_n(q)$, where $(a_{ij})^\phi = (a_{ij}^p)$ for all $(a_{ij}) \in \mathrm{GL}_n(q)$. Note that ϕ normalises Z and so it induces an automorphism of

$\mathrm{PGL}_n(q)$. We will abuse notation by writing ϕ for the induced automorphism. The *projective semilinear group* is defined to be $\mathrm{P\Gamma L}_n(q) = \mathrm{PGL}_n(q){:}\langle\phi\rangle$ and we write the elements of $\mathrm{P\Gamma L}_n(q)$ as (x, ϕ^l) where $x \in \mathrm{PGL}_n(q)$ and $\phi^l \in \langle\phi\rangle$. We refer to the map ϕ as a *standard* field automorphism of order f. More generally, we say that any element in $\mathrm{P\Gamma L}_n(q)\backslash\mathrm{PGL}_n(q)$ is a field automorphism, so they have the form $x\phi^l$ (or (x, ϕ^l)) with $1 \leqslant l < f$ and $x \in \mathrm{PGL}_n(q)$.

The inverse-transpose automorphism of $\mathrm{GL}_n(q)$ is defined by the map $\iota : \mathrm{GL}_n(q) \to \mathrm{GL}_n(q)$ such that $\iota(A) = A^{-T}$. Note that if $g \in \mathrm{PGL}_n(q)$ such that $g = AZ$, then $g^\iota = A^\iota Z$ and so the map ι induces an automorphism of $\mathrm{PGL}_n(q)$. Again we abuse notation and use ι to denote the induced automorphism. The *graph automorphisms* of G_0 are the elements of the form $x\iota$ with $x \in \mathrm{PGL}_n(q)$. Additionally, the *graph-field automorphisms* of G_0 are the elements of the form $x\phi^l\iota$ with $x \in \mathrm{PGL}_n(q)$ and $1 \leqslant l < f$. Then $\mathrm{Aut}(G_0) = \langle \mathrm{P\Gamma L}_n(q), \iota\rangle$. If $n = 2$, then ι coincides with an inner automorphism, so we have

$$\mathrm{Out}(G_0) = C_{(n,q-1)}{:}(C_f \times C_a)$$

where $a = 2$ if $n \geqslant 3$ and $a = 1$ otherwise.

2.3.2 Maximal subgroups

The primitive almost simple groups are a key focus within this thesis. We recall that every point stabiliser of a primitive permutation group is a maximal subgroup. Therefore the study of the maximal subgroups of almost simple groups plays a significant role throughout the work in this thesis. In particular, the main results within this section provide a framework for the proof of Theorem 1. The study of the subgroup structure of almost simple groups has a long and rich history, stretching back to the pioneering work of Galois in [35]. In recent years there have been many significant advances in this area, and here we briefly summarise some of the main results.

We begin by discussing the maximal subgroups of alternating and sporadic groups, followed by the classical groups, and then finally the exceptional groups of Lie type.

The alternating and sporadic groups

The original form of the O'Nan-Scott theorem [73] was stated in terms of the maximal subgroups of symmetric and alternating groups. Here we provide a simplified version of the theorem in this form.

Theorem 2.3.4. *Let $G = A_n$ or S_n with $n \geqslant 5$, and let H be a core-free maximal subgroup of G. Then one of the following holds:*

(i) *H acts intransitively on $\{1, \ldots, n\}$: $H = (S_k \times S_{n-k}) \cap G$ for some $1 \leqslant k < \frac{n}{2}$.*

(ii) *H acts transitively but imprimitively on $\{1, \ldots, n\}$: $H = (S_a \wr S_b) \cap G$ for some $a, b \geqslant 2$ with $n = ab$.*

(iii) *H acts primitively on $\{1, \ldots, n\}$.*

It is an impossible task to present a complete list of the maximal subgroups of the alternating and symmetric groups. For example, one of the subfamilies in case (iii) is the case where H is an almost simple group acting on the cosets of a maximal subgroup of index n. Additionally, some of the subgroups arising in the theorem are not maximal. However in [58], Liebeck, Praeger and Saxl determined all exceptions to maximality.

Now let us turn our attention to the sporadic groups. The maximal subgroups of the sporadic groups, aside from the Monster group $\mathbb{M}$, have been determined up to conjugacy. In the case of the Monster group, many of the maximal subgroups are known and there is a restrictive list of other potential maximal subgroups in this case. Below we provide a theorem bringing together all the current knowledge on the maximal subgroups of the Monster.

Theorem 2.3.5. *Let $G = \mathbb{M}$ and let H be a representative of a conjugacy class of maximal subgroups of G. Then one of the following holds:*

(i) *H belongs to a known list of 44 subgroups; or*

(ii) *H is almost simple with socle $\mathrm{L}_2(8)$, $\mathrm{L}_2(13)$, $\mathrm{L}_2(16)$ or $\mathrm{U}_3(4)$.*

See [80] for a detailed discussion on the maximal subgroups of sporadic groups and we note that the representatives of the conjugacy classes of maximal subgroups can be found in [80, Section 4].

The Classical groups

Let G be an almost simple classical group over $\mathbb{F}_q$ with socle G_0, where $q = p^f$ with p a prime. Let V denote the natural module for G_0. The main theorem on the subgroup structure of finite classical groups is due to Aschbacher [1], and this is one of the most important results for handling the classical groups in this thesis. The collections $\mathcal{C}$, $\mathcal{N}$ and $\mathcal{S}$ will be defined below.

Theorem 2.3.6 (Aschbacher)**.** *Let G be an almost simple classical group with socle G_0 and let H be a core-free maximal subgroup of G. Then $H \in \mathcal{C} \cup \mathcal{N} \cup \mathcal{S}$.*

Here the collection $\mathcal{C}$ is the union of eight subcollections, denoted $\mathcal{C}_1, \ldots, \mathcal{C}_8$, whose members are often referred to as *geometric* subgroups: since they are defined in terms of the underlying geometry of the natural module V. For example, the $\mathcal{C}_2$ collection consists of the stabilisers of appropriate direct sum decompositions of V. We will adopt the precise definition of these collections and the associated geometries used by Kleidman and Liebeck in [54], which differs slightly from the original set up in [1]. A brief description of each of these collections is given in Table 2.1. For the purposes of this thesis we refer to the subgroups in the $\mathcal{C}_1$ collection as the *subspace* subgroups since they comprise of the stabilisers of subspaces, or pairs of subspaces, of V. Conversely, we refer to any subgroup not contained in $\mathcal{C}_1$ as a *non-subspace* subgroup.

Following [54], we will often refer to the *type* of a maximal subgroup H of G. For $H \in \mathcal{C}$, the type typically describes the approximate group-theoretic structure of H, indicating the generic structure stabilised by H. For example, if $G_0 = \mathrm{L}_n(q)$ and H is of type $\mathrm{GL}_a(q) \wr S_t$, then H is the stabiliser of a direct sum decomposition $V = V_1 \oplus \cdots \oplus V_t$, where each V_i is a-dimensional. There are some exceptions to this notation. For instance, we use P_i to denote the stabiliser of a totally singular i-space (see [54, Section 2.1] for a definition of this terminology), adopting the convention that all subspaces of V are totally singular if $G_0 = \mathrm{L}_n(q)$. Additionally, if $G_0 = \mathrm{L}_n(q)$ with $n \geqslant 3$, then we use $P_{i,n-i}$ to denote the stabiliser of a pair of subspaces U and W such that $U < W$ with $\dim U = i$ and $\dim W = n - i$.

The members of the $\mathcal{S}$ collection are often called the *non-geometric* subgroups, and consist of almost simple groups with socle S such that S has a covering group $\hat{S} < \mathrm{GL}(V)$, which acts absolutely irreducibly on V. The formal definition of the $\mathcal{S}$ collection includes several other conditions to ensure that $\mathcal{C} \cap \mathcal{S} = \emptyset$ (see [54, p.3]). The subgroups that arise in the $\mathcal{S}$ collection are not known in general (but they are known up to conjugacy for $n \leqslant 12$: see [6]). We note that if $H \in \mathcal{S}$, the *type* of H refers to the socle S of the almost simple group H.

Let H be a core-free maximal subgroup of G. Set $H_0 = H \cap G_0$ and assume that $H \notin \mathcal{S}$. If H_0 is a maximal subgroup of G_0, then $H_0 \in \mathcal{C}$. However, there are some cases where H_0 is non-maximal: this leads to a small additional subgroup collection when $G_0 = \mathrm{PSp}_4(2^f)$ or $\mathrm{P}\Omega_8^+(q)$, which arises due to the existence of exceptional automorphisms. Following [9],

Table 2.1: Aschbacher's subgroup collections

$\mathcal{C}_1$	Stabilisers of subspaces, or pairs of subspaces, of V
$\mathcal{C}_2$	Stabilisers of direct sum decompositions $V = \bigoplus_{i=1}^{t} V_i$, where $\dim V_i = a$
$\mathcal{C}_3$	Stabilisers of prime degree extension fields of $\mathbb{F}_q$
$\mathcal{C}_4$	Stabilisers of tensor product decompositions $V = V_1 \otimes V_2$
$\mathcal{C}_5$	Stabilisers of prime index subfields of $\mathbb{F}_q$
$\mathcal{C}_6$	Normalisers of symplectic-type r-groups, $r \neq p$
$\mathcal{C}_7$	Stabilisers of tensor product decompositions $V = \bigotimes_{i=1}^{t} V_i$, where $\dim V_i = a$
$\mathcal{C}_8$	Stabilisers of non-degenerate forms on V
$\mathcal{S}$	Almost simple absolutely irreducible subgroups

Table 2.2: The collection $\mathcal{N}$

G_0	Type of H	Conditions
$\mathrm{PSp}_4(q)$	$\mathrm{O}_2^{\epsilon}(q) \wr S_2$	$p = 2$
	$\mathrm{O}_2^{-}(q^2).2$	$p = 2$
	$[q^4].\mathrm{GL}_1(q)^2$	$p = 2$
$\mathrm{P}\Omega_8^{+}(q)$	$\mathrm{GL}_1^{\epsilon}(q) \times \mathrm{GL}_3^{\epsilon}(q)$	
	$\mathrm{O}_2^{-}(q^2) \times \mathrm{O}_2^{-}(q^2)$	
	$G_2(q)$	
	$[2^9].\mathrm{SL}_3(2)$	$q = p > 2$
	$[q^{11}].\mathrm{GL}_2(q)\mathrm{GL}_1(q)^2$	

we use $\mathcal{N}$ to denote this subgroup collection and we refer to the elements of $\mathcal{N}$ as *novelty* subgroups. Note the maximal subgroups in the case where $G_0 = \mathrm{P}\Omega_8^{+}(q)$ were determined up to conjugacy by Kleidman [53]. Additionally, we note that subgroups of type $P_{i,n-i}$ are only maximal when G contains a graph or a graph-field automorphism (that is, if $G \not\leqslant \mathrm{P\Gamma L}_n(q)$). These provide another example of novelty subgroups (since H_0 is non-maximal in G_0 in this case); however, following [54], we include these subgroups in the $\mathcal{C}_1$ collection. In a similar manner to the $\mathcal{C}$ collection, if $H \in \mathcal{N}$ then the *type* of H typically describes the approximate group-theoretic structure of H, indicating the generic structure stabilised by H. The members of $\mathcal{N}$ are outlined in Table 2.2.

Kleidman and Liebeck's book, [54], is the definitive reference for information on the

existence, maximality and structure of the geometric subgroups. In [54], they provide a complete description of the structure of the geometric subgroups for all n, and determine their maximality (up to conjugacy) for $n \geqslant 13$. Additionally, Bray, Holt and Roney-Dougal [6], have completely determined all the maximal subgroups (up to conjugacy) of the low-dimensional classical groups with $n \leqslant 12$ (this includes the subgroups in $\mathcal{S}$).

The Exceptional groups of Lie type

The structure and classification of the maximal subgroups, up to conjugacy, of many of the almost simple exceptional groups of Lie type are well documented. See below for a list of references.

- ${}^2G_2(q)$ - Kleidman [52] (see also [6, Table 8.43]).
- ${}^2B_2(q)$ - Suzuki [78] (see also [6, Table 8.16]).
- ${}^3D_4(q)$ - Kleidman [51] (see also [6, Table 8.51]).
- $G_2(q)$ with q odd - Kleidman [52] (see also [6, Tables 8.41 and 8.42]).
- $G_2(q)$ with q even - Cooperstein [20] (see also [6, Table 8.30]).
- ${}^2F_4(q)$ - Malle [66].
- $F_4(q)$, $E_6(q)$ and ${}^2E_6(q)$ - Craven [24].

For the remaining exceptional groups with $G_0 = E_7(q)$ or $E_8(q)$, we state Theorem 2.3.7. Here we write $G = (\bar{G}_\sigma)'$, where $\bar{G}$ is a simple algebraic group of adjoint type over $\bar{\mathbb{F}}_p$ and σ is an appropriate Steinberg endomorphism of $\bar{G}$. A version of this result also applies, with minor adjustments, for the cases $G_0 \in \{G_2(q), F_4(q), {}^2E_6(q), E_6(q)\}$. This is a simplified version of [62, Theorem 8].

Theorem 2.3.7. *Let G be an almost simple group with socle $G_0 = (\bar{G}_\sigma)' \in \{E_7(q), E_8(q)\}$. Let H be a core-free maximal subgroup of G and set $H_0 = H \cap G_0$. Then one of the following holds:*

(I) *H is a maximal parabolic subgroup.*

(II) *$H = N_G(\bar{H}_\sigma)$ and $\bar{H}$ is a σ-stable non-parabolic maximal rank subgroup of $\bar{G}$: the possibilities for H are determined in [61].*

(III) *$H = N_G(\bar{H}_\sigma)$, where $\bar{H}$ is a maximal closed σ-stable positive dimensional subgroup of $\bar{G}$ (neither parabolic nor maximal rank).*

(IV) *H is of the same type as G over a subfield of $\mathbb{F}_q$.*

(V) *H is an exotic local subgroup (determined in [19]).*

(VI) *$G_0 = E_8(q)$, $p \geqslant 7$ and $H_0 = (A_5 \times A_6).2^2$.*

(VII) *H is almost simple and is not of type* (II), (III) *or* (IV).

The conjugacy classes of maximal parabolic subgroups (type (I)) for $G_0 = E_7(q)$ and $E_8(q)$ are in bijective correspondence with the nodes of the corresponding Dynkin diagrams. In this thesis, we are interested in the prime divisors of the orders of these subgroups. To obtain the prime divisors of a maximal parabolic subgroup P, it is convenient to use the Levi decomposition $P = QL$, where Q is the unipotent radical of P and L is a Levi subgroup. From here we can easily read off the prime divisors of $|L|$ using the Dynkin diagram (note that Q is a p-group). For example, if $G_0 = E_7(q)$ and $P = P_5$, then each prime divisor of $|L|$ must divide $|\mathrm{SL}_5(q)||\mathrm{SL}_3(q)|$.

Following [61, Theorem 8], the subgroups of type (III) can be partitioned into three cases as shown below:

Proposition 2.3.8. *Let G and H be as in Theorem 2.3.7, with H of type* (III). *Then one of the following holds:*

(i) *$G_0 = E_7(q)$, $p \geqslant 3$ and $H_0 = (2^2 \times \mathrm{P}\Omega_8^+(q).2^2).S_3$ or ${}^3D_4(q).3$,*

(ii) *$G_0 = E_8(q)$, $p \geqslant 7$ and $H_0 = \mathrm{PGL}_2(q) \times S_5$,*

(iii) *$(G_0, \mathrm{Soc}(H_0))$ is one of the cases listed in [62, Table 3].*

Next we present a similar proposition for the subgroups of type (VII). Here we use $\mathrm{Lie}(p)$ to denote the set of finite simple groups of Lie type defined over fields of characteristic p. The possibilities for $S = \mathrm{Soc}(H)$ have been significantly refined in recent years. The following result is taken from [14, Theorem 7.3], which is a combination of the main results in recent work of Craven [22, 23].

Proposition 2.3.9. *Let G and H be as in Theorem 2.3.7, with H of type* (VII) *and* $\mathrm{Soc}(H) = S$. *Then one of the following holds:*

(i) *$S \notin \mathrm{Lie}(p)$ and the possibilities for S are described in [63, Tables 10.1-10.4]; or*

(ii) $S \in \mathrm{Lie}(p)$ *and one of the following holds:*

(a) $G_0 = E_8(q)$ *and either* $S = \mathrm{L}_2(q_0)$ *with* $q_0 \leqslant (2, q-1).1312$ *or*

$$S \in \{\mathrm{L}_3^\epsilon(3), \mathrm{L}_3^\epsilon(4), \mathrm{U}_3(8), \mathrm{PSp}_4(2)', \mathrm{U}_4(2), {}^2B_2(8)\};$$

(b) $G_0 = E_7(q)$ *and* $S = \mathrm{L}_2(q_0)$ *with* $q_0 \in \{7, 8, 25\}$.

The list of possibilities for S in part (i) of Proposition 2.3.9 has been refined further; see Craven [21] and Litterick [65]. However, the tables in [63] will be sufficient for our purposes.

2.4 Number theory

In this section we present several number-theoretic results that will be useful throughout the remainder of this thesis. The results in this section are based on work in [13] and [44, Section 2]. We begin by presenting some general results, before moving on to discuss prime factors of binomial coefficients, and finally we provide some results regarding primitive prime divisors. Throughout this section, n is a positive integer and $q = p^f$ is a prime power. Our first result is [16, Lemma 2.6].

Lemma 2.4.1. *Let r and s be primes and let v and w be positive integers. If $r^v + 1 = s^w$, then one of the following holds:*

(i) $(r, s, v, w) = (2, 3, 3, 2)$.

(ii) $(r, w) = (2, 1)$ *and* $s = 2^v + 1$ *is a Fermat prime.*

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

We recall that for positive integers a and b, the notation $(a)_b$ denotes the largest b-power dividing a. For example $(24)_2 = 2^3$ and $(24)_3 = 3$.

Lemma 2.4.2. *Let r be a prime divisor of $q - \epsilon$, where $\epsilon = \pm 1$. Then*

$$(q^n - \epsilon)_r = \begin{cases} (q-\epsilon)_r (n)_r & n \text{ odd, or } r \text{ odd and } \epsilon = +1 \\ (q^2-1)_2 (n)_2/2 & n \text{ even, } r = 2, \epsilon = +1 \\ (r, 2) & n \text{ even, } \epsilon = -1 \end{cases}$$

Proof. This is [9, Lemma A.4] □

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 [72].

Lemma 2.4.3. *If $n \geqslant 12$, then there are at least two primes in the interval $(n/2, n)$.*

Our final general result concerns the solutions to congruence equations. For a proof of this result, see [3, Proposition 3.3.4] for example.

Lemma 2.4.4. *Suppose $a, b, k, n, m \in \mathbb{Z}$ such that $k, m \neq 0$ and $(k, m) = d$. Then the following hold:*

(i) *$ka \equiv kb \pmod{m}$ if and only if $a \equiv b \pmod{\frac{m}{d}}$.*

(ii) *The linear congruence $kx \equiv n \pmod{m}$ has solutions if and only if d divides n. Moreover, if d divides n then there exist exactly d solutions modulo m.*

2.4.1 Binomial coefficients

In Chapter 3, we need results on the prime factors of $\binom{n}{k}$, where n, k are positive integers with $1 \leqslant k < \frac{n}{2}$.

Lemma 2.4.5. *Suppose $k < \frac{n}{2}$. If $\binom{n}{k}$ is divisible by a prime power p^a, then $p^a \leqslant n$.*

Proof. See [27, Lemma, p.1084]. □

Lemma 2.4.6. *Write $\binom{n}{k} = UV$, where $k < \frac{n}{2}$, $U = p_1^{a_1} \cdots p_l^{a_l}$, $V = q_1^{b_1} \cdots q_m^{b_m}$ 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 [28, Theorem, p.258]. □

Lemma 2.4.7. *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 computation, using the fact that $\binom{n}{k} > \binom{n}{k-1}$ for all $1 \leqslant k < \frac{n}{2}$. □

A classical theorem of Sylvester and Schur (see [28, p.258]) states that $\binom{n}{k}$ is divisible by a prime $r > k$. For $k \geqslant 4$, we can now establish the following extension.

Proposition 2.4.8. *For $4 \leqslant k < \frac{n}{2}$, either $\binom{n}{k}$ is divisible by distinct primes $r, s > k$, or $(n,k) = (12,5), (9,4)$.*

Proof. Write $\binom{n}{k} = UV$ as in the statement of Lemma 2.4.6. 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 Lemma 2.4.6 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 2.4.5 we have $V \leqslant n$ and thus $\binom{n}{k} = UV \leqslant V^2 \leqslant n^2$. But this is a contradiction since $\binom{n}{k} > n^2$ 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 $\binom{n}{k}$, then $q_1, q_2 \neq k$ and we are done. Finally, suppose k is a prime divisor of $\binom{n}{k}$. Set $q_1 = k$, so $V = k^{b_1} q_2^{b_2}$ and $q_2 > k$. By Lemma 2.4.5 we have $k^{b_1}, q_2^{b_2} \leqslant n$ and so $V \leqslant n^2$. Since $U \leqslant V$ we have $\binom{n}{k} \leqslant n^4$ and thus Lemma 2.4.7 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. □

2.4.2 Primitive prime divisors

For the remainder of Section 2.4 we focus on primitive prime divisors, which play a key role in the proofs of Theorems 1 and 2 for groups of Lie type.

Let $a \geqslant 2$ and $n \geqslant 1$ be integers. We say a prime divisor of $a^n - 1$ is a *primitive prime divisor* (of $a^n - 1$) if it does not divide $a^i - 1$ for all $1 \leqslant i < n$. We define

$$P_a^n = \{r \mid r \text{ is a primitive prime divisor of } a^n - 1\}.$$

The following result is a famous theorem of Zsigmondy [85] from the 1890s regarding the existence of primitive prime divisors.

Theorem 2.4.9. *The set P_a^n is nonempty unless either $(n,a) = (1,2), (6,2)$, or $n = 2$ and $a = p$ is a Mersenne prime.*

The following result has an elementary proof. Details of the first part can be found in [9, Lemma A.1], and the second is an easy consequence of Fermat's Little Theorem.

Lemma 2.4.10. *Assume that $r \in P_a^n$ is an odd prime and let m be a positive integer. Then r divides $a^m - 1$ if and only if n divides m. Additionally, $r \equiv 1 \pmod{n}$.*

In this thesis, we are mainly interested in finding the size of unique primitive prime divisors in the case where $a = q = p^f$ is a prime power. In particular, we want to know for which n, q and d do we have $P_q^n = \{dn + 1\}$. The remainder of this section is dedicated to discussing this difficult problem.

The following lemma provides a connection between primitive prime divisors of $p^{fn} - 1$ and $q^n - 1$. We state the lemma in a more general setting.

Lemma 2.4.11. *Let a, b and c be positive integers such that $b \geqslant 2$ and $a = b^c$. Let $n \geqslant 2$ be an integer with prime factorisation $n = s_1^{g_1} \dots s_t^{g_t}$, where the s_i are distinct primes and each g_i is a positive integer. Then $P_b^{cn} \subseteq P_a^n$, with equality if and only if one of the following holds:*

(i) $(n, b) = (6, 2)$ *and c is prime;*

(ii) $n = 2$, *c is prime and b is a Mersenne prime; or*

(iii) $c = s_1^{h_1} \dots s_t^{h_t}$ *with $h_i \geqslant 0$ for all i.*

Moreover, $|P_a^n| = 1$ only if (i), (ii), *or* (iii) *holds, or* $(n, c, b) = (3, 2, 2), (2, 3, 2)$.

Proof. Assume $r \in P_b^{cn}$. Then by definition, r divides $b^{cn} - 1$, but does not divide $b^i - 1$ for all $1 \leqslant i < cn$. Thus it is easy to see that $r \in P_a^n$, so it follows that $P_b^{cn} \subseteq P_a^n$. In order to prove the first part of the lemma, it remains to prove the equality condition. Equality is clear for $c = 1$, so for the remainder of the proof we may assume $c \geqslant 2$.

Write $c = mk$, where $m = s_1^{h_1} \dots s_t^{h_t}$ with all $h_i \geqslant 0$, and $k \geqslant 1$ with $(k, n) = 1$. From here we define three separate cases:

(a) $k > 1$, $(n, m, b) \neq (6, 1, 2)$, and $(n, m) \neq (2, 1)$ when b is a Mersenne prime.

(b) $k > 1$ and $(n, m, b) = (6, 1, 2)$, or $(n, m) = (2, 1)$ and b is a Mersenne prime.

(c) $k = 1$.

First consider case (a). Define $v = mn$ and take $r \in P_b^v$ (note that our assumptions on n, m and b imply that such an r always exists). Since $v < cn$, we have $r \notin P_b^{cn}$ by definition. However, v divides cn but not $cd = mkd$ for any $1 \leqslant d < n$, implying $r \in P_a^n$ by Lemma 2.4.10. Therefore $P_b^{cn} \neq P_a^n$.

Next let us turn to case (b). Here $c = k$ and we let $c = p_1^{x_1} \dots p_l^{x_l}$ be the prime factorisation of c where the p_i are distinct primes. Suppose first that c is composite and

take $r \in P_b^{p_1 n}$. Then by definition $r \notin P_b^{cn}$ since $p_1 n < cn$. However $p_1 n$ divides cn, but not cd for any $1 \leqslant d < n$ since $(c, n) = 1$. Therefore $r \in P_a^n$, and so $P_b^{cn} \neq P_a^n$. Finally suppose that c is prime. Take r to be a prime divisor of $a^n - 1 = b^{cn} - 1$ such that $r \notin P_b^{cn}$. Then $r \in P_b^j$ for some $1 \leqslant j < cn$. If $j = 1$, then r divides $b^c - 1 = a - 1$ and thus $r \notin P_a^n$. Now suppose that $j \geqslant 2$ and note that j divides cn by Lemma 2.4.10. Then since c is prime, either j divides cd for some $1 \leqslant d < n$ or $j = n$. However $P_b^n = \emptyset$ by Zsigmondy's theorem, implying that $j \neq n$. Therefore $r \notin P_a^n$ by Lemma 2.4.10, so $P_a^n \subseteq P_b^{cn}$ and hence $P_b^{cn} = P_a^n$.

Finally let us assume that $k = 1$, as in case (c). Here $c = m = s_1^{h_1} \dots s_t^{h_t}$. As in case (b), we take r to be a prime divisor of $a^n - 1 = b^{cn} - 1$ such that $r \notin P_b^{cn}$. Then $r \in P_b^j$ for some $1 \leqslant j < cn$ such that j divides cn. Thus $j = s_1^{w_1} \dots s_t^{w_t}$ where $w_i \leqslant g_i + h_i$ (note that since $j \neq cn$ we must have that $w_i < g_i + h_i$ for at least one value of i). Define $d = s_1^{z_1} \dots s_t^{z_t}$, where

$$z_i = \begin{cases} w_i - h_i & \text{if } w_i - h_i > 0 \\ 0 & \text{otherwise} \end{cases}.$$

Then d divides n since $z_i \leqslant g_i$ for all i, and in particular $d \neq n$ since $j \neq cn$. By construction, j divides cd, so $r \notin P_a^n$. Thus equality holds.

For the final assertion of the lemma it is easy to see that $|P_a^n| = 1$ only if $P_b^{cn} = P_a^n$ or $|P_b^{cn}| = 0$. The result follows. □

We now focus on the existence of unique primitive prime divisors of $q^n - 1$, where $q = p^f$ is a prime power. Assume that $P_q^n = \{r\}$. For $n \geqslant 2$, Lemma 2.4.11 tells us that P_q^n contains every primitive prime divisor of P_p^{fn}. So if $P_p^{fn} \neq \emptyset$, then Lemma 2.4.10 implies that $r \geqslant nf + 1$. We dedicate the remainder of this section to improving this bound on r for certain values of n. We first state some results from the number theory literature that will be useful in the proofs of our remaining results. The first is an old theorem of Nagell [70] from 1920.

Theorem 2.4.12. *Let $p \geqslant 3$ be a prime. The only integer solutions to the equation*

$$x^2 + x + 1 = 3y^p$$

are $(x, y) = (1, 1)$ and $(x, y) = (-2, 1)$.

Theorem 2.4.13. *Let x, y, a and b be integers such that $|x|, |y| > 1$, $a > 2$ and $b \geqslant 2$. Suppose (x, y, a, b) is a solution to*

$$\frac{x^a - 1}{x - 1} = y^b,$$

such that $(x, y, a, b) \neq (3, 11, 5, 2), (7, 20, 4, 2), (18, 7, 3, 3)$ *or* $(-19, 7, 3, 3)$. *Then the following hold:*

(i) $b \geqslant 3$ *is prime.*

(ii) *The least prime divisor* r *of* a *satisfies* $r \geqslant 5$.

(iii) $|x| \geqslant 10^4$ *and* x *has a prime divisor* $r \equiv 1 \pmod{b}$.

Proof. This is [4, Proposition 1]. □

Our final result from the literature is [84, Lemma 2.6].

Theorem 2.4.14. *Let* x, y *and* a *be integers such that* $x, y > 1$ *and* $a > 2$. *Suppose* (x, y, a) *is a solution to*

$$x^2 + 1 = 2.y^a.$$

Then $(x, y, a) = (239, 13, 4)$.

Lemma 2.4.15. *Let* $n = 2^a 3^b > 2$ *for some* $a \geqslant 0$ *and* $b \in \{0, 1\}$. *If* $P_q^n = \{r\}$ *then* $r = dnf + 1$ *and either* $d \geqslant 8$, *or one of the following holds;*

(i) $d = 1$ *and* $(n, q) = (3, 4), (4, 2), (4, 3), (4, 7), (6, 3), (6, 4), (6, 5), (6, 8), (6, 19)$ *or* $(12, 2)$.

(ii) $d = 2$ *and* $(n, q) = (3, 2), (4, 4), (6, 23)$ *or* $(8, 2)$.

(iii) $d = 3$ *and* $(n, q) = (4, 5)$ *or* $(4, 239)$.

(iv) $d = 4$ *and* $(n, q) = (3, 3)$.

(v) $d = 5$ *and* $(n, q) = (4, 9)$ *or* $(8, 3)$.

(vi) $d = 6$ *and* $(n, q) = (3, 7), (6, 9), (6, 11)$ *or* $(12, 3)$.

(vii) $d = 7$ *and* $(n, q) = (4, 41)$ *or* $(6, 7)$.

Proof. Suppose $P_q^n = \{r\}$. Note that by Theorem 2.4.9 the set P_p^{nf} is nonempty if and only if $(n, q) \neq (3, 4)$. Let us first assume that $(n, q) = (3, 4)$. Then it is a simple calculation to show that $P_4^3 = \{7 = nf + 1\}$. Now for the remainder of the proof we may assume that $(n, q) \neq (3, 4)$. Since $P_p^{nf} \subseteq P_q^n$, it follows that $r = dnf + 1$ for some $d \geqslant 1$ and so we may assume that $d \in \{1, \ldots, 7\}$. We split the analysis into three main cases, namely, $b = 0$, $(a, b) = (0, 1)$, and $b = 1$ with $a \geqslant 1$.

Case 1. $b = 0$.

Using Lemma 2.4.10 it is easy to see that a prime s is an element of P_q^n if and only if s is an odd prime divisor of $q^{n/2}+1$.

First let us assume that q is even. Then $q^{n/2}+1 = r^l$ for some $l \geqslant 1$. By Lemma 2.4.1 we must have $l = 1$ and r is a Fermat prime, that is $2^{nf/2}+1 = dnf+1$. It is straightforward to show that for $d \in \{3,\ldots,7\}$ there are no solutions. For $d = 2$, the only solutions are $(n,q) = (4,4),(8,2)$, while for $d = 1$ the only solution is $(n,q) = (4,2)$.

Now assume that q is odd, so $q^{n/2}+1 = 2r^l$ for some $l \geqslant 1$. Then Theorem 2.4.14 tells us that $(n,q) = (4,239)$ if $l \geqslant 3$ (note here that $(r,l) = (13,4)$). Therefore, we may now assume that $l = 1$ or $l = 2$, and thus

$$p^{\frac{1}{2}nf}+1 = 2(dnf+1) \text{ or } p^{\frac{1}{2}nf}+1 = 2(dnf+1)^2$$

for $d \in \{1,\ldots,7\}$. From here it is straightforward to show that $(n,q,d) = (4,3,1)$, $(4,5,3)$, $(4,7,1)$,$(4,9,5)$, $(4,41,7)$ and $(8,3,5)$ are the only solutions. The result follows for $b = 0$.

Case 2. $b = 1$ and $a = 0$.

Here $n = 3$ and r divides q^2+q+1. Recall that here we may assume $q \neq 4$. If $s \geqslant 5$ is a prime divisor of q^2+q+1, it is easy to check that s does not divide $q-1$, so s is a primitive prime divisor of q^3-1 and thus $r = s$. Since q^2+q+1 is indivisible by 9 and odd, it follows that either $q^2+q+1 = r^l$, or $q \equiv 1 \pmod 3$ and $q^2+q+1 = 3r^l$ for some positive integer l.

Suppose $q \equiv 1 \pmod 3$ and $q^2+q+1 = 3r^l$. By Theorem 2.4.12, if $l \geqslant 3$ then there are no integer solutions (q,r). Thus we may assume $l = 1$ or 2, so

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

It is straightforward to check that $(7,19)$ is the only possibility, with $q^2+q+1 = 3r$.

Finally suppose $q \not\equiv 1 \pmod 3$ and $q^2+q+1 = r^l$. If $l \geqslant 2$ then by applying Theorem 2.4.13 we deduce that there are no solutions, so we may assume $l = 1$. It is straightforward to check that $(q,r) = (2,7)$ and $(3,13)$ are the only possibilities with $q^2+q+1 = r$.

Case 3. $b = 1$ and $a \geqslant 1$.

As in Case 2, it is easy to show that if $s \geqslant 5$ is a prime divisor of $q^{2^a}-q^{2^{a-1}}+1$, then $s = r$. Since $q^{2^a}-q^{2^{a-1}}+1$ is odd and indivisible by 9 (in particular, indivisible by 3 when $a \geqslant 2$), it follows that either $q^{2^a}-q^{2^{a-1}}+1 = r^l$, or $a = 1$, $q \equiv 2 \pmod 3$ and $q^{2^a}-q^{2^{a-1}}+1 = 3r^l$ for some positive integer l.

Suppose $a = 1$, $q \equiv 2 \pmod 3$ and $q^2 - q + 1 = 3r^l$. By Theorem 2.4.12, if $l \geqslant 3$ then there are no integer solutions (q, r), so we may assume $l = 1$ or 2, hence

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

It is straightforward to check that $(q, r) = (5, 7), (8, 19), (11, 37), (23, 13)$ are the only solutions.

Finally suppose $q^{2^a} - q^{2^{a-1}} + 1 = r^l$. Setting $x = -q^{2^{a-1}}$ we get an integer solution to the equation $x^2 + x + 1 = r^l$. By applying Theorem 2.4.13, if $l \geqslant 2$ then the only solution is $(x, r, l) = (-19, 7, 3)$, that is $n = 6$, $q = 19$, $r = 7$ and $q^2 - q + 1 = r^3$. Therefore we may now assume that $l = 1$. From here it is straightforward to show that the only solutions are $(n, q) = (6, 3)$ with $r = nf + 1 = 7$, $(n, q) = (6, 4), (12, 2)$ with $r = nf + 1 = 13$, $(n, q) = (6, 9), (12, 3)$ with $r = 6nf + 1 = 73$, or $(n, q) = (6, 7)$ with $r = 7nf + 1 = 43$. □

Remark 2.4.16. Note that the case $n = 2$ is excluded in Lemma 2.4.15. It is not difficult to see that $r \in P_q^2$ if and only if r is an odd prime divisor of $q+1$. So if $P_q^2 = \{r\}$, then for some positive integers k and l, either q is even and $q+1 = r^l$, or q is odd and $q+1 = 2^k r^l$. The q even case can be handled using Lemma 2.4.1, showing that either $(q, r) = (8, 3)$ or $q + 1$ is a Fermat prime. However, the q odd case leads to a much harder Diophantine equation to solve. In this case, we are unable to obtain a full solution, although Lemma 2.4.11 does provide restrictions on q. In particular if $P_q^2 = \{r\}$ for q odd, then either $q = 9$ (in which case $r = 5$), or $f = 2^m$ for some $m \geqslant 0$, or p is a Mersenne prime and f is a prime.

Remark 2.4.17. As the prime decomposition of n becomes more complicated, it becomes increasingly more difficult to find the size of a unique primitive prime divisor of $q^n - 1$. In particular, the associated Diophantine equation becomes more challenging to identify and solve. Here we briefly discuss some of the issues that arise when $n = 2^a j$ with $a \geqslant 0$ and $j \geqslant 5$ an odd prime (note the case $j = 3$ was handled in Lemma 2.4.15).

If there exists a unique primitive prime divisor r of $q^n - 1$, then (n, q, r) must be a solution to

$$\begin{cases} \frac{q^{2^{a-1}j}+1}{q^{2^{a-1}}+1} = (j, q^{2^{a-1}} + 1)r^l & \text{if } a \geqslant 1 \\ \frac{q^n-1}{q-1} = (n, q-1)r^l & \text{if } a = 0 \end{cases}$$

for some positive integer l. These are both special cases of the general *Nagell-Ljunggren equation*, for which there currently does not exist a complete set of integer solutions. However, bounds on the potential solutions have been established (see [69] for example).

This means that for $n = 2^a j$ with $j \geqslant 5$ we are unable to provide an analogue of Lemma 2.4.15. Nevertheless, we can give some details in the cases where $a \in \{0, 1\}$ and $q = 2^f$ for some positive integer f (see Lemma 2.4.18).

Lemma 2.4.18. *Let $n \geqslant 5$ be an odd prime and let $q = 2^f$ for some positive integer f. Suppose $P_q^{tn} = \{r\}$, where $t = 1$ or 2. Then either $r \geqslant 4nf + 1$, or $t = 2$, $r = 2nf + 1$ and one of the following holds:*

(i) $(n, q) = (5, 2)$; *or*

(ii) n *divides* $q + 1$.

Moreover, if $P_q^{tn} = \{r\}$ then $f = t^a n^b$ for some integers $a, b \geqslant 0$.

Proof. Suppose first that $t = 1$, so $P_q^n = \{r\}$. Then in the usual manner, r is the unique primitive prime divisor of $2^{fn} - 1$ and so $r = dnf + 1$ for some $d \geqslant 1$. By Lemma 2.4.11 we know that $f = n^j$ for some $j \geqslant 0$. Thus it follows that d must be even since both r and n are odd primes, so we may assume $r = 2nf + 1$, that is $r = 2n^{j+1} + 1$.

Assume n divides $2^f - 1 = 2^{n^j} - 1$. Then by Lemma 2.4.10, since n is prime, n is a primitive prime divisor of $2^{n^t} - 1$ for some $1 \leqslant t \leqslant j$. This implies that $n \equiv 1 \pmod{n^t}$ by Lemma 2.4.10, which is an obvious contradiction. Thus for any prime divisor k of $2^f - 1$, we conclude that $(2^{fn} - 1)_k = (2^f - 1)_k$ (see Lemma 2.4.2).

Suppose s is a prime divisor of $(2^{fn} - 1)/(2^f - 1)$. By the above argument it follows that s divides $2^{fn} - 1 = 2^{n^{j+1}} - 1$, but does not divide $2^f - 1 = 2^{n^j} - 1$. Therefore using Lemma 2.4.10 once again, we see that s is a primitive prime divisor of $2^{fn} - 1$.

In particular we conclude that,

$$\frac{2^{fn} - 1}{2^f - 1} = (2nf + 1)^l \tag{2.2}$$

for some positive integer l. By applying Theorem 2.4.13 we see there are no solutions to (2.2) when $l \geqslant 2$. Additionally, it is straightforward to show that the same conclusion holds when $l = 1$.

Finally suppose $t = 2$, so $P_q^{2n} = \{r\}$. Once again we have $r = 2nfd + 1$ for some $d \geqslant 1$, so we may assume $d = 1$. Assume s is a prime divisor of $q^{2n} - 1$. Then since n is an odd prime, either s is a divisor of $q^2 - 1$, or s is a primitive prime divisor of $q^n - 1$ or $q^{2n} - 1$. Thus any prime divisor of $q^n + 1$ is either a primitive prime divisor of $q^{2n} - 1$, or is a divisor of $q + 1$. By Lemma 2.4.2 it follows that

$$\frac{q^n + 1}{q + 1} = (n, q + 1)(2nf + 1)^l \tag{2.3}$$

for some positive integer l.

Suppose that n does not divide $q+1$. Then $(n, q+1) = 1$ and by applying Theorem 2.4.13 we see there are no solutions to (2.3) with $l \geqslant 2$. And for $l = 1$ it is straightforward to show that $(n, q) = (5, 2)$ is the only solution (note here that $r = 11$).

The final part of the lemma is a straightforward application of Lemma 2.4.11. □

Our final result is a number-theoretic application of the earlier results on primitive prime divisors. In particular, this result will be useful in the proof of Theorem 2.5.1.

Lemma 2.4.19. *If $n \geqslant 7$, then either $(n, q) \in \{(10, 2), (9, 2), (8, 3), (8, 2), (7, 3), (7, 2)\}$, or there exist distinct prime divisors $r, s > n + 2$ of*

$$N := \prod_{i=1}^{m} (q^{2i} - 1); \tag{2.4}$$

where $m = \lceil \frac{n-2}{2} \rceil$.

Proof. If $P_q^i \neq \emptyset$, then we will use r_i to denote the largest primitive prime divisor of $q^i - 1$. Recall that $r_i = ik_i + 1$ for some $k_i \geqslant 1$ (see Lemma 2.4.10).

Assume first that $n \geqslant 25$ and let $A = \{j \mid n - 12 \leqslant j \leqslant n - 1 \text{ and } j \text{ is even}\}$. Take $B = \{r_i \mid i \in A\}$ and note that each $r_i \in B$ divides N. Suppose first that $k_i = 1$ for all $i \in A$. Then B is a set of six consecutive odd numbers all greater than 3, so at least two are not prime, which is a contradiction. Now suppose that $k_i \geqslant 2$ for exactly one $i \in A$. Then B contains at least three consecutive odd numbers all greater than 3, implying that not all elements of B are prime, which is again a contradiction. Thus $k_i \geqslant 2$ for at least two $i \in A$, that is $r_i \geqslant 2i + 1$. Therefore the lemma holds for $n \geqslant 25$, since $2i + 1 > n + 2$.

Now assume $11 \leqslant n \leqslant 24$ and $q \neq 2$. Note that $r_8 \geqslant 41 > n + 2$ by Lemma 2.4.15, so for this case it remains to find an additional prime divisor of N larger than $n + 2$. For $16 \leqslant n \leqslant 24$ we can take $r_{14} \geqslant 29$. By Lemma 2.4.15 we know $r_{12} > 25$, so for $n = 15, 14$ or 13 we take r_{12}. Finally, if $n = 11$ or 12, Lemma 2.4.15 implies that $r_4 \geqslant 17$ if $q \notin \{3, 5, 7, 239\}$, while it is straightforward to calculate that $r_{10} \geqslant 61$ if $q \in \{3, 5, 7, 239\}$. Thus the lemma holds in this case.

Next assume $7 \leqslant n \leqslant 10$ and $q \neq 2$. By Lemma 2.4.15, if $q \notin \{3, 5, 7, 19\}$ then $r_4, r_6 \geqslant 13 > n + 2$. The cases $q \in \{3, 5, 7, 19\}$ can easily be handled by direct calculation.

Finally suppose that $q = 2$ and $7 \leqslant n \leqslant 24$. Once again, the result can be checked by direct calculation. In particular, if $15 \leqslant n \leqslant 24$ then $r_7 = 127$ and $r_5 = 31$ (these divide $q^{14} - 1$ and $q^{10} - 1$, respectively). If $11 \leqslant n \leqslant 14$ then $r_8 = 17$ and $r_5 = 31$. For $n = 9$ or

10 the only prime divisor of N larger than $n+2$ is 17. Additionally if $n = 7$ or 8 there are no prime divisors of N larger than $n+2$. □

2.5 Prime divisor reduction

Let G be an almost simple group with socle G_0 and let H be a corefree subgroup of G. Recall that $H_0 = H \cap G_0$ and $\pi(X)$ denotes the number of distinct prime divisors of $|X|$. Additionally we remind the reader that throughout this thesis all groups are finite. By Corollary 2.1.26 the problem of classifying the almost elusive groups of this form can be reduced to the cases in which $\pi(G_0) - \pi(H_0) \leqslant 1$. The subgroups M of a simple group G_0 with $\pi(G_0) = \pi(M)$ are described by Liebeck, Praeger and Saxl in [60]. In this section, we establish an extension of this result by determining the pairs (G_0, H) such that $\pi(G_0) - \pi(H_0) \leqslant 1$, where G is an almost simple group of Lie type with socle G_0 and H is a maximal subgroup of G. We remind the reader that we write $\mathcal{A} \cup \mathcal{B}$ for the set of simple groups of Lie type over $\mathbb{F}_q$, where the sets $\mathcal{A}$ (classical) and $\mathcal{B}$ (exceptional) are defined in Notation 2.3.2. The following result is essentially a combination of [44, Theorem 2] and [45, Theorem 2.12].

Theorem 2.5.1. *Let G be an almost simple group with socle $G_0 \in \mathcal{A} \cup \mathcal{B}$, and let H be a core-free maximal subgroup of G. Then $\pi(G_0) \leqslant \pi(H_0) + 1$ if and only if one of the following holds:*

(i) $\pi(G_0) = \pi(H_0)$ *and either:*

  (a) $G_0 \in \mathcal{A}$ *and (G_0, H) is found in Table A1; or*

  (b) $G_0 \in \mathcal{B}$ *and* $(G_0, H_0) = (G_2(3), \mathrm{L}_2(13))$ *or* $({}^2F_4(2)', \mathrm{L}_2(25))$.

(ii) $\pi(G_0) = \pi(H_0) + 1$ *and one of the following holds:*

  (a) $G_0 \in \mathcal{A}$ *and either (G_0, H) is listed in Table A2, or (G_0, H, i) is one of the cases recorded in Table A3 and there exists a unique primitive prime divisor of $q^i - 1$.*

  (b) $G_0 \in \mathcal{B}$, *(G_0, H, i) is one of the cases recorded in Table B1 and there exists a unique primitive prime divisor of $q^i - 1$.*

Remark 2.5.2. Notice we have excluded the almost simple groups with socle a sporadic or alternating group in the statement of Theorem 2.5.1. This is primarily due to the fact that the result is not particularly useful in these cases, for a variety of reasons:

(a) For sporadic groups, our main almost elusive results will be obtained using computational methods, apart from the Monster and the Baby Monster. And in the latter cases, it is easy to see that $\pi(G_0) - \pi(H_0) > 1$ for all possible maximal subgroups H (see Theorem 3.3 for more details).

(b) The alternating and symmetric groups have been omitted due to number-theoretic difficulties. For example, take $G_0 = A_n$ and let H be a maximal subgroup of G_0 that acts intransitively on $\{1, \ldots, n\}$. That is $H_0 = (S_k \times S_{n-k}) \cap G_0$,where $1 \leqslant k < \frac{n}{2}$. Then $\pi(G_0) - \pi(H_0)$ is precisely the number of distinct primes in the interval $(n-k, n]$. However, finding the number of distinct primes in this interval is a very hard problem in number theory.

The proof of Theorem 2.5.1 proceeds by direct comparison of the orders $|G_0|$ and $|H_0|$. We will approach the proof by handling each family $\mathcal{A}$ and $\mathcal{B}$ in turn. In both cases, the calculations are similar in most instances, so we only provide details in a handful of cases to illustrate the main methods.

2.5.1 Classical groups

Here we prove Theorem 2.5.1 for the groups with $G_0 \in \mathcal{A}$.

Theorem 2.5.3. *Let G be an almost simple group with socle $G_0 \in \mathcal{A}$, and let H be a core-free maximal subgroup of G. Then $\pi(G_0) \leqslant \pi(H_0) + 1$ if and only if one of the following holds:*

(i) $\pi(G_0) = \pi(H_0)$ *and (G_0, H) is found in Table A1.*

(ii) $\pi(G_0) = \pi(H_0) + 1$ *and either (G_0, H) is listed in Table A2, or (G_0, H, i) is one of the cases recorded in Table A3 and there exists a unique primitive prime divisor of $q^i - 1$.*

Let G, G_0 and H be as in Theorem 2.5.3. Recall that $H \in \mathcal{C} \cup \mathcal{N} \cup \mathcal{S}$ by Aschbacher's subgroup structure theorem (see Theorem 2.3.6). We divide the proof of Theorem 2.5.3 into two parts. Firstly, we handle the groups with $H \in \mathcal{C} \cup \mathcal{N}$, in which case H is a geometric or novelty subgroup. And then we handle the cases in which H is a non-geometric subgroup in $\mathcal{S}$. In the latter case we adopt a different approach because a complete list of the subgroups contained in $\mathcal{S}$ is not available. For these subgroups we appeal to a theorem of Guralnick et al. [43], which describes the subgroups $M \in \mathrm{GL}_n(q)$

such that $|M|$ is divisible by a primitive prime divisor of $q^i - 1$ for $\frac{n}{2} < i \leqslant n$. This provides a way to identify prime divisors of $|G_0|$ that do not divide $|H_0|$. Additionally, for certain low dimensional groups, we use the results in Bray, Holt and Roney-Dougal [6].

Before we begin the proof of Theorem 2.5.3 we state the following result which will be useful for both geometric and non-geometric subgroups. This is an immediate consequence of Lemma 2.4.19.

Lemma 2.5.4. *Let G_0 be a simple classical group over $\mathbb{F}_q$. Let n be the dimension of the natural module of G_0 and assume $n \geqslant 7$. Then either $|G_0|$ is divisible by distinct primes $r, s > n+2$, or $(n,q) \in \{(10,2),(9,2),(8,3),(8,2),(7,3),(7,2)\}$.*

Geometric subgroups

Here we prove Theorem 2.5.3 for $H \in \mathcal{C} \cup \mathcal{N}$. Recall that $\mathcal{C} = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_8$ is the collection of geometric subgroups, and $\mathcal{N}$ denotes the collection of novelty subgroups in Table 2.2. These subgroup collections are discussed in Section 2.3.2. We begin by stating a useful result for $G_0 = \mathrm{U}_n(q)$.

Lemma 2.5.5. *Let m and n be positive integers such that $n \geqslant 2$ and $m \leqslant n-1$, with $m = n-1$ only if n is even. Suppose r is a primitive prime divisor of $q^i - 1$, where $i = a\lfloor \frac{n}{2} \rfloor$ and*

$$a = \begin{cases} 2 & n \equiv 0, 1 \pmod 4 \\ 1 & n \equiv 2, 3 \pmod 4 \end{cases}. \tag{2.5}$$

Then r does not divide $|\mathrm{U}_m(q)|$.

Proof. This is an easy application of Lemma 2.4.10. □

Proposition 2.5.6. *Theorem 2.5.3 holds if $H \in \mathcal{C} \cup \mathcal{N}$.*

Proof. We proceed by inspecting the orders of G_0 (see [54, Table 5.1.A]) and H_0 (see [6] and [54]). In general, we search for primitive prime divisors of integers of the form $q^i - 1$ that divide $|G_0|$ but not $|H_0|$. Our approach is similar in most cases, so we only provide details in the following cases:

(a) $G_0 = \mathrm{P}\Omega_n^+(q)$ and H is of type $\mathrm{O}_m^-(q) \perp \mathrm{O}_{n-m}^-(q)$, where $2 \leqslant m < \frac{n}{2}$ even.

(b) $G_0 = \mathrm{U}_n(q)$ and H of type P_m, with $1 \leqslant m \leqslant n/2$.

(c) $G_0 = \mathrm{L}_n(q)$ and H is of type $\mathrm{GL}_m(q^k)$, where $n = mk$ and k is prime.

(d) $G_0 = \mathrm{L}_n(q), \mathrm{U}_n(q), \mathrm{PSp}_n(q)$ or $\mathrm{P}\Omega_n^+(q)$ and H is a $\mathcal{C}_6$-subgroup.

(e) $G_0 = \mathrm{P}\Omega_n^\epsilon(q)$ and H is of type $\mathrm{O}_1(q) \wr S_n$.

Case (a): *$G_0 = \mathrm{P}\Omega_n^+(q)$, H is of type $\mathrm{O}_m^-(q) \perp \mathrm{O}_{n-m}^-(q)$, and $2 \leqslant m < \frac{n}{2}$ even.*

By [54, Proposition 4.1.6], all prime divisors of $|H_0|$ divide

$$A := q(q^{\frac{n-m}{2}} + 1) \prod_{i=1}^{\frac{n-m-2}{2}} (q^{2i} - 1)$$

Hence, any primitive prime divisor of $q^j - 1$ with $j > n - m$ does not divide $|H_0|$.

Assume first that $m \geqslant 6$, (so $n \geqslant 14$). Since $n-m \leqslant n-6$, any primitive prime divisor of $q^{n-2} - 1$ or $q^{n-4} - 1$ divides $|G_0|$ but not $|H_0|$, so $\pi(G_0) - \pi(H_0) \geqslant 2$.

Now assume $m = 4$. As before, any primitive prime divisor of $q^{n-2} - 1$ does not divide $|H_0|$. If $n \equiv 2 \pmod 4$ then Lemma 2.4.10 implies that any primitive prime divisor of $q^{\frac{n}{2}} - 1$ is not a divisor of $|H_0|$, since $\frac{n}{2}$ is odd and $n - m < n$. Similarly, if $n \equiv 0 \pmod 4$ then any primitive prime divisor of $q^{(n-2)/2} - 1$ does not divide $|H_0|$. Thus $\pi(G_0) - \pi(H_0) \geqslant 2$.

Finally assume $m = 2$. Let

$$i = \begin{cases} \frac{n}{2} & \text{if } n \equiv 2 \pmod 4 \\ \frac{(n-2)}{2} & \text{if } n \equiv 0 \pmod 4 \end{cases}.$$

By the same reasoning, any primitive prime divisor of $q^i - 1$ divides $|G_0|$ but not $|H_0|$. These are the only possible primes that divide $|G_0|$ that do not divide $|H_0|$. By Theorem 2.4.9, there is always at least one primitive prime divisor of $q^i - 1$. Thus $\pi(G_0) - \pi(H_0) \leqslant 1$ if and only if there is a unique primitive prime divisor of $q^i - 1$ in which case, $\pi(G_0) - \pi(H_0) = 1$. This leads to Cases O6 and O7 in Table A3.

Case (b): *$G_0 = \mathrm{U}_n(q)$, H of type P_m with $1 \leqslant m \leqslant n/2$.*

Here

$$\begin{aligned} |H_0| &= dq^{m(2n-m)}(q^2 - 1)|\mathrm{SL}_m(q^2)||\mathrm{SU}_{n-2m}(q)| \\ &= dq^b \prod_{i=1}^{m}(q^{2i} - 1) \prod_{i=2}^{n-2m} (q^i - (-1)^i) \end{aligned}$$

where $d = 1/(q+1, n)$ and $b = n(n-1)/2$ (see [54, Proposition 4.1.18]).

We first assume that $(n,m) \neq (3,1),(4,2),(6,3)$ and $(n,q) \neq (4,2),(5,2),(6,2)$. These assumptions ensure the existence of the primitive prime divisors involved in the argument below. Take r and s to be primitive prime divisors of q^i-1 and q^j-1, respectively, where

$$i = \begin{cases} 2n-2 & n \text{ is even} \\ 2n & n \text{ is odd} \end{cases}, \qquad j = \begin{cases} 2n-6 & m \neq 1 \text{ and } n \text{ is even} \\ 2n-4 & m \neq 1 \text{ and } n \text{ is odd} \\ a\lfloor n/2 \rfloor & m = 1 \end{cases}$$

and a is as defined in (2.5). By inspection of $|G_0|$, it is easy to see that both r and s are prime divisors of $|G_0|$. For example, since $i/2 \leqslant n$ is odd, we know that $q^{i/2}+1$ divides $|G_0|$, and by definition r is a prime divisor of $q^{i/2}+1$. However, since $2m, 2(n-2m) < i$ the definition of a primitive prime divisor implies that r does not divide $|H_0|$. Using a similar argument for $m \neq 1$, we see that s is not a divisor of $|H_0|$. Finally if $m = 1$, then $|H_0| = dq^b(q^2-1)|\mathrm{U}_{n-2}(q)|$ and so Lemma 2.5.5 implies that s does not divide $|H_0|$. Thus $\pi(G_0) - \pi(H_0) \geqslant 2$ in all cases.

Assume that $(n,m) = (3,1)$ and take r to be a prime divisor of $|G_0| = dq^3(q^2-1)(q^3+1)$ that does not divide $|H_0| = dq^3(q^2-1)$. Then r must be an odd prime divisor of q^3+1, so r is a primitive prime divisor of either q^6-1 or q^2-1 by Lemma 2.4.10. However r cannot be a prime divisor of q^2-1, so the only possible prime divisors of $|G_0|$ that do not divide $|H_0|$ are the primitive prime divisors of q^6-1. Since $q \geqslant 3$, Theorem 2.4.9 implies that there always exists a primitive prime divisor of q^6-1. Thus $\pi(G_0)-\pi(H_0) \leqslant 1$ if and only if there exists a unique primitive prime divisor of q^6-1, in which case $\pi(G_0)-\pi(H_0) = 1$. This leads to Case U2 in Table A3. The cases with $(n,m) = (4,2)$ and $(6,3)$ are similar; here the only possible prime divisors of $|G_0|$ that do not divide $|H_0|$ are primitive prime divisors of $q^{2n-2}-1$. This case leads to Case U1 in Table A3.

The final cases to handle are those in which $(n,q) = (4,2),(5,2)$ or $(6,2)$. Here the result can be checked by direct calculation of $|G_0|$ and $|H_0|$; we find that the only cases with $\pi(G_0)-\pi(H_0) \leqslant 1$ are $(n,q,m) = (4,2,1),(4,2,2),(5,2,2),(6,2,3)$, which are recorded in Table A2, as well as Case U1 in Table A3.

Case (c): *$G_0 = \mathrm{L}_n(q)$, H is of type $\mathrm{GL}_m(q^k)$, where $n = mk$ and k is prime.*

Here all prime divisors of $|H_0|$ divide

$$A = kq^{\frac{n(m-1)}{2}} \prod_{i=1}^{m} (q^{ki}-1)$$

by [54, Proposition 4.3.6].

Assume first that $k \notin \{n, 2\}$ (note this implies $n \geqslant 6$). Take r and s to be primitive prime divisors of $q^{n-1}-1$ and $q^{n-2}-1$ respectively. Then $r \geqslant n$ and $s \geqslant n-1$ by Lemma 2.4.10, so $r, s > k$. Additionally, we note that $n-2 > k(m-1)$, so r and s do not divide $\prod_{i=1}^{m-1}(q^{ki}-1)$. Similarly, both $n-1$ and $n-2$ do not divide $n = km$, therefore we conclude that r and s are distinct prime divisors of $|G_0|$ that do not divide $|H_0|$.

Next assume that $n \geqslant 7$ and $k \in \{n, 2\}$. Here we observe that primitive prime divisors of $q^{n-3}-1$ and q^i-1 , where $i = n-1$ if $k = 2$, and $i = n-2$ if $k = n$, divide $|G_0|$ but not $|H_0|$. Thus it remains to deal with the cases $(n, k) = (6, 2), (5, 5), (4, 2), (3, 3)$ and $(2, 2)$.

Assume $(n, k) = (4, 2)$ or $(6, 2)$. Here the only possible prime divisors of $|G_0|$ that do not divide $|H_0|$ are primitive prime divisors of $q^{n-1}-1$. For example, if $(n, k) = (4, 2)$ then $A = 2q^2(q^2-1)(q^4-1)$ and $|G_0| = dq^6(q^2-1)(q^3-1)(q^4-1)$, where $d = 1/(q-1, 4)$. Thus $\pi(G_0) - \pi(H_0)$ is precisely the number of primitive prime divisors of q^3-1, so the result follows.

Next suppose that $(n, k) = (5, 5)$. Here $A = 5(q^5-1)$ so any primitive prime divisor of q^3-1 divides $|G_0|$ and not $|H_0|$. If $p \neq 5$ then p does not divide $|H_0|$, implying that $\pi(G_0) - \pi(H_0) \geqslant 2$, so we may assume $p = 5$. Take s to be the largest primitive prime divisor of q^4-1. Then s divides $|H_0|$ if and only if $s = 5$. Thus by Lemma 2.4.15 we may assume $q = 5$. This final case can be handled by direct calculation.

Now suppose that $(n, k) = (3, 3)$, in which case

$$|H_0| = \frac{3(q^3-1)}{(q-1)(q-1, 3)}.$$

Immediately we note that if $p \neq 3$, then p does not divide $|H_0|$. Additionally, by Lemma 2.4.2, if $r \neq 3$ is a prime divisor of $q-1$, then r divides $|G_0|$ but not $|H_0|$. Suppose first that $p \neq 3$. Then since p does not divide $|H_0|$, we may assume $q-1 = 3^l$ for some $l \geqslant 1$ (otherwise $\pi(G_0) - \pi(H_0) \geqslant 2$). By Lemma 2.4.1 this occurs if and only if $q = 4$, in which case it is easy to check that 2 and 5 divide $|G_0|$ but not $|H_0|$. Now suppose that $p = 3$. Then 3 does not divide $q-1$, so we may assume that $q-1 = r^l$ is a prime power, whence $q \in \{3, 9\}$ by Lemma 2.4.1. The case $q = 3$ does not occur since H is not maximal (see [6, Table 8.3]), and $q = 9$ can be handled by direct calculation (2 and 7 divide $|G_0|$ but not $|H_0|$).

Finally suppose that $(n, k) = (2, 2)$. Here $|H_0| = 2(q+1)$, so the only prime divisors of $|G_0|$ that do not divide $|H_0|$ are p if $p \geqslant 3$, and any odd prime divisor of $q-1$. Thus we may assume that either $p = 2$ and $q-1 = r^l$ for some prime r, or that $p \geqslant 3$ and $q-1 = 2^l$ (note that $\pi(G_0) - \pi(H_0) = 1$ in both cases). First assume $p = 2$ and $q-1 = r^l$,

so $q-1=2^f-1$ is a Mersenne prime by Lemma 2.4.1. Similarly, if $p \geqslant 3$ and $q-1=2^l$, then either $q=9$ or q is a Fermat prime. The result follows.

Case (d): *$G_0 = \mathrm{L}_n(q), \mathrm{U}_n(q), \mathrm{PSp}_n(q)$ or $\mathrm{P}\Omega_n^+(q)$ and H is a $\mathcal{C}_6$-subgroup.*

Here $n=r^m$ with r prime and $p \neq r$. From [54, Propositions 4.6.5-9], all prime divisors of $|H_0|$ divide

$$A := r\prod_{i=1}^{m}(r^i+1)(r^i-1).$$

Thus if s is a prime divisor of $|H_0|$ then $s \leqslant r^m+1 = n+1$. Let s_i be the largest primitive prime divisor of q^i-1.

Suppose first that $n \geqslant 7$. By Lemma 2.5.4 we easily reduce to the cases $(n,q) = (9,2),(8,3),(8,2),(7,3)$ and $(7,2)$, which can be handled by directly computing $|G_0|$ and $|H_0|$. For example, if $(n,q)=(7,2)$ then $|G_0| = 2^{21}.3^4.5.7^2.31.127$ and $|H_0| = 7.|\mathrm{Sp}_2(7)| = 2^4.3.7$, so $\pi(G_0)-\pi(H_0)=3$.

Next suppose $n=5$, so $G_0 = \mathrm{L}_5(q)$ or $\mathrm{U}_5(q)$, and $A = 2^3.3.5$. By Lemma 2.4.10 we have $s_5, s_{10} \geqslant 11$. Additionally, $s_4 \geqslant 13$ when $q \notin \{2,3,7\}$ by Lemma 2.4.15. Note that if $q \in \{2,3,7\}$ then H is not maximal (see [6, Tables 8.18 and 8.20]), so we do not need to consider these cases. Therefore we conclude that $\pi(G_0)-\pi(H_0) \geqslant 2$.

Now suppose $n=4$, so $A = 2.3^2.5$. If $p \geqslant 11$, then p does not divide $|H_0|$ and we have $s_4 \geqslant 13$ by Lemma 2.4.15, so $\pi(G_0)-\pi(H_0) \geqslant 2$. Now assume $p \leqslant 7$. Here we reduce to the cases $G_0 = \mathrm{L}_4(5), \mathrm{U}_4(3), \mathrm{U}_4(7), \mathrm{PSp}_4(3), \mathrm{PSp}_4(5)$ and $\mathrm{PSp}_4(7)$, see [6], (and recall that $\mathrm{PSp}_4(3) \notin \mathcal{A}$), which can all be handled by direct calculation. For example, if $G_0 = \mathrm{PSp}_4(5)$ then $|G_0| = 2^6.3^2.5^4.13$ and $|H_0| = 2^6.3.5$, so $\pi(G_0)-\pi(H_0)=1$.

Suppose $n=3$, so the only prime divisors of $|H_0|$ are 2 and 3. By the maximality of H, we must have $p>3$ (see [6]), so p does not divide $|H_0|$. Additionally, $s_3, s_6 \geqslant 7$ by Lemma 2.4.10, so $\pi(G_0)-\pi(H_0) \geqslant 2$.

Finally suppose $n=2$. Then $G_0 = \mathrm{L}_2(q)$ with $q=p \geqslant 5$, and the only prime divisors of $|H_0|$ are 2 and 3. Therefore p does not divide $|H_0|$. Additionally, the only other possible prime divisors of $|G_0|$ that do not divide $|H_0|$ are divisors of q^2-1 greater than 3. Thus we may assume that $q^2-1 = 2^a.3^b$ for some $a,b \geqslant 0$, since otherwise we have $\pi(G_0)-\pi(H_0) \geqslant 2$. Using Lemma 2.4.1 it is easy to see that $a,b \geqslant 1$. Now since $q+1$ and $q-1$ cannot both be divisible by 3, we see that two cases arise:

(i) $q+1 = 2^x 3^b$ and $q-1 = 2^y$, or

(ii) $q+1 = 2^x$ and $q-1 = 2^y 3^b$

where $x, y \geqslant 0$ and $x+y=a$. In case (i), Lemma 2.4.1 implies that $q = 2^y+1$ is a Fermat prime and we see that $2(2^{y-1}+1) = 2^x 3^b$, so $x = 1$ and $2^{y-1}+1 = 3^b$. Using Lemma 2.4.1, the only solutions are $(y,b) = (4,2)$ and $(2,1)$, so the only solutions in case (i) are $q = 5$ and 17. Similarly we can show that the only solution in case (ii) is $q = 7$.

Case (e): *$G_0 = \mathrm{P}\Omega_n^\epsilon(q)$, H is of type $\mathrm{O}_1(q) \wr S_n$.*

Here $q = p \geqslant 3$ and [54, Proposition 4.2.15] implies that all prime divisors of $|H_0|$ divide $n!$. Thus using Lemma 2.5.4, we immediately reduce to the cases $(n,q) = (8,3)$ and $(7,3)$. These can be handled by direct calculation and we deduce that $\pi(G_0) - \pi(H_0) \leqslant 1$ only if $(\epsilon, n, q) = (+,8,3)$ or $(\circ,7,3)$. In particular, $\pi(G_0) - \pi(H_0) = 1$ in both cases. □

Non-geometric subgroups

We now turn to the subgroups contained in the $\mathcal{S}$ collection (see Section 2.3.2 for more details). Recall that the *type* of $H \in \mathcal{S}$ coincides with the socle S of H. For $n \leqslant 12$ we can read off the possibilities for H from the tables in [6, Section 8.2]. Thus the proof for the low dimensional groups is similar to the proof of Proposition 2.5.6. For $n \geqslant 13$, our main tool is a result of Guralnick et al. [43], which describes the subgroups M of $\mathrm{GL}_n(q)$ such that $|M|$ is divisible by a primitive prime divisor of $q^i - 1$ for $\frac{n}{2} < i \leqslant n$ (see [43, Examples 2.1-2.9]).

Proposition 2.5.7. *Suppose $n \geqslant 13$ and $H \in \mathcal{S}$ has socle S. Then $|H_0|$ is divisible by a primitive prime divisor of $q^i - 1$ with $\frac{n}{2} < i \leqslant n$ only if either*

(i) *$S = A_m$ and $m = n+1, n+2$; or*

(ii) *(S, n, i) is found in Table 2.3.*

Lemma 2.5.8. *Theorem 2.5.3 holds if $H \in \mathcal{S}$, $n \geqslant 13$ and $S = A_m$ with $m = n+1$ or $n+2$.*

Proof. Assume $S = A_m$ with $m = n+1$ or $n+2$, so every prime divisor of $|H_0|$ divides $(n+2)!$. Since $n \geqslant 13$, $|G_0|$ is divisible by at least two primes larger than $n+2$ by Lemma 2.5.4, hence $\pi(G_0) - \pi(H_0) \geqslant 2$. □

Lemma 2.5.9. *Theorem 2.5.3 holds if $H \in \mathcal{S}$, $n \geqslant 13$ and $S \neq A_m$ for $m = n+1$ or $n+2$.*

Table 2.3: The table for Proposition 2.5.7

S	n	i
M_{23}	22	22
M_{24}	23	22
J_1	20	18
J_3	18	$16, 18$
Co_3	23	22
Co_2	23	22
Co_1	24	22
Ru	28	28
${}^2B_2(8)$	14	12
$G_2(3)$	14	12
$\mathrm{PSp}_4(4)$	18	16
$\mathrm{L}_d(s), d \geqslant 3$	$\frac{s^d-1}{s-1} - 1, \frac{s^d-1}{s-1}$	$\frac{s^d-1}{s-1} - 1$
$\mathrm{U}_d(s), d \geqslant 3$	$\frac{s^d+1}{s+1} - 1, \frac{s^d+1}{s+1}$	$\frac{s^d+1}{s+1} - 1$
$\mathrm{PSp}_{2d}(s)$	$\frac{1}{2}(s^n - 1), \frac{1}{2}(s^n + 1)$	$\frac{1}{2}(s^n - 1)$
$\mathrm{PSp}_{2d}(3)$	$\frac{1}{2}(3^n - 1), \frac{1}{2}(3^n + 1)$	$\frac{1}{2}(3^n - 3)$
$\mathrm{L}_2(s)$	$s-1, s, s+1$	$s-2$
	$s, s+1$	s
	$s-1, s, s+1$	$s-1$
	$\frac{1}{2}(s-1), \frac{1}{2}(s+1)$	$\frac{1}{2}(s-1)$
	$\frac{1}{2}(s-1), \frac{1}{2}(s+1)$	$\frac{1}{2}(s-3)$

Proof. Take r_j, r_k and r_l to be primitive prime divisors of $q^j - 1$, $q^k - 1$ and $q^l - 1$ respectively, where $j := 2\lfloor \frac{n-1}{2} \rfloor$, $k := 2\lfloor \frac{n-3}{2} \rfloor$ and $l := 2\lfloor \frac{n-5}{2} \rfloor$. Note that r_j, r_k and r_l all exist and divide $|G_0|$, and $\frac{n}{2} < j, k, l < n$. Proposition 2.5.7 implies that if (S, n) does not appear in Table 2.3 then r_j, r_k and r_l do not divide $|H_0|$ and thus $\pi(G_0) - \pi(H_0) \geqslant 3$. Assume (S, n, i) is found in Table 2.3 and $(S, n, i) \neq (\mathrm{L}_2(s), s+1, s-2)$. By inspection of the table we have $n - 2 \leqslant i \leqslant n$, which implies that neither r_k nor r_l divide $|H_0|$, so $\pi(G_0) - \pi(H_0) \geqslant 2$. Finally assume $(S, n, i) = (\mathrm{L}_2(s), s+1, s-2)$. If $|H_0|$ is divisible by a primitive prime divisor of $q^t - 1$ for $\frac{n}{2} < t \leqslant n$ then $t = n - 3$. Thus r_j and r_l do not divide $|H_0|$, and so once again we conclude that $\pi(G_0) - \pi(H_0) \geqslant 2$. □

Lemma 2.5.10. *Theorem 2.5.3 holds if $H \in \mathcal{S}$ and $n \leqslant 12$.*

Proof. Here we inspect the appropriate tables in [6, Section 8.2]. For brevity, we only provide the details in the following cases:

(a) $G_0 = \mathrm{P}\Omega_8^+(q)$ and $S = {}^3D_4(q_0)$ with $q = q_0^3$.

(b) $G_0 = \mathrm{U}_5(q)$ and $S = \mathrm{L}_2(11)$.

(c) $G_0 = \mathrm{PSp}_4(q)$ and $S = {}^2B_2(q)$ with $q \geqslant 4$ even.

(d) $G_0 = \mathrm{L}_2(q)$ and $S = A_5$.

First we consider (a). Here $|H_0| = q_0^{12}(q_0^8 + q_0^4 + 1)(q_0^6 - 1)(q_0^2 - 1)$ and we immediately observe that any primitive prime divisor of $q_0^{18} - 1$ $(= q^6 - 1)$ divides $|G_0|$ but not $|H_0|$. Take s to be a primitive prime divisor of $q_0^4 - 1$. By Lemma 2.4.10, s divides $q_0^{12} - 1 = q^3 - 1$, so s divides $|G_0|$. Additionally, Lemma 2.4.10 shows that $s \geqslant 5$ and does not divide $q_0^{12}(q_0^6 - 1)(q_0^2 - 1)$. By Lemma 2.4.2 we have $(q_0^{12} - 1)_s = (q_0^4 - 1)_s$, so s does not divide $|H_0|$. Therefore $\pi(G_0) - \pi(H_0) \geqslant 2$.

Next, let us turn to case (b). From [6, Table 8.21] we have $q = p \equiv 2, 6, 7, 8, 10 \pmod{11}$ and the prime divisors of $|H_0|$ are 2,3,5 and 11. Suppose $q \notin \{2, 7\}$. Then by Lemma 2.4.15, there exist primitive prime divisors r_4 and r_6 of $q^4 - 1$ and $q^6 - 1$, respectively, such that $r_4, r_6 \geqslant 13$, so $\pi(G_0) - \pi(H_0) \geqslant 2$. The remaining cases $q \in \{2, 7\}$ can be handled by direct calculation, showing that $\pi(G_0) - \pi(H_0) = 0$ when $q = 2$, and $\pi(G_0) - \pi(H_0) = 3$ when $q = 7$.

Now consider case (c). Here we have $q = 2^f$ with $f \geqslant 3$ odd. Note that $|{}^2B_2(q)| = q^2(q^2 + 1)(q - 1)$, so any odd prime divisor of $q + 1$ divides $|G_0|$ but not $|H_0|$. Therefore

we may assume $q+1 = r^l$ for some odd prime r. By Lemma 2.4.1 this occurs if and only if $f = 3$, or $f = 2^n$ and $r = 2^f + 1$ is a Fermat prime. However, $f \geqslant 3$ is odd, so we may assume $q = 8$. Here it is straightforward to show that 3 is the only prime dividing $|G_0|$ that does not divide $|H_0|$.

Finally we turn to case (d). From [6, Table 8.2] we have $q = p \equiv \pm 1 \,(\mathrm{mod}\, 10)$, or $q = p^2$ with $p \equiv \pm 3 \,(\mathrm{mod}\, 10)$. Note that the prime divisors of $|H_0|$ are 2, 3 and 5. Suppose first that $p \geqslant 7$. Then p does not divide $|H_0|$ and the only other possible prime divisors of $|G_0|$ that do not divide $|H_0|$ are the prime divisors r of $q^2 - 1$ with $r \geqslant 7$. Therefore, if $q^2 - 1 = 2^a.3^b.5^c$ for some $a, b, c \geqslant 0$ we have $\pi(G_0) - \pi(H_0) = 1$, otherwise $\pi(G_0) - \pi(H_0) \geqslant 2$. Finally suppose $p \leqslant 7$. Here $q = 9$ and by direct computation we obtain $\pi(G_0) - \pi(H_0) = 0$. □

2.5.2 Exceptional groups

Here we complete the proof of Theorem 2.5.1 by handling the groups with $G_0 \in \mathcal{B}$, a simple exceptional group of Lie type over $\mathbb{F}_q$. That is we prove the following:

Theorem 2.5.11. *Let G be an almost simple group with socle $G_0 \in \mathcal{B}$, and let H be a core-free maximal subgroup of G. Then $\pi(G_0) \leqslant \pi(H_0) + 1$ if and only if one of the following holds:*

(i) $\pi(G_0) = \pi(H_0)$ *and* $(G_0, H_0) = (G_2(3), \mathrm{L}_2(13))$ *or* $({}^2F_4(2)', \mathrm{L}_2(25))$.

(ii) $\pi(G_0) = \pi(H_0) + 1$, (G_0, H, i) *is one of the cases recorded in Table B1 and there exists a unique primitive prime divisor of* $q^i - 1$.

Proof. As before, we proceed by inspecting the orders of G_0 and H_0 (see [54, Table 5.1.B] and the references provided in Section 2.3.2). The analysis is similar in most instances, so we only provide details for a handful of cases:

(a) $G_0 = {}^2F_4(q)$ and $H_0 = a^{\pm}{:}12$, where $a^{\pm} = (q^2 \pm \sqrt{2q^3} + q \pm \sqrt{2q} + 1)$.

(b) $G_0 = E_6(q)$ and $H_0 = E_6(q_0).((3, q-1), k)$, where $q = q_0^k$ and k is a prime.

(c) $G_0 = {}^3D_4(q)$ and $H_0 = G_2(q)$.

(d) $G_0 = E_7(q)$ and H is a P_7 parabolic subgroup.

(e) $G_0 = E_8(q)$ and $\mathrm{Soc}(H) = S = \mathrm{L}_2(q_0) \in \mathrm{Lie}(p)$, with $q_0 \leqslant (2, q-1)1312$.

First consider case (a) and note that $|G_0| = q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$, and $q = 2^f$ where $f = 2n+1$ for some $n \geqslant 1$. Additionally, it is easy to see that $a^+a^- = q^4 - q^2 + 1 = (q^6+1)/(q^2+1)$, so both a^+ and a^- divide q^6+1. Thus all prime divisors of $|H_0|$ divide $6(q^6+1)$. Assume first that $f = 3$. Here it is easy to show computationally that both 7 and 19 divide $|G_0|$ and not $|H_0|$, so $\pi(G_0) - \pi(H_0) = 2$. Finally assume that $f > 3$. Take s_6 to be the largest primitive prime divisor of $q^6 - 1$ and let s_2 be the largest primitive prime divisor of $2^{2f} - 1$ (these both exist by Theorem 2.4.9). Note that s_2 is also a primitive prime divisor of $q^2 - 1$ (see Lemma 2.4.11). By Lemma 2.4.10 we have $s_6 = 6d + 1$ and $s_2 = 2fh + 1$ for some $d, h \geqslant 1$. Thus $s_6, s_2 \geqslant 7$. Additionally both s_6 and s_2 divide $q^6 - 1$ and so cannot divide $q^6 + 1$. Therefore neither s_2 nor s_6 divide $|H_0|$, implying that $\pi(G_0) - \pi(H_0) \geqslant 2$.

Now let us assume we are in case (b). Here we have $|G_0| = \frac{1}{d}q_0^{36k}\prod_{i\in I}(q_0^{ik} - 1)$ with $I = \{2, 5, 6, 8, 9, 12\}$, where $d = (3, q-1)$ and every prime divisor of $|H_0|$ must divide $q_0\prod_{j\in J}(q_0^j - 1)$ with $J = \{5, 9, 12\}$. It is clear that primitive prime divisors of $q_0^{12k} - 1$ and $q_0^{9k} - 1$ divide $|G_0|$, but not $|H_0|$, since $12k, 9k \geqslant 18$.

Next consider the case (c). Here

$$|G_0| = q^{12}(q^6-1)^2(q^4-q^2+1) \text{ and } |H_0| = q^6(q^2-1)(q^6-1).$$

First observe that r is a primitive prime divisor of $q^{12}-1$ if and only if r divides q^4-q^2+1. Thus the only prime divisors of $|G_0|$ that do not divide $|H_0|$ are the prime divisors of q^4-q^2+1. Therefore $\pi(G_0)-\pi(H_0) = 1$ if and only if $q^4-q^2+1 = r^l$ for some odd prime r. Using the substitution $x = -q^2$ in Theorem 2.4.13, we deduce there are no appropriate solutions to this equation for $l \geqslant 2$. So we may assume $q^4 - q^2 + 1 = r$, which leads to case D2 in Table B1. We note that there are solutions to the equation $q^4 - q^2 + 1 = r$ with r prime. For example, we can take $q \in \{2, 3, 4, 9\}$.

Next let us assume we are in case (d). Here $|G_0| = \frac{1}{d}q^{63}\prod_{i\in I}(q^i - 1)$, where $I = \{2, 6, 8, 10, 12, 14, 18\}$ and $d = (2, q-1)$, and we have $H_0 = QL$ where Q is a p-group and the prime divisors of $|L|$ divide $|E_6(q)|$. Thus all prime divisors of $|H_0|$ divide

$$q(q^5-1)(q^8-1)(q^9-1)(q^{12}-1),$$

hence primitive prime divisors of $q^{14} - 1$ and $q^{18} - 1$ divide $|G_0|$, but not $|H_0|$.

Finally assume we are in case (e) and let $q_0 = p^t$. Here

$$|G_0| = p^{120f}\prod_{i\in I}(p^{if} - 1) \text{ and } |S| = \frac{1}{d}p^t(p^{2t} - 1),$$

where $I = \{2, 8, 12, 14, 18, 20, 24, 30\}$ and $d = (2, p^t - 1)$. We note that $|H_0|$ divides $|S|dt$. The largest powers of 2 and 3 less than $(2, q-1)1312$ are 2^{10} and 3^8 respectively. Therefore we may assume $t \leqslant 10$, which implies that $2t < 24f, 30f$. Thus primitive prime divisors of $p^{24f} - 1$ and $p^{30f} - 1$ divide $|G_0|$, but not $|H_0|$. □

By combining Theorems 2.5.3 and 2.5.11, we conclude that the proof of Theorem 2.5.1 is complete.

CHAPTER

3

ALTERNATING AND SPORADIC GROUPS

In this chapter we prove Theorems 1 and 2 for almost simple groups with an alternating or sporadic socle. The content of this chapter is a combination of the work in [13, Sections 3 and 5] and [45, Section 4].

3.1 Alternating socle: The primitive case

Here we begin the proof of Theorem 1 by considering the almost simple primitive 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 Tables P1 or P2.*

First we handle the cases with $n \leqslant 20$.

Proposition 3.1.1. *The conclusion to Theorem 3.1 holds if $n \leqslant 20$.*

Proof. This is an entirely straightforward Magma [5] calculation. For each group G with socle A_n such that $5 \leqslant n \leqslant 20$, we use the function `MaximalSubgroups` to obtain a list

of maximal subgroups of G (up to conjugacy). Then for each maximal subgroup H we use the `IsConjugate` command to determine the fusion of conjugacy classes of elements of prime order between H and G. Then G is almost elusive if and only if there is a unique G-class of elements of prime order that intersects H. □

For the remainder of this section, we may assume $G = A_n$ or S_n with $n > 20$. We will divide the rest of the proof into three parts, according to the action of H on $\{1, \ldots, n\}$ (see Theorem 2.3.4). 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.

3.1.1 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 $1 \leqslant k < n/2$. Note that $|\Omega| = \binom{n}{k}$.

Lemma 3.1.2. *If $k \geqslant 4$ then G is not almost elusive.*

Proof. Suppose $k \geqslant 4$. Since $n > 20$, Proposition 2.4.8 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 3.1.3. *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 of this proof 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 $[2^{n/2}]$ (recall $n > 20$). 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 3.1.4. *If $k = 2$ then G is almost elusive if and only if $G = S_n$ 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 2.4.1 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 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 2.4.1, it follows that either $n = 9$, or $n = r = 2^m + 1$ is a Fermat prime.

Since $n > 20$ we may assume $n = r = 2^m + 1$ is a Fermat prime, so $|\Omega| = 2^{m-1}r$ 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 3.1.5. *The conclusion to Theorem 3.1 holds if H is intransitive.*

Proof. Due to Lemmas 3.1.2, 3.1.3 and 3.1.4 we may assume $k = 3$ and since $n \geqslant 21$ our aim is to show that G is not almost elusive. 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.

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 2.4.1 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 $l \geqslant 11$ 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 $l = 3^a$, $a > 2$ 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 2.4.1 implies that there are no solutions for $n > 20$. 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 2.4.1 we deduce that there are no solutions for $n > 20$, so we conclude that G is not almost elusive.

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 no solutions with $n \geqslant 21$ by Lemma 2.4.1. Therefore G is not 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 2.4.1 it follows that $(b, c) = (1, 2)$ and thus $n = 5$, which is a contradiction since $n \geqslant 21$. □

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 3.1.1, we will assume $n \geqslant 21$.

Lemma 3.1.6. *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. □

Proposition 3.1.7. *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 3.1.1, we may assume $n \geqslant 21$. Applying Lemma 2.4.3, 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 3.1.6 implies that every r-cycle and every s-cycle in G is a derangement. Therefore, G is not almost elusive. □

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 3.1.8. *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 [11, Proposition 3.5], which follows by combining classical results of Jordan [49] and Manning [68]. Now consider (ii). Seeking a contradiction, suppose $|\Omega| = r^a$ for some prime r.

First assume $G = A_n$. By [42, Theorem 1] we have $n = r^a$ and $H \cong A_{n-1}$, so [81, 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 $H \cap L = \mathrm{Stab}_L(k) \leqslant \mathrm{Stab}_G(k)$ for some $k \in \{1, \ldots, n\}$. Since $|H : H \cap L| = 2$ we have $|H : \mathrm{Stab}_L(k)| = 2$ and thus $\mathrm{Stab}_L(k)$ is normal in H. In particular, $\mathrm{Stab}_L(k) = \mathrm{Stab}_L(k^h)$ 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 3.1.9. *The conclusion to Theorem 3.1 holds if H is primitive.*

Proof. By Proposition 3.1.1, we may assume $n \geqslant 21$. Then Lemma 3.1.8 implies that G is not almost elusive. □

In view of Propositions 3.1.5, 3.1.7 and 3.1.9 the proof of Theorem 3.1 is complete.

3.2 Alternating socle: The quasiprimitive case

Throughout Section 3.2 we let G be an almost simple group with socle $G_0 = A_n$ and let H be a core-free non-maximal subgroup of G such that $G = G_0H$. We note that due to Lemma 2.1.28, we may embed H in a core-free maximal subgroup M of G. Recall that we say a pair of groups (G, H) is almost elusive if G is almost elusive with respect to the natural action of G on G/H.

Here we prove Theorem 2 for the almost simple groups with alternating socle. That is we prove the following result.

Theorem 3.2. *The pair (G, H) is almost elusive if only if (G, H) is recorded in the first three rows of Table Q2.*

Remark 3.2.1. Suppose (G, H) is recorded in the first row of Table Q2. Then $(G, H) = (\mathrm{M}_{10}, 3^2{:}4)$. In this case (G, K) is almost elusive for any subgroup K of G isomorphic to H. Next let us suppose that (G, H) is as in the second or third row of Table Q2. Then $(G, H, M) = (A_9, (A_5 \times 3){:}2, (A_6 \times 3){:}2)$ or $(S_9, S_5 \times S_3, S_6 \times S_3)$. In both cases there are exactly two conjugacy classes of subgroups of G with representatives isomorphic to H. However, only one of these conjugacy classes leads to an almost elusive example. In particular, for (G, H) to be almost elusive, we require the relevant A_5 or S_5 subgroup of H to be a primitive subgroup of the corresponding A_6 or S_6 subgroup of M.

In order to prove Theorem 3.2, we may assume that (G, M) is primitive and almost elusive by Lemma 2.1.30. That is it remains to handle the cases where (G, M) is contained in Table P1 or P2. We begin by considering some small cases.

Proposition 3.2.2. *Theorem 3.2 holds when $n \leqslant 20$.*

Proof. Let M be a core-free maximal subgroup of G such that $H < M$. Then by Lemma 2.1.30, (G, M) is recorded in Table P1 or P2. As in the proof of Proposition 3.1.1, we can use Magma to construct G and M. Then using the `MaximalSubgroups` command, we obtain a list of representatives of the conjugacy classes of maximal subgroups of M. For each such maximal subgroup L, we first check that $|L||G_0|/|L \cap G_0| = |G|$, which ensures that G acting on the cosets of L is quasiprimitive, and we use `Core` to check that L is a core-free subgroup of G. We then determine if (G, L) is almost elusive by using `IsConjugate` to identify the fusion of L-classes of prime order elements in G. If (G, L) is not almost elusive, then it is discarded. However if (G, L) is almost elusive, then we inspect the maximal subgroups of L and we repeat this process until no further almost elusive groups arise. □

In view of Proposition 3.2.2 it remains to handle Cases 6-10 in Table P1. Recall we say that (G, H) contains a derangement of order r if G contains a derangement of order r with respect to the natural action of G on G/H.

Proposition 3.2.3. *Theorem 3.2 holds for (G, M) as in Case 6, 9 or 10 of Table P1.*

Proof. Here $(G, M) = (A_n, A_{n-1})$ or (S_n, S_{n-1}), where $n = r^a$ and r is a prime (with $a \geqslant 1$ in Case 6, and $a \geqslant 2$ in Case 9), or $n = 2r^a$ with $r \geqslant 3$ a prime and $a \geqslant 2$. Since $H < M$ and (G, M) is almost elusive with a unique class of derangements of order r, we conclude that (G, H) contains derangements of order r. In view of Proposition 3.2.2, we may assume that $n > 20$.

To begin the analysis, by Lemma 2.1.29 we may assume that H is a maximal subgroup of M, where we view M as the stabiliser in G of $n \in \{1, \ldots, n\}$. Therefore H either acts intransitively, imprimitively or primitively on $\{1, \ldots, n-1\}$. Suppose first that $\pi(M_0) > \pi(H_0)$. Then there exists a prime $s \in \alpha(M_0)$ such that $s \notin \alpha(H_0)$ and so every element of order s in G_0 is a derangement. If $s \neq r$ then it is easy to see that G is not almost elusive, since G contains derangements of order s and r. If $s = r$, then in particular $r \in \alpha(M_0)$ and so $a \geqslant 2$. Therefore G contains at least two conjugacy classes of elements of order r, so G is not almost elusive. Thus we may assume that $\pi(M_0) = \pi(H_0)$. By [60, Corollary 5] we deduce that H must act intransitively on $\{1, \ldots, n-1\}$. That is, $H = (S_k \times S_{n-1-k}) \cap M$ for some $1 \leqslant k < (n-1)/2$. In particular, H is the stabiliser in G of the partition

$$\{1, \ldots, k\} \cup \{k+1, \ldots, n-1\} \cup \{n\}.$$

We will show that in each case (G, H) also contains derangements of order s for some prime $s \neq r$, so (G, H) is not almost elusive.

Assume first that $k \geqslant 4$. The result follows from inspection of the proof of Lemma 3.1.2. However we provide the details for completeness. First observe that $|G : H| = n\binom{n-1}{k}$. By Proposition 2.4.8, $\binom{n-1}{k}$ is divisible by a prime s such that $s > k$, and note that s does not divide n. Thus $s \neq r$ and s divides $n-1-t$ for some $t \in \{0, 1, \ldots, k-1\}$. Consider an element $g \in G$ with cycle shape $[s^{(n-1-t)/s}, 1^{t+1}]$. Since $t < k$ it follows that $g \notin H$, so g is a derangement.

Next let us assume that $k = 1$ or 2. Suppose s is an odd prime divisor of $n-1$. Then every element in G with cycle shape $[s^{(n-1)/s}, 1]$ is a derangement. Thus we may assume that $n - 1 = 2^t$ for some $t \geqslant 5$ (recall we are assuming that $n > 20$). This implies $n = r$ is a Fermat prime by Lemma 2.4.1, in which case $G = S_n$ and $M = S_{n-1}$ (see Table P1). If $k = 1$, then any element in G with cycle shape $[2^{(n-1)/2}, 1]$ is a derangement. And if $k = 2$ and s is an odd prime divisor of $n-2$, then $s \neq r$ and any element in G with cycle shape $[s^{(n-2)/s}, 1^2]$ is a derangement.

Finally we assume $k = 3$. Suppose there exist prime divisors s_1 and s_2 of $n-1$ and $n-2$ respectively, such that $s_1, s_2 \geqslant 5$. Then any element in G with cycle shape $[s_1^{(n-1)/s_1}, 1]$ or $[s_2^{(n-2)/s_2}, 1^2]$ is a derangement. Thus G is almost elusive only if both $n-1$ and $n-2$ are only divisible by the primes 2 and 3. Then either $(n-1, n-2) = (2^m, 3^b)$ or $(3^b, 2^m)$ for some $b \geqslant 3$ and $m \geqslant 5$ (recall $n > 20$), but this is impossible by Lemma 2.4.1. The result follows. □

Proposition 3.2.4. *Theorem 3.2 holds for (G, M) as in Case 7 or 8 of Table P1.*

Proof. Here $G = S_n$, $M = S_{n-2} \times S_2$ and either $n = 2^m$ and $n - 1 = r$ is a Mersenne prime (Case 7), or $n = 2^m + 1 = r$ is a Fermat prime (Case 8). By Proposition 3.2.2 we may assume $n > 20$. Note that (G, H) contains derangements of order r.

By Lemma 2.1.29, we may begin by assuming that H is maximal in M. By applying [79, Lemma 1.3], we see that the maximal subgroups of M are as follows:

(i) $(A_{n-2} \times 1).2$

(ii) S_{n-2}

(iii) $L \times S_2$ where L is a maximal subgroup of S_{n-2}.

First suppose that H is as in case (i). Then up to conjugacy

$$H = \langle A_{n-2}, (n-3, n-2)(n-1, n) \rangle \leqslant G_0,$$

which contradicts the fact that $G = G_0 H$.

Now suppose H is as in case (ii). Here $H = S_{n-2}$ and every element of H has cycle shape $[a, 1^2]$, where a is a partition of $n - 2$. If $n = 2^m$, then any involution in G with cycle shape $[2^{n/2}]$ is a derangement. Similarly, if $n = 2^m + 1$ is a Fermat prime, then any involution in G with cycle shape $[2^{(n-1)/2}, 1]$ is a derangement. Thus (G, H) contains derangements of order r and of order 2, so (G, H) is not almost elusive.

Finally suppose H is as in case (iii). By Lemma 2.1.27, we may assume $\pi(M_0) = \pi(H_0)$, so $|H_0|$ is divisible by every prime $p \leqslant n-2$. Thus $|L|$ must be divisible by the two largest primes not exceeding $n - 2$. Therefore, [60, Theorem 4] implies that either $L = A_{n-2}$, or $L = S_k \times S_{n-2-k}$ for some $1 \leqslant k < (n-2)/2$. We recall that (G, H) contains a conjugacy class of derangements of order r (where $r = n - 1$ when $n = 2^m$, and $r = n$ when n is a Fermat prime). We show that in each of these cases (G, H) contains an additional class of derangements of prime order, so (G, H) is not almost elusive.

Suppose first that $H = A_{n-2} \times S_2$. If $n = 2^m$, then any involution in G with cycle shape $[2^{n/2}]$ is a derangement (since $n/2$ is even). Similarly, if $n = 2^m + 1$ is a Fermat prime, then any involution in G with cycle shape $[2^{(n-1)/2}, 1]$ is a derangement (since $(n-1)/2$ is even).

For the remainder of the proof we may assume $H = S_k \times S_{n-2-k} \times S_2$ for some $1 \leqslant k < (n-2)/2$. Up to conjugacy, H is the stabiliser of the partition

$$\{1, \ldots, k\} \cup \{k+1, \ldots, n-2\} \cup \{n-1, n\}.$$

Suppose $k \geqslant 4$. By Proposition 2.4.8 there exists a prime $s > k$ that divides $\binom{n-2}{k}$, which means that $s \neq r$ and s divides $n-2-t$ for some $t \in \{0, 1, \ldots, k-1\}$. Thus any element in G with cycle shape $[s^{(n-2-t)/s}, 1^{t+2}]$ is a derangement. Now suppose $k = 1$ or 2. Let s be an odd prime divisor of $n-2$. Then any element in G with cycle shape $[s^{(n-2)/s}, 1^2]$ is a derangement. Finally suppose $k = 3$. Assume first that $n = 2^m$ and $n-1$ is a Mersenne prime. Then any element with cycle shape $[2^{n/2}]$ is a derangement. Now assume $n = r = 2^m + 1$ is a Fermat prime. Then $n - 2 = 2^m - 1$ is odd and by Lemma 2.4.1 there exists a prime $s \geqslant 5$ such that s divides $n-2$ (recall $n > 20$). Thus any element in G with cycle shape $[s^{(n-2)/s}, 1^2]$ is a derangement. The result follows. □

This completes the proof of Theorem 3.2.

3.3 Sporadic socle

Next we prove Theorems 1 and 2 for the almost simple groups with socle a sporadic group.

Theorem 3.3. *Let G be an almost simple group with socle G_0, a simple sporadic group. Let H be a core-free subgroup of G such that $G = G_0H$. Then G is not almost elusive.*

Proof. Suppose that H is maximal in G. Assume first that G is not the Monster or the Baby Monster. Here we can use the GAP Character Table Library [7] to show that G is not almost elusive. Indeed, the character tables of both G and H are available in [7]. We begin by obtaining the character table of G using the `CharacterTable` command. From the character table, we use `OrdersClassRepresentatives` to obtain a list of the orders of the conjugacy class representatives in G. The maximal subgroups of G (and their character tables) can be accessed using the `Maxes` function. For each maximal subgroup H we obtain the character table and then use `FusionConjugacyClasses` to return the fusion of H-classes in G. It is now a routine exercise to check that G has at least two conjugacy classes of prime order derangements, with the exception of the elusive example $(G, H) = (\mathrm{M}_{11}, \mathrm{L}_2(11))$.

Next assume $G = \mathbb{B}$ is the Baby Monster. The complete list of maximal subgroups of G (up to conjugacy) is conveniently presented in the Web-Atlas [82] and it is easy to check that $\pi(G) - \pi(H) \geqslant 2$ 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 $G = \mathbb{M}$ is the Monster. By Theorem 2.3.5 there are 44 known conjugacy classes of maximal subgroups of G and any additional maximal subgroup has to be almost simple, with socle $\mathrm{L}_2(8)$, $\mathrm{L}_2(13)$, $\mathrm{L}_2(16)$ or $\mathrm{U}_3(4)$. In every case, including the list of candidate maximal subgroups, one checks that $\pi(G) - \pi(H) \geqslant 2$ and the result follows as before.

The result now follows immediately from Lemma 2.1.30. □

CHAPTER

4

CLASSICAL GROUPS

In this chapter we prove Theorems 1 and 2 for the classical groups. Recall that throughout this thesis, unless stated otherwise, all groups are finite. Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple quasiprimitive permutation group with socle G_0 a simple classical group over $\mathbb{F}_q$ (where $q = p^f$ for p prime and $f \geqslant 1$). We recall that we use $\mathcal{A}$ to denote the set of classical groups as defined in Notation 2.3.2, and throughout this chapter we will take $G_0 \in \mathcal{A}$.

We partition this chapter into three sections. We begin by providing some preliminary results on the classical groups, including results on elements of prime order and their conjugacy classes. We then focus on the primitive classical groups and prove Theorem 1 in this setting. Finally we turn our attention to the quasiprimitive groups and prove Theorem 2 for classical groups.

We note that the content of this chapter is a combination of work from [13, Sections 4.1 and 4.2], [44] and [45, Section 4].

4.1 Conjugacy classes

In order to classify the almost elusive almost simple classical groups we require an understanding of the conjugacy classes of prime order elements. In this section, we provide a

brief overview of this topic, working closely with [9, Chapter 3], which provides a more detailed analysis. Throughout this section, let G be an almost simple group with socle G_0, a simple classical group over $\mathbb{F}_q$, where $q = p^f$ such that p is prime and $f \geqslant 1$, and let V denote the natural module for G_0. As well as understanding the representatives of conjugacy classes of elements of prime order, we are also interested in the number of such classes. We begin by stating a well known result (see [34], for example).

Lemma 4.1.1. *Let G be a group and let H be a subgroup of G. Take r to be a prime divisor of $|H|$ and suppose that H has α conjugacy classes of elements of order r. Then G has at least $\alpha/|G : H|$ conjugacy classes of elements of order r.*

Proof. Let $\mathcal{K}_r(G)$ and $\mathcal{K}_r(H)$ denote the number of conjugacy classes of elements of order r in G and H, respectively. Additionally let G_r and H_r denote the set of elements of order r in G and H, respectively. By the Orbit-Counting Lemma (working with the action of G on G_r by conjugation, and similarly H on H_r) we have

$$\mathcal{K}_r(G) = \frac{1}{|G|}\sum_{x\in G}|C_G(x)\cap G_r|, \quad \mathcal{K}_r(H) = \frac{1}{|H|}\sum_{x\in H}|C_H(x)\cap H_r|.$$

We note that $H_r \subseteq G_r$ and for all $x \in G$ we have $C_H(x) \subseteq C_G(x)$. Thus

$$\sum_{x\in H}|C_H(x)\cap H_r| \leqslant \sum_{x\in G}|C_G(x)\cap G_r|.$$

Therefore

$$\begin{aligned}\mathcal{K}_r(G) &\geqslant \frac{1}{|G|}\sum_{x\in H}|C_H(x)\cap H_r| \\ &= \frac{1}{|G:H|}\mathcal{K}_r(H).\end{aligned}$$

□

This result is a useful tool for showing that a group is not almost elusive. In most cases we can focus on looking at conjugacy classes of derangements of prime order in G_0 and $\mathrm{Inndiag}(G_0)$ (the group generated by the inner and diagonal automorphisms of G_0, see Section 2.3.1), and then by applying Lemma 4.1.1 we can determine a lower bound on the number of such classes in $\mathrm{Aut}(G_0)$.

The analysis of conjugacy classes of elements of prime order in $\mathrm{Inndiag}(G_0)$ divides naturally into two cases: semisimple and unipotent. Take $x \in \mathrm{Inndiag}(G_0)$ to be an element of prime order r. We say that x is *semisimple* if $(r, p) = 1$, and *unipotent* if $r = p$. We begin with a discussion of the semisimple elements.

4.1.1 Semisimple elements

Our main focus will be on semisimple elements of odd prime order; at the end of this section, we comment briefly on semisimple involutions. We first state [40, Theorem 4.2.2(j)].

Theorem 4.1.2. *Suppose $x \in \mathrm{Inndiag}(G_0)$ is a semisimple element of prime order. Then $x^{G_0} = x^{\mathrm{Inndiag}(G_0)}$.*

We will now discuss the notation we use for semisimple elements.

Semisimple elements of odd prime order

Take $x \in \mathrm{Inndiag}(G_0)$ to be an element of odd prime order $r \neq p$, so r is a primitive prime divisor of $q^i - 1$ for some $i \geqslant 1$. Note that by Lemma 2.4.10 we may write $r = di + 1$ for some $d \geqslant 1$.

Suppose that $(G_0, i) \neq (\mathrm{L}_n(q), 1)$ or $(\mathrm{U}_n(q), 2)$. In this case $x \in G_0$. By [9, Lemma 3.1.3], we can write $x = \hat{x}Z$, for some unique $\hat{x}$ of order r in the corresponding matrix group $\widehat{G}$ to G_0, where $\widehat{G} = \mathrm{GL}^\epsilon_n(q)$ if $G_0 = \mathrm{L}^\epsilon_n(q)$, $\mathrm{Sp}_n(q)$ if $G_0 = \mathrm{PSp}_n(q)$, or $\mathrm{O}_n(q)$ if $G = \mathrm{P}\Omega^\epsilon_n(q)$ with n even, or $\Omega_n(q)$ with n odd, and where Z is the centre of $\widehat{G}$. For example, suppose $G_0 = \mathrm{L}_n(q)$ (note that the notation and set up is similar in the other classical groups with slight variations, see [9, Chapter 3]). Recall that $\mathrm{Inndiag}(G_0) = \mathrm{PGL}_n(q)$. Then $\widehat{G} = \mathrm{GL}_n(q)$ and let $\hat{x} \in G$ be an element of order r. Let $T(r)$ denote the set of nontrivial r^{th} roots of unity in $\mathbb{F}_{q^i}$. Then $\hat{x}$ is diagonalisable over $\mathbb{F}_{q^i}$, but not over any proper subfield, so $\hat{x}$ fixes a direct sum decomposition

$$V = U_1 \oplus \cdots \oplus U_s \oplus C_V(\hat{x})$$

by Maschke's Theorem. Here $C_V(\hat{x})$ denotes the 1-eigenspace of $\hat{x}$, and each U_j is an i-dimensional subspace on which $\hat{x}$ acts irreducibly. The set of eigenvalues of $\hat{x}$ on $U_j \otimes \mathbb{F}_{q^i}$ are of the form $\Lambda = \{\lambda, \lambda^q, \ldots, \lambda^{q^{i-1}}\}$ for some $\lambda \in T(r)$; this coincides with an orbit on $T(r)$ under the action of the Frobenius automorphism $\sigma : \mu \longmapsto \mu^q$ of $\mathbb{F}_{q^i}$. There are $t = (r-1)/i$ distinct σ-orbits, which we label as $\Lambda_1, \ldots, \Lambda_t$. We may abuse notation and write

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

where a_j is the multiplicity of Λ_j in the multiset of eigenvalues of $\hat{x}$ on $V \otimes \mathbb{F}_{q^i}$ and $e = \dim C_V(\hat{x})$. Let $\mathcal{I}$ denote the set of non-zero t-tuples $(a_1, \ldots, a_t) \in \mathbb{N}_0^t$ such that $i\sum_j a_j \leqslant n$. The following is [9, Lemma 3.1.7], see also [9, Proposition 3.2.1] (recall we are under the assumption that $c \geqslant 2$).

Lemma 4.1.3. *Let $\hat{x} \in \mathrm{GL}_n(q)$ be a semisimple element of order r. Then $\hat{x}$ is $\mathrm{GL}_n(q)$-conjugate to $[\Lambda_1^{a_1}, \ldots, \Lambda_t^{a_t}, I_e]$ for a unique t-tuple $(a_1, \ldots, a_t) \in \mathcal{I}$, where $e = \dim C_V(\hat{x})$.*

Thus the conjugacy classes of elements of order r in $\mathrm{PGL}_n(q) = \mathrm{Inndiag}(\mathrm{L}_n(q))$ are uniquely determined by the multisets of eigenvalues in $\mathbb{F}_{q^i}$. With suitable changes there are similar descriptions for the other classical groups $\mathrm{GU}_n(q)$, $\mathrm{Sp}_n(q)$ and $\mathrm{O}_n^\epsilon(q)$. For example, in $\mathrm{Sp}_n(q)$ the main difference is that for i odd the Λ_j sets arise in inverse pairs. Thus elements of order r in $\mathrm{PGSp}_n(q)$, when i is odd, have the form $x = [(\Lambda_1, \Lambda_1^{-1})^{a_1}, \ldots, (\Lambda_{t/2}, \Lambda_{t/2}^{-1})^{a_{t/2}}, I_e]Z$, where $\Lambda_j^{-1} = \{\lambda^{-1} \mid \lambda \in \Lambda_j\}$.

Remark 4.1.4. Let us also highlight a special case with $G_0 = \mathrm{U}_n(q)$, which will be useful later. Let $G_0 = \mathrm{U}_n(q)$ and suppose that r is a prime divisor of $|G_0|$ and a primitive prime divisor of $q^i - 1$, where $i \equiv 2 \,(\mathrm{mod}\, 4)$ and $i \geqslant 10$. Set $b = \frac{i}{2}$. Any element $x \in \mathrm{PGU}_n(q)$ of order r is in fact an element of G_0 since $|\mathrm{PGU}_n(q) : G_0| = (n, q+1)$ is indivisible by r. Additionally, x can be written as $x = \hat{x}Z$ where $Z = Z(\mathrm{GU}_n(q))$ and $\hat{x} \in \mathrm{GU}_n(q)$ is of order r. By [9, Proposition 3.3.2], $\hat{x}$ fixes an orthogonal decomposition of V (the natural module) into irreducible summands, U_j, and $C_V(\hat{x})$. Here $C_V(\hat{x})$ is non-degenerate (or trivial) and the irreducible summands are non-degenerate b-spaces on which $\hat{x}$ has eigenvalues

$$\Lambda_j = \{\lambda_j, \lambda_j^{q^2}, \ldots, \lambda_j^{q^{2(b-1)}}\}, \tag{4.1}$$

on $U_j \otimes \mathbb{F}_{q^i}$, for some primitive r^{th} root of unity $\lambda_j \in \mathbb{F}_{q^i}$. We may abuse notation and write $\hat{x} = [\Lambda_1^{a_1}, \ldots, \Lambda_s^{a_s}, I_e]$, where $s = (r-1)/b$, a_j is the multiplicity of Λ_j in the multiset of eigenvalues of $\hat{x}$ on $V \otimes \mathbb{F}_{q^i}$ and $e = \dim C_V(\hat{x})$ (note the Λ_j sets coincide with the σ^2-orbits in $T(r)$, where $\sigma^2 : \mu \longmapsto \mu^{q^2}$). From [9, Proposition 3.3.2], there exists a bijection

$$\theta : (a_1, \ldots, a_s) \longmapsto ([\Lambda_1^{a_1}, \ldots, \Lambda_s^{a_s}, I_e]Z)^{\mathrm{PGU}_n(q)}$$

between the non-zero s-tuples $(a_1, \ldots, a_s) \in \mathbb{N}_0^s$ such that $i\sum_j a_j \leqslant 2n$ and the set of $\mathrm{PGU}_n(q)$-classes of elements of order r in G_0. In addition Theorem 4.1.2 implies that $x^{G_0} = x^{\mathrm{PGU}_n(q)}$ for any element of order r in G_0. We direct the reader to [9, Chapter 3] for more details on conjugacy in all of the classical groups.

Suppose now that $G_0 = \mathrm{L}_n(q)$ and $i = 1$, or $G_0 = \mathrm{U}_n(q)$ and $i = 2$. In this case we still represent elements of prime order r as $x = \hat{x}Z$, with $\hat{x} \in \widehat{G}$, where $\widehat{G} = \mathrm{GL}_n(q)$ when $G_0 = \mathrm{L}_n(q)$, or $\mathrm{GU}_n(q)$ when $G_0 = \mathrm{U}_n(q)$, and Z is the centre of $\widehat{G}$. However in this

case x may not lift to an element of order r in $\widehat{G}$, and extra conjugacy classes of elements of order r exist that are not present in the case $c \geqslant 2$. In both of these cases a similar description of conjugacy is available, see [9, Proposition 3.2.2] and [9, Proposition 3.3.3] respectively.

Semisimple involutions

Assume p is odd and $G = \mathrm{PGL}_n^\epsilon(q), \mathrm{PGSp}_n(q)$ or $\mathrm{PGO}_n^\epsilon(q)$. The conjugacy class representatives of involutions in G are given in [40, Table 4.5.1] and a detailed discussion can be found in [9, Sections 3.2.2, 3.3.2, 3.4.2 and 3.5.2]. Here we will give a brief overview in the case $G = \mathrm{PGL}_n(q)$.

Here the distinct classes of involutions in G are represented by elements labeled t_i for $1 \leqslant i \leqslant n/2$, and $t'_{n/2}$, using the notation from [9, Section 3.2.2], which is consistent with [40, Table 4.5.1]. The elements t_i lift to involutions in $\mathrm{GL}_n(q)$ with i-dimensional (-1)-eigenspaces, while $t'_{n/2}$ lifts to an element of order $2(q-1)_2$. Furthermore, $t_i \in G_0$ if and only if i is even, or i is odd and $(q-1)_2 > (n)_2$. In particular, if n is even then $t_{n/2} \in G_0$ if and only if $n \equiv 0 \pmod 4$ or $q \equiv 1 \pmod 4$, and $t'_{n/2} \in G_0$ if and only if $q \equiv 3 \pmod 4$ or $(n)_2 > (q-1)_2$. See [9, Section 3.2.2] for more details.

4.1.2 Unipotent elements

For $i \geqslant 1$, we use J_i to denote the $i \times i$ standard (lower triangular) Jordan block with eigenvalues 1, and we write J_i^k to denote k copies of J_i. Let $x \in \mathrm{Inndiag}(G_0)$ be an element of order p. By [9, Lemma 3.1.3] we can write $x = \hat{x}Z$, for some unique $\hat{x}$ of order p in the corresponding matrix group $\widehat{G}$ to G_0, where $\widehat{G} = \mathrm{GL}_n^\epsilon(q)$ if $G_0 = \mathrm{L}_n^\epsilon(q)$, $\mathrm{Sp}_n(q)$ if $G_0 = \mathrm{PSp}_n(q)$, or $\mathrm{O}_n(q)$ if $G = \mathrm{P}\Omega_n^\epsilon(q)$ with n even, or $\Omega_n(q)$ with n odd, and where Z is the centre of $\widehat{G}$. Then $\hat{x}$ has Jordan form,

$$\hat{x} = [J_p^{a_p}, \ldots, J_1^{a_1}],$$

a block diagonal matrix with respect to some basis, where a_i is the multiplicity of the standard unipotent Jordan block J_i. Let $\mathcal{P}$ denote the set of nontrivial partitions of n with parts of size at most p. The following result is [9, Lemma 3.1.14].

Lemma 4.1.5. *There is a bijection*

$$\theta : (p^{a_p}, \ldots, 1^{a_1}) \mapsto [J_p^{a_p}, \ldots, J_1^{a_1}]^{\mathrm{GL}_n(q)}$$

from $\mathcal{P}$ to the set of $\mathrm{GL}_n(q)$-classes of elements of order p in $\mathrm{GL}_n(q)$.

Again there is a similar description of the conjugacy classes of unipotent elements in the other classical groups. In the symplectic and orthogonal cases, there are conditions on the multiplicities of the Jordan blocks. A convenient reference for the following lemma is [9, Lemmas 3.4.1 and 3.5.1].

Lemma 4.1.6. *Suppose p is odd and $\hat{x} \in \mathrm{Sp}_n(q)$ or $\mathrm{O}^\epsilon_n(q)$ has Jordan form $[J_p^{a_p}, \dots, J_1^{a_1}]$. If $\hat{x} \in \mathrm{Sp}_n(q)$, then a_i is even for all odd i. Similarly, if $\hat{x} \in \mathrm{O}^\epsilon_n(q)$, then a_i is even for all even i.*

The behaviour of unipotent classes in symplectic and orthogonal groups is more complicated when $p = 2$. Following [2, Section 7], for each $1 \leqslant s \leqslant n/2$ we define elements a_s and c_s if s is even and b_s if s is odd, all of which have Jordan form $[J_2^s, J_1^{n-2s}]$. If n is even, $p = 2$ and $\widehat{G} = \mathrm{Sp}_n(q)$ or $\mathrm{O}^\pm_n(q)$, then each involution has Jordan form $[J_2^s, J_1^{n-2s}]$ and is conjugate to b_s if s is odd, or exactly one of a_s or c_s if s is even. We refer the reader to [9, Sections 3.4.4 and 3.5.4] for more details on these elements.

4.2 The primitive case

Here we prove Theorem 1 when G is a classical group over $\mathbb{F}_q$.

Theorem 4.1. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive permutation group with socle $G_0 \in \mathcal{A}$ and point stabiliser H. Then G is almost elusive if and only if (G, H) is contained in Table P1 or P2.*

For the remainder of this section we may assume that G, G_0 and H are as in Theorem 4.1. First recall that (G, H) is almost elusive only if $\pi(G_0) - \pi(H_0) \leqslant 1$ (see Corollary 2.1.26). Thus in view of Theorem 2.5.1, we may assume for the remainder of this section that either (G_0, H) is a case in Table A1 or A2, or (G_0, H, i) is found in Table A3 and there exists a unique primitive prime divisor r of $q^i - 1$. In the latter case, note that every nontrivial element of order r in G_0 is a derangement (see Lemma 2.1.25).

For certain low dimensional groups over small fields, we can calculate the number of conjugacy classes of derangements of prime order directly using Magma [5]. Let us write an arbitrary group in $\mathcal{A}$ of dimension n over $\mathbb{F}_q$ as $X_n(q)$. We can then define

$\mathcal{D} = \mathcal{D}_1 \cup \mathcal{D}_2 \cup \mathcal{D}_3 \subseteq \mathcal{A}$, where

$$\mathcal{D}_1 = \{X_n(q) \in \mathcal{A} \mid 3 \leqslant n \leqslant 4 \text{ with } q \leqslant 8 \text{ , or } 5 \leqslant n \leqslant 8 \text{ with } q = 2\},$$
$$\mathcal{D}_2 = \{\mathrm{L}_2(q),\, \mathrm{U}_3(q') \mid q \leqslant 49 \text{ and } 9 \leqslant q' \leqslant 19\},$$
$$\mathcal{D}_3 = \{\mathrm{L}_5(3), \mathrm{PSp}_6(3), \Omega_7(3), \mathrm{P}\Omega_8^{\epsilon}(3), \Omega_8^{\epsilon}(4), \Omega_{10}^{\epsilon}(2), \Omega_{12}^{\epsilon}(2)\}.$$

The almost simple groups with socle in $\mathcal{D}$ can be handled in Magma. In particular, this covers most cases in Tables A1 and A2.

Proposition 4.2.1. *Theorem 4.1 holds for $G_0 \in \mathcal{D}$.*

Proof. This is a straightforward Magma [5] calculation. For each $G_0 \in \mathcal{D}$ we use the command `AutomorphismGroupSimpleGroup` to obtain $\mathrm{Aut}(G_0)$ as a permutation group. Then using `LowIndexSubgroups` we obtain all almost simple groups with socle G_0. For each group, we call `MaximalSubgroups` and we can easily identify the type of each maximal subgroup by its order or structure. Then for each group G and each maximal subgroup H of G we use `IsConjugate` to determine the fusion of H-classes of prime order in G. Finally, we use the fact that there is a unique G-class of elements of prime order that does not intersect H if and only if G is almost elusive. □

It now remains to deal with Cases XII, XIII, XVII-XX and XXII in Table A1, Cases I-V in Table A2 and all the remaining cases in Table A3.

Aschbacher's theorem (see Theorem 2.3.6) provides a framework for the proof. The subspace subgroups comprising the $\mathcal{C}_1$ collection require special attention. These are relatively large subgroups so finding prime order derangements can be more challenging. Before beginning the proof, we provide some preliminary lemmas that will be useful for both non-subspace and subspace subgroups. We remind the reader that our notation for elements of classical groups was set up in Section 4.1. The following two lemmas are special cases of [9, Lemma 4.2.4].

Lemma 4.2.2. *Suppose $G_0 \in \{\mathrm{PSp}_n(q), \mathrm{P}\Omega_n^{\epsilon}(q)\}$, where $n \equiv 0 \pmod 4$. Let r be a primitive prime divisor of $q^{n/2} - 1$ and let $x = \hat{x}Z \in G_0$ be an element of order r such that $\hat{x} = [\Lambda, I_{n/2}]$. Then x does not fix a totally singular $n/2$-space.*

Lemma 4.2.3. *Suppose $G_0 = \mathrm{U}_n(q)$, where $n \geqslant 6$ is even and $n \not\equiv 0 \pmod 8$. Let r be a primitive prime divisor of $q^i - 1$, where $i = n/2$ if $n \equiv 4 \pmod 8$, and $i = n$ if $n \equiv \pm 2$*

(mod 8). *Let $x = \hat{x}Z \in G_0$ be an element of order r such that*

$$\hat{x} = \begin{cases} [\Lambda_1^3, \Lambda_2] & \text{if } n \equiv 4 \pmod 8 \\ [\Lambda_1, \Lambda_2] & \text{if } n \equiv \pm 2 \pmod 8 \end{cases}, \tag{4.2}$$

where $\Lambda_1 \neq \Lambda_2$. Then x does not fix a totally singular $n/2$-space.

4.2.1 Non-subspace subgroups

In this section we prove Theorem 1 when the maximal subgroup H is either contained in one of the geometric collections $\mathcal{C}_2, \ldots, \mathcal{C}_8$, or is contained in one of the collections denoted $\mathcal{N}$ and $\mathcal{S}$ (see Section 2.3.2 for more details on these subgroup collections). We begin the proof by immediately handling some of the cases with symplectic socle in Table A3. The remainder of the proof is organised by the various non-subspace subgroup collections. We begin by handling the $\mathcal{C}_2$, $\mathcal{C}_3$, $\mathcal{C}_5$ and $\mathcal{C}_8$ collections in turn. Note that out of the cases left to handle there are none in which H in contained in the $\mathcal{C}_4$, $\mathcal{C}_6$ or $\mathcal{C}_7$ collections. We then finally handle the $\mathcal{N}$ and $\mathcal{S}$ collections.

First we state a helpful lemma in order to handle the symplectic cases S4, S5, S7, S10 and S11 in Table A3. We remind the reader that for positive integers a and n, P_a^n is the set of primitive prime divisors of $a^n - 1$.

Lemma 4.2.4. *Let $G_0 = \mathrm{PSp}_n(q)$ such that $n \in \{4, 6\}$ and suppose $P_q^4 = \{r\}$. Then either G_0 contains at least two G-classes of elements of order r, or one of the following holds:*

(i) $(n, q) = (4, 3), (4, 7), (6, 2), (6, 3), (6, 7)$ *and* $r = 5$.

(ii) $(n, q) = (4, 4)$, $G = \mathrm{Aut}(G_0)$ *and* $r = 17$.

Proof. Here any element $x = \hat{x}Z \in G_0$ of order r is of the form $\hat{x} = [\Lambda]$ if $n = 4$, and $\hat{x} = [\Lambda, I_2]$ if $n = 6$ (see Section 4.1 and [9, Section 3.4]). Since r is the unique primitive prime divisor of $q^4 - 1$, by Lemma 2.4.11 it is also the unique primitive prime divisor of $p^{4f} - 1$, so $r = 4fd + 1$ for some $d \geqslant 1$. Therefore G_0 contains $(r-1)/4 = fd$ distinct $\mathrm{PGSp}_n(q)$-classes of elements of order r (see [9, Proposition 3.4.3]). Since $|\mathrm{Aut}(G_0) : \mathrm{PGSp}_n(q)| = kf$, where $k = 2$ if $(n, p) = (4, 2)$ and 1 otherwise, it follows by Lemma 4.1.1 that there are at least $(r-1)/4kf \geqslant d/2$ distinct G-classes of elements of order r in G_0.

By Lemma 2.4.15, either $d \geqslant 4$ or $(d, q) = (3, 5), (3, 239), (2, 4), (1, 2), (1, 3)$ or $(1, 7)$. If $d \geqslant 3$, then by the argument above there are at least 2 distinct G-classes in G_0 of elements

of order r. In the remaining cases we have $q \in \{2, 3, 4, 7\}$ and the result is easily checked using Magma [5]. □

With this result in hand, we can immediately deal with a large number of the cases with symplectic socle in Table A3.

Proposition 4.2.5. *Theorem 4.1 holds for Cases* S4, S5, S7, S10 *and* S11 *in Table A3.*

Proof. In all of these cases we have $G_0 = \mathrm{PSp}_n(q)$ with $n = 4$ or 6. Additionally we are assuming that there exists a unique primitive prime divisor of $q^4 - 1$, say r, which is the unique prime dividing $|G_0|$ and not $|H_0|$. Note if $n = 6$ we are in case S10 and $q \geqslant 4$ is even. And if $n = 4$ then we can assume $q \geqslant 9$ by Proposition 4.2.1. So Lemma 4.2.4 implies that G contains at least two conjugacy classes of derangements of order r and thus G is not almost elusive. □

We organise the remainder of the proof according to Aschbacher's theorem.

Notation 4.2.6. If (G_0, H, i) is a case in Table A3, then we use r_i to denote the unique primitive prime divisor of $q^i - 1$.

We remind the reader that if (G_0, H, i) is found in Table A3, then Lemma 2.1.25 implies that every element of order r_i in G_0 is a derangement.

$\mathcal{C}_2$ subgroups

Proposition 4.2.7. *Theorem 4.1 holds for Case* II *in Table A2.*

Proof. Here $G_0 = \mathrm{L}_2(q)$ with $q = p = 2^k - 1$ and H is of type $\mathrm{GL}_1(q) \wr S_2$, that is $H_0 = D_{q-1}$. We note that the only prime dividing $|G_0|$ that does not divide $|H_0|$ is p. First assume that $G = G_0$. Then G contains two distinct conjugacy classes of elements of order p (see [9, Proposition 3.2.7]). Thus G is not almost elusive. Finally assume that $G = \mathrm{PGL}_2(p)$. Then there is a unique class of elements of order p. Since $|\Omega| = 2^{k-1}p$ the only other possible prime for prime order derangements must be 2. However both classes of involutions in G have fixed points. Indeed, since $q \equiv 3 \pmod 4$ it follows that the involutions in H_0 are of type t_1', while the involution in the center of $H = D_{2(q-1)}$ is of type t_1 (see Section 4.1.1). It follows that $\mathrm{PGL}_2(p)$ is almost elusive. □

Proposition 4.2.8. *Theorem 4.1 holds for Case* L4 *in Table A3.*

Proof. Here $(G_0, i) = (\mathrm{L}_2(q), 2)$ with $q = 2^f$ and H is of type $\mathrm{GL}_1(q) \wr S_2$, that is $H_0 = D_{q-1}$. Since there exists a unique primitive prime divisor, r, of $q^2 - 1$ we may assume that $q + 1 = r^b$ for some $b \geqslant 1$. Thus Lemma 2.4.1 implies that either $q = 8$ or $b = 1$, f is a 2-power and $q + 1$ is a Fermat prime. In view of Proposition 4.2.1 we can assume we are in the latter situation with $f = 2^m$ and $m \geqslant 3$. Here, by Lemma 4.1.1, G has at least $q/2f \geqslant 2$ conjugacy classes of elements of order r, whence G is not almost elusive. □

We remind the reader that we use V to denote the natural G_0-module.

Proposition 4.2.9. *Theorem 4.1 holds for Case* U4 *in Table A3.*

Proof. Here $(G_0, i) = (\mathrm{U}_n(q), 2n - 2)$ with $n = 4$ or 6, and H is the stabiliser in G of a decomposition $V = V_1 \oplus V_2$, where the V_j are both maximal totally singular spaces of dimension $n/2$. In this case we recall that every element of order r_{2n-2} in G_0 is a derangement.

Suppose first that $n = 6$. By Proposition 4.2.1 we may assume $q \geqslant 3$. Take s to be a primitive prime divisor of $q^6 - 1$ and let $x = \hat{x}Z \in G_0$ be an element of order s where $\hat{x}$ is defined as in (4.2). Then x does not fix V_1 or V_2 by Lemma 4.2.3 and does not interchange V_1 and V_2 since $|x| = s > 2$. Thus x is a derangement of order $s \neq r_{10}$, so G is not almost elusive.

Finally suppose $n = 4$. In this case, by Proposition 4.2.1, we may assume $q \geqslant 9$. Take $x = \hat{x}Z \in G_0$ to be a unipotent element of order p. By definition of H, if x interchanges V_1 and V_2, then $p = 2$ and x has Jordan form $[J_2^2]$ on V. Similarly if x fixes both V_1 and V_2 then by [9][Lemma 2.2.17] each Jordan block in the Jordan form of x on V has even multiplicity. Thus we conclude that any element in G_0 with Jordan form $[J_2, J_1^2]$ is a derangement. Therefore G contains derangements of order r_6 and p, thus G is not almost elusive. □

Proposition 4.2.10. *Theorem 4.1 holds for Case* O8 *in Table A3.*

Proof. In this case $(G_0, i) = (\mathrm{P}\Omega_8^+(q), 6)$, and H is the stabiliser in G of a decomposition $V = V_1 \oplus V_2$, where the V_j are both maximal totally singular spaces of dimension 4.

Take s to be a primitive prime divisor of $q^4 - 1$. Let $x = \hat{x}Z \in G_0$ be an element of order s where $\hat{x} = [\Lambda, I_{n/2}]$. Then x does not fix V_1 or V_2 by Lemma 4.2.2, and does not interchange V_1 and V_2 since $|x| = s > 2$. Thus x is a derangement. It follows that G contains derangements of order r_6 and s, so is not almost elusive. □

$\mathcal{C}_3$ subgroups

For the following lemma we recall that V denotes the natural G_0-module.

Lemma 4.2.11. *Let $H \in \mathcal{C}_3$ be a subgroup arising from a field extension of prime degree k. Let $x \in H_0$ be an element of order p. Then either;*

(i) *x has Jordan form $[J_p^{ka_p}, \dots, J_1^{ka_1}]$ on V; or*

(ii) *$k = p$ and x has Jordan form $[J_k^{n/k}]$ on V.*

Proof. This follows by applying Lemmas 5.3.2 and 5.3.11 in [9]. □

Proposition 4.2.12. *Theorem 4.1 holds for Case* III *and* IV *in Table A2.*

Proof. In these cases $G_0 = \mathrm{L}_2(q)$ where $q = p = 2^k + 1$ in Case III and $q = 2^f$ such that $q - 1 = r$ is prime in Case IV, and H is of type $\mathrm{GL}_1(q^2)$. That is $H_0 = D_{q+1}$ and $|\Omega| = \frac{1}{2}q(q-1)$. First suppose we are as in Case IV. Then $q = 2^f$ such that $f \geqslant 7$ is a prime (the cases $f = 3$ and 5 were handled in Proposition 4.2.1). Note that r divides $|G|$ but not $|H|$ and so every nontrivial element of order r in G is a derangement. Since G contains at least $(r-1)/2f \geqslant 2$ distinct classes of such elements, we conclude that G is not almost elusive.

Finally let us suppose we are as in Case III. Note that every element in G_0 of order p is a derangement (since p divides $|G_0|$ and not $|H_0|$). If $G = G_0$ then G has two classes of elements of order p, 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 p. The involutions in $H_0 = D_{q+1}$ are of type t_1 (note that $q \equiv 1 \pmod 4$), 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 4.2.13. *Theorem 4.1 holds for Cases* L5 *and* S6 *in Table A3.*

Proof. In both cases we know that G_0 contains derangements of order r_i. By Lemma 4.2.11 any element in G_0 of order p with Jordan form $[J_2, J_1^{n-2}]$ on V is also a derangement. Thus G_0 contains derangements of order p and r_i, so G is not almost elusive. □

Proposition 4.2.14. *Theorem 4.1 holds for Case* O9 *in Table A3.*

Proof. Here $(G_0, i) = (\mathrm{P}\Omega_8^+(q), 3)$ and H of type $\mathrm{GU}_4(q)$. Assume first that $p \neq 2$. Then any element in G_0 of order p with Jordan form $[J_3, J_1^5]$ on V is a derangement by

Lemma 4.2.11. Thus G_0 contains semisimple and unipotent derangements, so G is not almost elusive. Finally assume $p = 2$. Note that $H_0 = C_{q+1}.\mathrm{PGU}_4(q).\langle\psi\rangle$, where ψ is an involutory graph automorphism of $\mathrm{U}_4(q)$ arising from an involutory field automorphism of $\mathbb{F}_{q^2}$ (see [9, Lemma 5.3.6]). If $x \in H_0$ is an involution with Jordan form $[J_2^2, J_1^4]$ on V, then x has Jordan form $[J_2, J_1^2]$ on the natural $\mathrm{U}_4(q)$-module. In G_0 there are precisely two G_0-classes of involutions with Jordan form $[J_2^2, J_1^4]$ on V (these are represented by the elements a_2 and c_2; see [9, Section 3.5.4] for more details). However there is a unique class of involutions in H_0 with Jordan form $[J_2, J_1^2]$ on the natural $\mathrm{U}_4(q)$-module (see [9, Proposition 3.3.7]), so we conclude that G_0 must contain derangements of order $p = 2$. Thus G is not almost elusive. □

Proposition 4.2.15. *Theorem 4.1 holds for Case* XII *in Table A1.*

Proof. Here $G_0 = \mathrm{PSp}_4(q)$ and H is of type $\mathrm{Sp}_2(q^2)$, so $H_0 = \mathrm{PSp}_2(q^2).2$ (see [54, Proposition 4.3.10]). Note we may assume $q \geqslant 9$ by Proposition 4.2.1. From Lemma 4.2.11 any element in G_0 of order p with Jordan form $[J_2, J_1^2]$ is a derangement. Take r to be a primitive prime divisor of $q^i - 1$ where $i = 1$ if q is a Mersenne prime and $i = 2$ otherwise (note r always exists by Lemma 2.4.1 and Zsigmondy's theorem). Let $x = \hat{x}Z \in G_0$ be an element of order r such that

$$\hat{x} := \begin{cases} [\Lambda, I_2] & i = 2 \\ [\Lambda, \Lambda^{-1}, I_2] & i = 1 \end{cases}.$$

Then [9, Lemma 5.3.2] implies that any element of order r in H_0 must have a trivial one-eigenspace, implying that x is a derangement. Therefore the result holds. □

$\mathcal{C}_5$ subgroups

Proposition 4.2.16. *Theorem 4.1 holds for Case* L6 *in Table A3.*

Proof. In this case $(G_0, i) = (\mathrm{L}_2(q), 2)$ and H is of type $\mathrm{GL}_2(q_0)$, where $q = q_0^2$. Therefore $H_0 = \mathrm{PGL}_2(q_0)$ and $|\Omega| = \frac{1}{d}q_0(q+1)$, where $d = (2, q-1)$. We recall that r_2 is the unique primitive prime divisor of $q^2 - 1$, so $q + 1 = r_2^b$ for some $b \geqslant 1$. Suppose q is odd. 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 [6, 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 suppose $q = 2^f$ is even. Since f is even, Lemma 2.4.1 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 4.2.17. *Theorem 4.1 holds for Case* U5 *in Table A3.*

Proof. Here $(G_0, i) = (\mathrm{U}_n(q), 2n-2)$ with $n = 4$ or 6, and H is of type $\mathrm{Sp}_n(q)$. Note that by Proposition 4.2.1 we can assume $q \geqslant 9$ when $n = 4$ and $q \geqslant 3$ when $n = 6$.

Assume $p \geqslant 3$ and take $x \in G_0$ to be an element of order p with Jordan form $[J_3, J_1^{n-3}]$, then $x \notin H_0$ (recall all odd sized Jordan blocks must have even multiplicity, see Lemma 4.1.6). Thus for $p \geqslant 3$ we are done.

Now assume $p = 2$. Suppose $n = 6$ and take s to be a primitive prime divisor of $q^6 - 1$. Take $x = \hat{x}Z \in G_0$ to be an element of order s, such that $\hat{x} = [\Lambda, I_3]$. Then $x \notin H$ since $\Lambda \neq \Lambda^{-1} = \{\lambda^{-1} \mid \lambda \in \Lambda\}$ (see [9, Proposition 3.4.3]), so x is a derangement. Similarly suppose $n = 4$ and take s to be a primitive prime divisor of $q^2 - 1$. Let $x = \hat{x}Z \in \mathrm{PGU}_4(q)$ be an element of order s such that $\hat{x} = [\lambda I_1, I_3]$. Then by the same reasoning as for the $n = 6$ case, x is a derangement, and $x \in G_0$ since $(4, s) = 1$ (see [9, Proposition 3.3.3]). Thus G is not almost elusive. □

Proposition 4.2.18. *Theorem 4.1 holds for Case* U6 *in Table A3.*

Proof. In this case $(G_0, i) = (\mathrm{U}_4(q), 6)$ and H is of type $\mathrm{O}_4^-(q)$ with q odd. Take $x \in G_0$ to be an element of order p with Jordan form $[J_2, J_1^{n-2}]$. Then x is a derangement (recall all even sized blocks in the Jordan form of a unipotent element in H_0 must have even multiplicity, see Lemma 4.1.6). Thus G is not almost elusive, since G_0 contains derangements of order p and r_6 (the unique primitive prime divisor of $q^6 - 1$). □

Proposition 4.2.19. *Theorem 4.1 holds for Case* U7 *in Table A3.*

Proof. In this case $(G_0, i) = (\mathrm{U}_3(q), 6)$ and H is of type $\mathrm{O}_3(q)$ with q odd. By Lemma 2.4.15 we see that $r_6 \geqslant 12f + 1$ and we note that G_0 contains $(r_6 - 1)/3 \geqslant 4f$ distinct $\mathrm{PGU}_3(q)$-classes of such elements (see [9, Proposition 3.3.2]). Since $|\mathrm{Aut}(G_0) : \mathrm{PGU}_3(q)| = 2f$ it follows, by Lemma 4.1.1, that there are at least $(r_6 - 1)/6f \geqslant 2$ such classes in G and we conclude that G is not almost elusive. □

Proposition 4.2.20. *Theorem 4.1 holds for Case* O10 *in Table A3.*

Proof. Here $(G_0, i) = (\mathrm{P}\Omega_8^+(q), 6)$ and H is of type $\mathrm{O}_8^-(q_0)$, where $q = q_0^2$. Take s to be a primitive prime divisor of $q_0^8 - 1$ and note that s is also a primitive prime divisor of $q^4 - 1$.

Let $x = \hat{x}Z \in G_0$ be an element of order s such that $\hat{x} = [\Lambda, I_4]$. By [9, Proposition 3.5.4] any element $y = \hat{y}Z' \in H_0$ of order s must have the form $\hat{y} = [\Lambda']$, where $Z' = Z(\mathrm{O}_8^-(q_0))$, $\Lambda' = \{\lambda, \lambda^{q_0}, \ldots, \lambda^{q_0^7}\}$ and λ is some nontrivial s^{th} root of unity in $\mathbb{F}_{q^4}$. Thus $x \notin H_0$ since it has a 4-dimensional 1-eigenspace, so x is a derangement. Thus G_0 contains derangements of distinct prime order, implying that G is not almost elusive. □

$\mathcal{C}_8$ subgroups

Proposition 4.2.21. *Theorem 4.1 holds for Case* L7 *in Table A3.*

Proof. Here $(G_0, i) = (\mathrm{L}_n(q), n-1)$ with H of type $\mathrm{Sp}_n(q)$ and $n = 4$ or 6. Assume first that $p \geqslant 3$ and let $x \in G_0$ be an element of order p with Jordan form $[J_3, J_1^{n-3}]$. Then x is a derangement since all odd sized blocks in symplectic groups must have even multiplicity (see Lemma 4.1.6). Thus for the remainder of the proof we may assume that $p = 2$. By Proposition 4.2.1 we may assume that $q \geqslant 16$ when $n = 4$, and $q \geqslant 4$ when $n = 6$. Thus $r_{n-1} \geqslant 4(n-1)f + 1$ by Lemmas 2.4.15 and 2.4.18. In the usual manner G_0 contains $(r_{n-1}-1)/(n-1) = 4f$ distinct $\mathrm{PGL}_n(q)$-classes of elements of order r_{n-1}. Since $|\mathrm{Aut}(G_0) : \mathrm{PGL}_n(q)| = 2f$, there are at least 2 distinct G-classes of elements of order r_{n-1} in G_0. □

Proposition 4.2.22. *Theorem 4.1 holds for Case* L8 *in Table A3.*

Proof. Here $(G_0, i) = (\mathrm{L}_n(q), 3)$ and H is of type $\mathrm{O}_n^\epsilon(q)$ such that $(\epsilon, n) = (\circ, 3), (-, 4)$ and q is odd. Take $x \in G_0$ to be a unipotent element with Jordan form $[J_2, J_1^{n-2}]$. Then x is a derangement (since in orthogonal groups even sized Jordan blocks must have even multiplicity). Thus G_0 contains unipotent and semisimple derangements, so G is not almost elusive. □

Proposition 4.2.23. *Theorem 4.1 holds for Cases* S8 *and* S9 *in Table A3 and Case* XIII *in Table A1.*

Proof. Here $G_0 = \mathrm{PSp}_n(q)$ with q even and H is of type $\mathrm{O}_n^\epsilon(q)$ (recall $n \geqslant 4$ since $G_0 \in \mathcal{A}$). The cases $\epsilon = +$ and $\epsilon = -$ are similar, so we only provide details for the $\epsilon = +$ case.

Assume $\epsilon = +$. Take s to be an odd prime divisor of $q^{n/2} + 1$ and let j be such that s is a primitive prime divisor of $q^j - 1$. Then j divides n and does not divide $n/2$, implying j is even and n/j is odd. Let $x = \hat{x}Z \in G_0$ be an element of order s such that $\hat{x} = [\Lambda^{n/j}] \in \mathrm{Sp}_n(q)$, then by [9, Remark 3.5.5] $x \notin \mathrm{O}_n^+(q)$, so is a derangement. Thus we

may assume that $q^{n/2}+1 = s^l$ for some $l \geqslant 1$. By Lemma 2.4.1 this occurs if and only if one of the following holds;

(i) $(n,q) = (6,2)$

(ii) $fn = 2^m$ with $m \geqslant 2$, and s is a Fermat prime.

The case (i) was handled in Proposition 4.2.1 thus we may assume that (n,q) is as in Case (ii). Here $s = 2^{fn/2}+1$ and G_0 contains $(s-1)/n$ distinct $\mathrm{PGSp}_n(q)$-classes of elements of order s (see [9, Section 3.4.1]). Since $|\mathrm{Aut}(G_0) : \mathrm{PGSp}_n(q)| = af$ where $a = 2$ when $n = 4$ and $a = 1$ otherwise (see [9, Section 2.4]), there are at least $c := (s-1)/afn$ distinct G-classes of elements of order s in G_0. It is straightforward to see that $c = 2^{fn/2}/afn \geqslant 2$ for $(n,q) \neq (4,2),(4,4)$. Thus G is not almost elusive when $(n,q) \neq (4,2),(4,4)$. The remaining cases $(n,q) = (4,2),(4,4)$ have been handled already in Proposition 4.2.1. □

We have now handled the cases in which H is contained in one of the Aschbacher collections $\mathcal{C}_2,\ldots,\mathcal{C}_8$. Thus to complete the proof of Theorem 4.1 for $H \notin \mathcal{C}_1$ it remains for us to handle the remaining subgroups in $\mathcal{N}$ (the novelty subgroups) and $\mathcal{S}$ (the non-geometric subgroups). That is Cases XIX and XX in Table A1, Case V in Table A2 and Cases O11 and O20 in Table A3 (recall that Cases S10 and S11 have been handled already in Proposition 4.2.5).

Novelty subgroups

Proposition 4.2.24. *Theorem 4.1 holds for Case* O11 *in Table A3.*

Proof. In this case $(G_0,i) = (\mathrm{P}\Omega_8^+(q),4)$ and $H_0 = H \cap G_0 = G_2(q)$. By [53, Proposition 3.1.1 (vi)] every element of H_0 fixes a nonsingular 1-space (a reducible subgroup of type $\mathrm{O}_7(q)$). Thus any element in G_0 that does not fix a nonsingular 1-space is a derangement. Therefore G is not almost elusive by Propositions 4.2.48 and 4.2.49. □

We note that the proofs of Propositions 4.2.48 and 4.2.49 are given in Section 4.2.2.

Non-geometric subgroups

Here we handle the remaining subgroups $H \in \mathcal{S}$. We recall that here *type of* H refers to the socle of H. We will use S to denote the type of H, that is $S = \mathrm{Soc}(H)$.

Proposition 4.2.25. *Theorem 4.1 holds for Cases* V *in Table A2.*

Proof. Here $G_0 = \mathrm{L}_2(p)$ with $H_0 = A_5$ and $p \geqslant 7$. 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 [6, 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. □

Proposition 4.2.26. *Theorem 4.1 holds for Cases* XIX *and* XX *in Table A1.*

Proof. Here $G_0 = \mathrm{P}\Omega_8^+(q)$ and $S = H_0 = \Omega_7(q)$ if q is odd or $S = H_0 = \mathrm{Sp}_6(q)$ if q is even. By [53, Proposition 2.2.4] there exists a triality graph automorphism τ of G_0 such that H_0^τ is a $\mathcal{C}_1$ subgroup of type $\mathrm{O}_1(q) \perp \mathrm{O}_7(q)$ when q is odd and $\mathrm{Sp}_6(q)$ (a stabiliser in G_0 of a nonsingular 1-space) if q is even. Then, again G is shown to be not almost elusive in Propositions 4.2.48 and 4.2.49. □

Proposition 4.2.27. *Theorem 4.1 holds for Case* O20 *in Table A3.*

Proof. Here $(G_0, i) = (\Omega_7(q), 4)$ and $S = G_2(q)$. By Proposition 4.2.1 we may assume that $q \geqslant 5$. Since r_4 is the unique primitive prime divisor of $q^4 - 1$, by Lemma 2.4.15 we may assume that either $q = 7$ and $r_4 = 5$, or $r_4 \geqslant 12f + 1$. Assume first that $r_4 \geqslant 12f + 1$. Then G_0 contains $(r_4 - 1)/4 \geqslant 3f$ distinct $\mathrm{PGO}_7(q)$-classes of derangements of order r_4. Additionally since $|\operatorname{Aut}(G_0) : \mathrm{PGO}_7(q)| = f$ we have that G_0 contains at least $(r_4 - 1)/4f \geqslant 3$ distinct G-classes of derangements of order r_4 and so the result follows. Finally assume $q = 7$. It is straightforward to check using Magma that there are three conjugacy classes of semisimple involutions in G_0, and that there is a unique class of involutions in $G_2(q)$. Therefore we conclude that G_0 contains derangements of order 2 and r_4, so the result follows. □

In view of all the propositions proved in this section and Proposition 4.2.1 we have shown the following;

Proposition 4.2.28. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive permutation group with classical socle $G_0 \in \mathcal{A}$ and point stabiliser $H \notin \mathcal{C}_1$. Then G is almost elusive if and only if (G, H) is a case recorded in Table P1 or P2 with $H \notin \mathcal{C}_1$.*

4.2.2 Subspace subgroups

Here we complete the proof of Theorem 4.1 by handling the cases when H is a subspace subgroup, that is H is contained in the $\mathcal{C}_1$ Aschbacher subgroup collection. Once again we recall that when (G_0, H, i) is a case in Table A3 we are assuming there exists a unique primitive prime divisor r_i of $q^i - 1$, and any element in G_0 of order r_i is a derangement.

Symplectic groups

The remaining cases with $G_0 = \mathrm{PSp}_n(q)$ are the following cases in Table A3;

(a) Case S1: H is of type P_1 and $i = n$ with $n \equiv 0 \pmod 4$;

(b) Case S2: H is of type P_2 and $i = n$ with $n = 4$;

(c) Case S3: H is of type $\mathrm{Sp}_2(q) \perp \mathrm{Sp}_{n-2}(q)$ and $i = n$ with $n \equiv 0 \pmod 4$.

Proposition 4.2.29. *Theorem 4.1 holds for Cases* S1*,* S2 *and* S3 *in Table A3 with* $n = 4$.

Proof. By Proposition 4.2.1 we may assume that $q \geqslant 9$, so either $q = 239$ and $r_4 = 13$, or $r_4 \geqslant 16f + 1$ by Lemma 2.4.15. First suppose that $r_4 \geqslant 16f + 1$. Then there are $(r_4 - 1)/4 \geqslant 4f$ distinct $\mathrm{PGSp}_4(q)$-classes of derangements of order r_4 in G_0 (see [9, Proposition 3.4.3]). It follows that there are at least $(r_4 - 1)/8f \geqslant 2$ distinct G-classes of derangements of order r_4 in G_0 since $|\operatorname{Aut}(G_0) : \mathrm{PGSp}_4(q)| \leqslant 2f$.

Finally suppose that $q = 239$. Then by a similar argument to before (noting that in this case $|\operatorname{Aut}(G_0) : \mathrm{PGSp}_4(q)| = f = 1$) we conclude that there are at least $(r_4 - 1)/4 = 3$ distinct G-classes of derangements of order $r_4 = 13$ in G_0, so G is not almost elusive. □

Proposition 4.2.30. *Theorem 4.1 holds for Cases* S1 *and* S3 *in Table A3 with* $n \geqslant 8$.

Proof. Assume first $(n, q) \neq (12, 2)$ and take s to be a primitive prime divisor of $q^{n/2} - 1$. Let $x = \hat{x}Z \in G_0$ be an element of order s such that $\hat{x} = [\Lambda^2]$. Since $\dim C_V(\hat{x}) = 0$ and $|\Lambda| = n/2$, x does not fix a 1-space or a 2-space and thus is a derangement. Therefore G contains derangements of order s and r_n (the unique primitive prime divisor of $q^n - 1$).

For the final case $(n, q) = (12, 2)$ it is easy to see that elements in G_0 of order 13 of the form $[\Lambda]Z$ are derangements. Similarly elements $[\Lambda^3]Z \in G_0$ of order 5 are also derangements. □

Linear groups

Before we handle the remaining linear group cases we first provide a result on the number of conjugacy classes of elements of certain orders in $G_0 = \mathrm{L}_n(q)$ for $n \geqslant 3$. In the following lemma we let $K_{G_0}(G, r)$ denote the number of G-classes of elements of order r in G_0 and ϕ denotes a field automorphism of $\mathrm{L}_n(q)$ of order f.

Lemma 4.2.31. *Let* $G_0 = \mathrm{L}_n(q)$ *where* $q = p^f$ *and* $n \geqslant 3$*. Suppose* r *is a primitive prime divisor of* $p^{fn} - 1$ *such that* $r = knf + 1$ *for some positive integer* k*. Then if*

$G \leqslant \langle \mathrm{PGL}_n(q), \phi \rangle$ then $K_{G_0}(G, r) \geqslant k$. In particular, $K_{G_0}(G, r) \geqslant k/2$ for any group $G \leqslant \mathrm{Aut}(G_0)$.

Proof. By Lemma 2.4.11 we know that r is also a primitive prime divisor of $q^n - 1$, so any element in G_0 of order r must have the form $x = [\Lambda]Z$ (see Section 4.1). Thus by [9, Proposition 3.2.1], G_0 contains $(r-1)/n = kf$ distinct $\mathrm{PGL}_n(q)$-classes of elements of order r since $n \geqslant 3$. Note that $|\mathrm{Aut}(G_0) : \mathrm{PGL}_n(q)| = 2f$ and $|\langle \mathrm{PGL}_n(q), \phi \rangle : \mathrm{PGL}_n(q)| = f$, so the result follows by Lemma 4.1.1. □

The remaining cases left to handle with $G_0 = \mathrm{L}_n(q)$ are case I in Table A2 and the following cases found in Table A3;

(a) Case L1: H is of type P_1 and $i = n$;

(b) Case L2: H is of type $\mathrm{GL}_1(q) \oplus \mathrm{GL}_{n-1}(q)$ and $i = n$;

(c) Case L3: H is of type $P_{1,n-1}$ and $i = n = 3$ and $q = p$ is a Mersenne prime.

We note that in Case L2 the maximality of H implies that $n \geqslant 3$.

Proposition 4.2.32. *Theorem 4.1 holds for Case* L3 *in Table A3.*

Proof. Here by assumption $q = p$ is a Mersenne prime, so $r_3 \geqslant 13 = 4nf + 1$ by Lemma 2.4.15. Therefore G_0 contains at least 2 distinct G-classes of derangements of order r_3 by Lemma 4.2.31, so G is not almost elusive. □

Proposition 4.2.33. *The conclusion to Theorem 4.1 holds for Case* I *in Table A2 and for Case* L1 *in Table A3 with $n = 2$.*

Proof. Here $H_0 = (C_p)^f{:}C_{(q-1)/d}$ and $|\Omega| = q+1$, where $d = (2, q-1)$. We may identify Ω with the set of 1-dimensional subspaces of the natural module V. Additionally we recall that by Proposition 4.2.1 we may assume $q > 49$. Let us first assume we are in Case I in Table A2. Here $q = 2^k - 1$ is a Mersenne prime, that is $q + 1 = 2^k$, and every involution in G_0 is a derangement. Since q is prime $G = G_0$ or $\mathrm{PGL}_2(q)$ and $|\Omega| = 2^k$. We note that each involution in G_0 is of type t_1' (since $q \equiv 3 \pmod 4$) (see Section 4.1.1). 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 assume that we are in Case L1 in Table A3 with $n = 2$. Here there exists a unique primitive prime divisor r of $q^2 - 1$. Therefore here we are assuming $q+1 = 2^a r^b$ for some $a \geqslant 0$ and $b \geqslant 1$ and we note that every element in G_0 of order r is a derangement.

First suppose that $a = 0$, then $q + 1 = r^b$. By Lemma 2.4.1 (recalling that $q > 49$), $b = 1$ and r is a Fermat prime (in which case, $q = 2^f$ and $f \geqslant 6$ is a 2-power). Then 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.

Next suppose that $a \geqslant 2$. Then $q \equiv 3 \pmod 4$ and we note that the involutions in G_0 (which are of type t_1') are derangements.

Finally suppose that $a = 1$ so $q + 1 = 2.r^b$. If $\mathrm{PGL}_2(q) \leqslant G$, then G contains involutions of type t_1' and these elements are derangements. So we may assume that $G \cap \mathrm{PGL}_2(q) = G_0$. Additionally we note that the involutions in G_0 are t_1-type involutions (since $q \equiv 1 \pmod 4$) and these visibly fix a 1-space. By Theorem 2.4.9 there exists a primitive prime divisor s of $p^{2f} - 1$ and by applying Lemma 2.4.11 we get that $r = s$, $f = 2^m \geqslant 1$ is a 2-power and $r = 2fd + 1$ for some $d \geqslant 1$. If $r > 2f + 1$ then G has at least $(r-1)/2f \geqslant 2$ distinct conjugacy classes of such elements, so G is not almost elusive. Thus we may assume $r = 2f + 1$. If $f = 1$ then $r = 3$ and $G = \mathrm{L}_2(p)$ is almost elusive since it contains a unique class of elements of order 3, so let us assume for the remainder of the proof that $f \geqslant 2$. Let $x = p^{f/2}$ (noting that $f \geqslant 2$ is a power of 2). Then the equation $q + 1 = 2.r^b$ becomes

$$x^2 + 1 = 2.r^b. \tag{4.3}$$

By Theorem 2.4.14 for $b > 2$ there are no solutions to (4.3) such that r is a Fermat prime. Thus we may assume that $b \in \{1, 2\}$. From here it is a simple calculation to show that there are no solutions for $q > 49$. □

Proposition 4.2.34. *If $n \geqslant 4$ is composite, then Theorem 4.1 holds for Cases* L1 *and* L2 *in Table A3.*

Proof. Write $n = jh$ such that $j, h \neq 1$. First assume $n = 4$ and $q = p$ is a Mersenne prime. Note that we may assume $q > 8$ by Proposition 4.2.1. Additionally we note r_4 is also a primitive prime divisor of $p^{4f} - 1$, and $r_4 \geqslant 16f + 1$ by Lemma 2.4.15. Thus by Lemma 4.2.31, G_0 contains at least 2 distinct G-classes of derangements of order r_4, so G is not almost elusive. In the remaining cases without loss of generality we can choose h such that $h \notin \{2, 6\}$, thus there always exists a primitive prime divisor, s, of $q^h - 1$. Take $x = \hat{x}Z \in G_0$ to be an element of order s such that $\hat{x} = [\Lambda^s]$. Then x does not fix a 1-dimensional subspace of V, so x is a derangement. Therefore G is not almost elusive since G_0 contains derangements of order s and r_n. □

Proposition 4.2.35. *Assume $n \geqslant 3$ is prime. Then Theorem 4.1 holds for Cases* L1 *and* L2 *in Table A3.*

Proof. Since r_n is the unique primitive prime divisor of $q^n - 1$, it must also be the unique primitive prime divisor of $p^{fn} - 1$ (note by Proposition 4.2.1 we may assume $P_p^{fn} \neq \emptyset$). Thus it follows that $r_n = kfn + 1$ for some $k \geqslant 1$. By Lemma 2.4.11, $f = n^j$ for some $j \geqslant 0$, and since r_n and n are both odd primes it follows that $k \geqslant 2$ is even.

Assume first that Case L1 holds, that is H is of type P_1. To ensure maximality of H we require $G \leqslant \langle \mathrm{PGL}_n(q), \phi \rangle$ where ϕ is a field automorphism of $\mathrm{L}_n(q)$ of order f (since the inverse-transpose graph automorphism interchanges the stabilisers of m-spaces and $(n-m)$-spaces). Thus by Lemma 4.2.31 we conclude that G is not almost elusive.

For the remainder of the proof we may assume that Case L2 holds, that is H is of type $\mathrm{GL}_1(q) \oplus \mathrm{GL}_{n-1}(q)$. First suppose $p \geqslant 3$ and let $x = \hat{x}Z \in H_0 = H \cap G_0$ be an element of order p. Then $\hat{x} \in \mathrm{GL}_1(q) \oplus \mathrm{GL}_{n-1}(q)$ is $\mathrm{GL}_n(q)$-conjugate to $[J_p^{a_p}, \ldots, J_2^{a_2}, J_1^{a_1+1}]$ with $a_t \geqslant 0$ for all t and $\sum_{t=1}^{p} t a_t = n - 1$. Therefore any element in G_0 of order p with Jordan form $[J_3, J_2^{(n-3)/2}]$ is a derangement. Thus G is not almost elusive since G_0 contains derangements of order r_n and p. Finally suppose $p = 2$ and recall that if $n = 3$ then by Proposition 4.2.1 we may assume $q \geqslant 9$. Thus $k \geqslant 4$ by Lemma 2.4.18, so by Lemma 4.2.31 G is not almost elusive. □

Unitary groups

The remaining cases in which $G_0 = \mathrm{U}_n(q)$ are the cases in Table A3 outlined below

(a) Case U1: H is of type $P_{n/2}$ and $i = 2n - 2$ with $n = 4$ or 6;

(b) Case U2: H is of type P_1 and $i = 6$ with $n = 3$;

(c) Case U3: H is of type $\mathrm{GU}_1(q) \perp \mathrm{GU}_{n-1}(q)$ and i is defined as follows;

$$i := \begin{cases} n & n \equiv 0 \pmod 4 \\ n/2 & n \equiv 2 \pmod 4 \\ 2n & \text{otherwise} \end{cases}.$$

Proposition 4.2.36. *Theorem 4.1 holds for Case* U1 *in Table A3.*

Proof. Here H is the stabiliser of a totally singular $n/2$-space with $n = 4$ or 6. Suppose first that $n = 6$. Note that by Proposition 4.2.1 we may assume that $q \geqslant 3$. Let s be a

primitive prime divisor of q^6-1 and take an element $x = \hat{x}Z \in G_0$ of order s defined as in (4.2). Then x is a derangement by Lemma 4.2.3. Finally suppose $n = 4$. By Proposition 4.2.1 we may assume $q > 8$, so either $q = 19$ or $r_6 \geqslant 13$ by Lemma 2.4.15. Assume $q \neq 19$, then in G_0 there are $(r_6-1)/3 \geqslant 4$ distinct $\mathrm{PGU}_4(q)$-classes of elements of order r_6. Since $|\mathrm{Aut}(G_0) : \mathrm{PGU}_4(q)| = 2$ there are at least $(r_6-1)/6 \geqslant 2$ distinct G-classes of elements of order r_6 in G_0. Finally assume $q = 19$ and take $x = \hat{x}Z \in G_0$ to be an element of order 5 (the unique primitive prime divisor of q^2-1) such that $\hat{x} = [\mu, \mu^2, \mu^3, \mu^4]$ with $\mu \in \mathbb{F}_{q^2}$ a primitive 5^{th} root of unity. Since the eigenvalues of $\hat{x}$ (on $V \otimes \mathbb{F}_{q^2}$) have odd multiplicity, x is a derangement (see [9, Lemma 4.2.4]). □

Proposition 4.2.37. *Theorem 4.1 holds for Case* U2 *and Case* U3 *with* $n = 3$ *in Table A3.*

Proof. In this case $(G_0, i) = (\mathrm{U}_3(q), 6)$ and H is of type P_1 or $\mathrm{GU}_1(q) \perp \mathrm{GU}_2(q)$. In view of Proposition 4.2.1, we may assume $q \geqslant 23$. Recall that r_6 is a primitive prime divisor of q^6-1 and every element in G_0 of order r_6 is a derangement. By applying Lemma 2.4.15 we get $r_6 \geqslant 12f+1$, where $q = p^f$ as above, and we note that G_0 contains $(r_6-1)/3 \geqslant 4f$ distinct $\mathrm{PGU}_3(q)$-classes of such elements (see [9, Section 3.3.1]). Since $|\mathrm{Aut}(G_0) : \mathrm{PGU}_3(q)| = 2f$ it follows that there at least $(r_6-1)/6f \geqslant 2$ such classes in G and we conclude that G is not almost elusive. □

It now remains to deal with Case U3 in Table A3 for $n \geqslant 4$. In particular, this leads to a special case appearing in Theorem 1 (see Case 1 in Table P1). In order to handle this remaining case we first provide some important results. Let $G_0 = \mathrm{U}_n(q)$. Following [54], for $x \in \mathrm{Aut}(G_0)$ we use $\ddot{x}$ to denote the coset $G_0x \in \mathrm{Out}(G_0) = \mathrm{Aut}(G_0)/G_0$. By [54, Proposition 2.3.5],

$$\mathrm{Out}(G_0) = \langle \ddot{\delta} \rangle{:}\langle \ddot{\phi} \rangle,$$

where $|\ddot{\delta}| = (n, q+1)$, $|\ddot{\phi}| = 2f$ and $\ddot{\delta}^{\ddot{\phi}} = \ddot{\delta}^p$. With respect to an orthonormal basis $\{v_1, \ldots, v_n\}$ for V we may assume that ϕ is the field automorphism of order $2f$ corresponding to the Frobenius map $\sum_i \lambda_i v_i \longmapsto \sum_i \lambda_i^p v_i$ on V, and δ is the diagonal automorphism of order $(n, q+1)$ induced by conjugation by $[\mu, I_{n-1}]$, where $\mu \in \mathbb{F}_{q^2}$ has order $q+1$. Note that $\phi^f = \gamma$ is a graph-automorphism and that $\mathrm{Aut}(G_0) = \langle \mathrm{PGU}_n(q), \phi \rangle$. We remind the reader that the notation for prime order elements in classical groups was set up in Section 4.1.

We will first look at how the outer automorphisms affect the number of conjugacy classes of elements of certain prime orders. Take $G = G_0.J$ such that $J \leqslant \mathrm{Out}(G_0)$ and take r to be a prime divisor of $|G_0|$ such that r is a primitive prime divisor of $q^i - 1$ for some $i \geqslant 2$ such that i is even. Define $\Phi = \{\Lambda_1, \ldots, \Lambda_s\}$, where the Λ_j's are the multisets of eigenvalues in $\mathbb{F}_{q^i}$ as defined in (4.1). Since the diagonal automorphisms act trivially on the set Φ, they do not affect the number of conjugacy classes of elements of order r in G_0. However the field automorphisms $\phi^l \in \langle\phi\rangle$ act on Φ as

$$\phi^l \cdot \Lambda_j = \{\mu_j^{p^l}, \mu_j^{q^2p^l}, \ldots, \mu_j^{q^{2(b-1)}p^l}\} \in \Phi,$$

so $\langle\phi\rangle$ induces a permutation on Φ. Thus the number of G-classes of elements of order r in G_0 depends entirely on how J projects onto $\langle\ddot{\phi}\rangle$. In Lemma 4.2.38 we prove precisely how many orbits the group $\langle\phi^k\rangle$ has with its action on Φ, where k is some divisor of $2f$. Recall that P_a^b denotes the set of primitive prime divisors of $a^b - 1$ for positive integers a and b. In the following lemma we use i, Λ_j, Φ, q and ϕ as defined above.

Lemma 4.2.38. *Suppose $r \in P_q^i \cap P_p^m$ for some $m \leqslant if$ and let $D = \langle\phi^k\rangle$ where $2f = kh$. Define $a := (m, f)$ and $d := (a, k)$. Then the orbits of D acting on Φ are of size $\frac{at}{k}$, where $t = 2$ if $\frac{k}{d}$ is odd, otherwise $t = 1$.*

Proof. Since $a = (m, f)$ we may write $m = av$ and $f = az$ such that $(v, z) = 1$. By assumption r is a primitive prime divisor of both $q^i - 1$ and $p^m - 1$, which implies that $v = i$, that is $m = ai$. We note that a is odd since $(a, i) = 1$ and i is even.

In view of the orbit stabiliser theorem we focus our attentions on the size of the stabilisers in D of each $\Lambda_j \in \Phi$, which we denote as D_{Λ_j}. Fix $\Lambda_j \in \Phi$ and take $\phi^{lk} \in D$ for some $0 \leqslant l < h$. We may assume $l > 0$, otherwise we have the identity element. Here $\phi^{lk} \in D_{\Lambda_j}$ if and only if $\lambda_j^{q^{2w}p^{lk}} = \lambda_j$ for some $1 \leqslant w \leqslant i/2 - 1$. Since $\lambda_j \in T(r)$, this occurs if and only if $p^{2wf+lk} \equiv 1 \pmod{r}$. In turn this occurs if and only if m divides $2fw + lk$, which is equivalent to saying that $lk = xa$ for some $1 \leqslant x \leqslant 2z - 1$ and that there exists a $c \in \{1, \ldots, 2z - 1\}$ such that $2zw = ci - x$.

Assume $lk = xa$ for some $1 \leqslant l < h$ and $1 \leqslant x \leqslant 2z - 1$. First suppose that x is odd. Since i is even there does not exist a c such that $2zw = ci - x$. Next suppose x is even and note that z is odd since $(i, z) = 1$. Then by Lemma 2.4.4 there always exists at least one $1 \leqslant c \leqslant 2z - 1$ such that $ci - x \equiv 0 \pmod{2z}$. So we conclude that $\phi^{lk} \in D_{\Lambda_j}$ for $1 \leqslant l < h$ if and only if $lk = xa$ for some even $1 \leqslant x \leqslant 2z - 1$.

Suppose first that k/d is even. Then lk/a is even, so $|D_{\Lambda_j}|$ is precisely the number of multiples of a/k in $\{0, \ldots, h-1\}$. Thus $|D_{\Lambda_j}| = 2z$ since $h = 2za/k$. Finally suppose that

k/d is odd. In this case lk/a is even if and only if l is even. Thus in a similar manner $|D_{\Lambda_j}|$ is precisely the number of even multiples of a/k in $\{0, \dots, h-1\}$, so $|D_{\Lambda_j}| = z$.

Since the size of $|D_{\Lambda_j}|$ is independent of j we conclude that all the orbits have the same size. Thus the result follows by the orbit-stabiliser theorem since $|D| = h = 2za/k$. □

Corollary 4.2.39. *Let G be an almost simple group with socle $G_0 = \mathrm{U}_n(q)$, where $n \geqslant 5$ is odd. Let r be a primitive prime divisor of both $q^{2n}-1$ and p^m-1 and define $a := (m, f)$. Then there exists a unique G-class of elements of order r in G_0 if and only if*

(i) *$r = 2na + 1$; and*

(ii) *G/G_0 projects onto $\langle \ddot{\phi} \rangle$.*

Proof. Let $K_{G_0}(G, r)$ be the number of G-classes of elements of order r in G_0 and let $J = G/G_0 \leqslant \mathrm{Out}(G_0)$. Since r is a primitive prime divisor of $p^m - 1$, $m = 2na$ and $r = 2naw + 1$ for some positive integer w. The $\mathrm{PGU}_n(q)$-classes of elements of order r in G_0 are represented by the elements $x_j = [\Lambda_j]Z$, where Λ_j is as defined in (4.1) and $1 \leqslant j \leqslant s = (r-1)/n = 2aw$ (see [9, Proposition 3.3.2]).

Assume first that the projection of J to $\langle \ddot{\phi} \rangle$ is trivial. Then $G \leqslant \mathrm{PGU}_n(q)$ so $K_{G_0}(G, r) = 2aw \geqslant 2$. Now assume that the projection of J to $\langle \ddot{\phi} \rangle$ is nontrivial, say J projects onto $\langle \ddot{\phi}^k \rangle$ for some $1 \leqslant k < 2f$. Then by Lemma 4.2.38, $K_{G_0}(G, r) = 2kw/t$ where $t = 2$ if $k/(a, k)$ is odd and $t = 1$ otherwise. Therefore $K_{G_0}(G, r) = 2kw/t = 1$ if and only if $k = w = 1$. □

Next we prove that all prime order derangements must be in $\mathrm{PGU}_n(q)$ when n is odd and H is of type $\mathrm{GU}_1(q) \perp \mathrm{GU}_{n-1}(q)$.

Lemma 4.2.40. *Let $G_0 = \mathrm{U}_n(q)$ such that n is odd and take $x \in \mathrm{Aut}(G_0) \setminus \mathrm{PGU}_n(q)$ to be an element of prime order. Then x is $\mathrm{PGU}_n(q)$-conjugate to ϕ^i for some $1 \leqslant i < 2f$.*

Proof. The group $\mathrm{Aut}(G_0)$ may be split up into a union of cosets of $\mathrm{PGU}_n(q)$, namely $\mathrm{Aut}(G_0) = \mathrm{PGU}_n(q) \cup \mathrm{PGU}_n(q)\phi \cup \cdots \cup \mathrm{PGU}_n(q)\phi^{2f-1}$. Thus if $x \in \mathrm{Aut}(G_0) \setminus \mathrm{PGU}_n(q)$ is an element of prime order r, we may assume that $x \in \mathrm{PGU}_n(q)\phi^i$ such that $|\phi^i|$ has order r. Assume first that $i \neq f$. By [9, Lemma 3.1.17] every element of prime order in $\mathrm{PGU}_n(q)\phi^i$ is $\mathrm{PGU}_n(q)$-conjugate to ϕ^i, so the result holds. Finally assume $i = f$. Then $\phi^i = \gamma$ which implies that $r = 2$ and x is a graph automorphism. Note every involutory graph automorphism of G_0 is contained in $\mathrm{PGU}_n(q)\gamma$. Then by [9, Proposition 3.3.15], x is $\mathrm{PGU}_n(q)$-conjugate to γ. Thus the result follows. □

Corollary 4.2.41. *Let $G_0 = \mathrm{U}_n(q)$ such that n is odd and take $x \in \mathrm{Aut}(G_0) \setminus \mathrm{PGU}_n(q)$ to be an element of prime order. Let V denote the natural G_0-module. Then x fixes a non-degenerate m-space for $1 \leqslant m \leqslant n$.*

Proof. Let $\{v_1, \ldots, v_n\}$ be an orthonormal basis for $V = (\mathbb{F}_{q^2})^n$. We recall that the standard field automorphisms are defined as

$$\phi^i : \sum_j \lambda_j v_j \longmapsto \sum_j \lambda_j^{p^i} v_j.$$

Thus each ϕ^i fixes the non-degenerate m-space $\langle v_1, \ldots, v_m \rangle$ for all $1 \leqslant i < 2f$. Thus the result follows by Lemma 4.2.40. □

We are now in a position to handle Case U3 with $n \geqslant 4$.

Proposition 4.2.42. *Theorem 4.1 holds for Case* U3 *with $n \geqslant 4$ in Table A3.*

Proof. Let $x = \hat{x}Z \in H_0$ be an element of order p. Then $\hat{x}$ fixes a non-degenerate 1-space U and the non-degenerate $(n-1)$-space, $U^\perp$, so $\hat{x} \in \mathrm{GU}_1(q) \times \mathrm{GU}_{n-1}(q)$. Therefore $\hat{x}$ is $\mathrm{GU}_n(q)$-conjugate to $[J_p^{a_p}, \ldots, J_2^{a_2}, J_1^{a_1+1}]$, where $\sum_{t=1}^{p} t a_t = n - 1$. Thus a unipotent element in G_0 is a derangement if and only if its Jordan form does not contain a Jordan 1-block. This implies that G_0 does not contain a derangement of order p if and only if n is odd and $p = 2$.

Assume n is even, or n is odd with $p \geqslant 3$. Then by the argument above G_0 contains both unipotent and semisimple derangements, so G is not almost elusive. Thus for the remainder of the proof we may assume that n is odd and $p = 2$. We recall that in this case any element of order $r_i = r_{2n}$ in G_0 is a derangement, where r_{2n} is the unique primitive prime divisor of $q^{2n} - 1$ (see Lemma 2.1.25).

Suppose first that n is not prime and $n \neq 9$. Then without loss of generality we can write $n = th$ for positive integers t and h such that $t, h \neq 1$ and $t \geqslant 5$. Take s to be a primitive prime divisor of $q^{2t} - 1$ and let $x = \hat{x}Z \in G_0$ be an element of order s such that $\hat{x} = [\Lambda^h]$. Then x is a derangement, so G_0 contains semisimple derangements of distinct prime order (namely s and r_{2n}). Thus G is not almost elusive.

Now let us suppose that $n = 9$ and $q \neq 2$. Take s to be a primitive prime divisor of $q^6 - 1$ and let $x = \hat{x}Z$ be an element of order s such that $\hat{x} = [\Lambda^3]$. Then x is a derangement, so G is not almost elusive.

Next suppose that $(n, q) = (9, 2)$. Then 3 is a divisor of $|\Omega|$ and in particular it is the unique primitive prime divisor of $q^2 - 1$. Take $x = \hat{x}Z \in G_0$ to be an element of order 3

such that $\hat{x} = [\Lambda^3]$ with $\Lambda = \{\mu, \mu^{q^2}, \mu^{q^4}\}$ for some $\mu \in \mathbb{F}_{q^6}$ of order 9. Note that $x \in G_0$ since $(9)_3 > (q+1)_3$ (see [9, Proposition 3.3.3]) and x is a derangement.

Finally assume n is prime. Note that r_{2n} is also the unique primitive prime divisor of $2^{2nf} - 1$, so $r_{2n} = 2nfd + 1$ for some $d \geqslant 1$. Thus G_0 contains $(r_{2n} - 1)/n = 2fd$ distinct $\mathrm{PGU}_n(q)$-classes of elements of order r_{2n}. Since $|\operatorname{Aut}(G_0) : \mathrm{PGU}_n(q)| = 2f$ there are at least $(r_{2n} - 1)/2nf = d$ distinct G-classes of elements of order r_{2n} in G_0. Therefore G is not almost elusive if $d \geqslant 2$, so we may assume $r_{2n} = 2nf + 1$. Thus by Lemma 2.4.18 either $(n, q, r_{2n}) = (5, 2, 11)$ or n divides $q+1$. The case $(n, q, r_{2n}) = (5, 2, 11)$ has already been handled in Proposition 4.2.1, so we may assume that n divides $q + 1$.

We note that the only prime divisors of $|\Omega|$ are 2, r_{2n} and n (see [9, Case III of Table 4.1.2] and Remark 2.4.17). Thus these are the only possible primes for prime order derangements in G. Additionally, we note that by Lemma 4.2.40 and Corollary 4.2.41 any prime order derangement in G must be contained in $\mathrm{PGU}_n(q)$. Thus by arguments at the beginning of the proof there are no derangements of order $p = 2$ in G.

Note that n is a primitive prime divisor of $q^2 - 1$. Let $x = \hat{x}Z \in \mathrm{PGU}_n(q)$ be an element of order n. Then by [9, Proposition 3.3.3], either x fixes a non-degenerate 1-space, or $x \notin G_0$ and is such that $\hat{x} = [\Lambda]$ with $\Lambda = \{\mu, \mu^{q^2}, \ldots, \mu^{q^{2(n-1)}}\}$ for some $\mu \in \mathbb{F}_{q^{2n}}$ of order $n(q+1)_n$. Thus $\mathrm{PGU}_n(q)$ contains a derangement of order n and G_0 does not. We conclude that if $\mathrm{PGU}_n(q) \leqslant G$ then G is not almost elusive.

Thus we are left to handle the case in which $G \cap \mathrm{PGU}_n(q) = G_0$. In this case the only possible derangements of prime order in G are the elements of order $r_{2n} = 2nf + 1$ in G_0. Write $G = G_0.J$ where

$$J \leqslant \operatorname{Out}(G_0) = \langle \ddot{\delta} \rangle : \langle \ddot{\phi} \rangle = C_n : C_{2f}$$

Then by Corollary 4.2.39, G is almost elusive if and only if J projects onto $\langle \ddot{\phi} \rangle$. This completes the proof of the proposition. □

Remark 4.2.43. This leaves us with a potentially infinite family of almost simple almost elusive groups with socle $G_0 \in \mathcal{A}$. However, due to the severe number theoretic restrictions in this case (namely $r_{2n} = 2nf + 1$ being the unique primitive prime divisor of $q^{2n} - 1$ with $q = 2^f$ and n dividing $q+1$), we anticipate there are in fact no groups that satisfy all the required conditions. In Remark 2.4.17 we discuss how finding values for f and n for which these conditions are satisfied boils down to being able to solve specific Diophantine equations, which currently do not have a complete set of integer solutions. We can use Lemma 2.4.18 to deduce that $f = 2^a n^b$ for some integers $a, b \geqslant 0$ and with the aid of a

computer we can deduce that $f, n > 100$ for an almost elusive case to arise here.

Orthogonal groups

To complete the proof of Theorem 4.1 it remains to handle the orthogonal groups with point stabiliser in $\mathcal{C}_1$. These cases are outlined in Table 4.1. We begin with a definition.

Definition 4.2.44. Let $G_0 = \mathrm{P}\Omega_n^\epsilon(q)$ with natural module V and let Q denote the associated quadratic form. When n is odd we say that Q is *parabolic* (here $\epsilon = \circ$). When n is even and Q has Witt defect 1 we say Q is *elliptic* (here $\epsilon = -$). Similarly for n even and Q with Witt defect 0 we say Q is *hyperbolic* (here $\epsilon = +$). Additionally we say that a subspace W of V is parabolic (elliptic or hyperbolic) if the restriction of Q to W is parabolic (elliptic or hyperbolic).

Now we note that if $x \in \mathrm{P}\Omega_n^\epsilon(q)$ is an element of order r, such that r is a primitive prime divisor of $q^i - 1$ with i even, then $x = \hat{x}Z$ and $\hat{x}$ fixes an orthogonal decomposition of the form

$$V = U_1 \perp \cdots \perp U_t \perp \mathrm{C}_V(\hat{x})$$

where each U_j is an elliptic i-space on which $\hat{x}$ acts irreducibly, and $\mathrm{C}_V(\hat{x})$ is non-degenerate or trivial. We note this is similar to the description of prime order elements in linear groups as discussed in Section 4.1.1 (see also [9, Proposition 3.5.4]).

In Propositions 4.2.45, 4.2.46 and 4.2.47 we handle the cases in which H is the stabiliser of a totally singular m-space for particular m.

Proposition 4.2.45. *Theorem 4.1 holds for Case* O1 *in Table A3.*

Proof. Here H is the stabiliser of a totally singular 1-space and

$$|\Omega| = (q^{n/2} - 1)(q^{(n-2)/2} + 1)/(q - 1).$$

Let s be a primitive prime divisor of $q^{n/2} - 1$ and note that $n/2$ is even (by Proposition 4.2.1 we are assuming $(n, q) \neq (12, 2)$ so s always exists). Take $x = \hat{x}Z \in G_0$ to be an element of order s such that $\hat{x} = [\Lambda^2]$. Then x does not fix a 1-space, so is a derangement. Therefore G is not almost elusive since G_0 contains derangements of order s and of order r_{n-2} (where r_{n-2} denotes the unique primitive prime divisor of $q^{n-2} - 1$). □

Proposition 4.2.46. *Theorem 4.1 holds for Case* O2 *in Table A3 .*

Table 4.1: Orthogonal groups with $\mathcal{C}_1$ subgroups from Tables A1 and A3

Case	G_0	Type of H	Conditions	i
O1	$\mathrm{P}\Omega_n^+(q)$	P_1	$n \equiv 0 \pmod 4$	$n-2$
O2		P_4	$n = 8$	$n-2$
O3		$\mathrm{Sp}_{n-2}(q)$	$n \equiv 2 \pmod 4$	$n/2$
XVIII		$\mathrm{Sp}_{n-2}(q)$	$n \equiv 0 \pmod 4$	
O4		$\mathrm{O}_1(q) \perp \mathrm{O}_{n-1}(q)$	$n \equiv 2 \pmod 4$	$n/2$
XVII		$\mathrm{O}_1(q) \perp \mathrm{O}_{n-1}(q)$	$n \equiv 0 \pmod 4$	
O5		$\mathrm{O}_2^+(q) \perp \mathrm{O}_{n-2}^+(q)$	$n \equiv 0 \pmod 4$	$n-2$
O6		$\mathrm{O}_2^-(q) \perp \mathrm{O}_{n-2}^-(q)$	$n \equiv 0 \pmod 4$	$(n-2)/2$
O7		$\mathrm{O}_2^-(q) \perp \mathrm{O}_{n-2}^-(q)$	$n \equiv 2 \pmod 4$	$n/2$
O12	$\mathrm{P}\Omega_n^-(q)$	P_1	$n \equiv 2 \pmod 4$	n
O13		$\mathrm{Sp}_{n-2}(q)$		n
O14		$\mathrm{O}_1(q) \perp \mathrm{O}_{n-1}(q)$		n
O15		$\mathrm{O}_2^+(q) \perp \mathrm{O}_{n-2}^-(q)$	$n \equiv 2 \pmod 4$	n
O16	$\Omega_n(q)$	P_1	$n \equiv 1 \pmod 4$	$n-1$
O17		$\mathrm{O}_1(q) \perp \mathrm{O}_{n-1}^+(q)$		$n-1$
O18		$\mathrm{O}_1(q) \perp \mathrm{O}_{n-1}^-(q)$	$n \equiv 3 \pmod 4$	$(n-1)/2$
XXII		$\mathrm{O}_1(q) \perp \mathrm{O}_{n-1}^-(q)$	$n \equiv 1 \pmod 4$	
O19		$\mathrm{O}_2^\epsilon(q) \perp \mathrm{O}_{n-2}(q)$	$n \equiv 1 \pmod 4$	$n-1$

Proof. Here $(G_0, i) = (\mathrm{P}\Omega_8^+(q), 6)$ and H is the stabiliser of a totally singular 4-space. In this case $|\Omega| = (q+1)(q^2+1)(q^3+1)$. Let s be a primitive prime divisor of q^4-1 and take $x = \hat{x}Z \in G_0$ to be an element of order s such that $\hat{x} = [\Lambda, I_4]$. Then x is a derangement by Lemma 4.2.2. Thus the result follows. □

Proposition 4.2.47. *Theorem 4.1 holds for Cases* O12 *and* O16 *in Table A3.*

Proof. Suppose that (G_0, H, i) is as in Case O12 (respectively, O16) in Table A3 and all relevant conditions hold. Then H is the stabiliser of a totally singular 1-space and

$$|\Omega| = (q^{n/2}+1)(q^{(n-2)/2}-1)/(q-1)$$

(respectively, $(q^{n-1}-1)/(q-1)$).

Assume first that $(n,q) \neq (14,2)$ (note this initial assumption is only necessary for Case O12) and take s to be a primitive prime divisor of $q^{(n-2)/2}-1$ (respectively, $q^{(n-1)/2}-1$). Let $x = \hat{x}Z \in G_0$ be an element of order s such that $\hat{x} = [\Lambda^2, I_2]$ (respectively, $\hat{x} = [\Lambda^2, I_1]$). By [9, Remark 3.5.5] the 1-eigenspace of x is elliptic (respectively parabolic). Therefore x is a derangement, so G_0 contains derangements of order r_n (respectively, r_{n-1}) and order s. Finally assume $(n,q) = (14,2)$ and note that 3 is a primitive prime divisor of q^2-1. Take $x = \hat{x}Z \in G_0$ to be an element of order 3 such that $\hat{x} = [\Lambda^7]$. Then x does not fix a 1-space, so is a derangement. Thus the result follows since $s \neq r_n$. □

In the following proposition we handle the cases in which H is the stabiliser of a non-singular 1-space.

Proposition 4.2.48. *Theorem 4.1 holds for Cases* O3 *and* O13 *in Table A3 and case* XVIII *in Table A1.*

Proof. Here $G_0 = \mathrm{P}\Omega_n^\epsilon(q)$ and H is the stabiliser of a non-singular 1-space. Recall by Proposition 4.2.1 we may assume that $q > 2$ for $n = 8, 10$ and 12. Note that here $q = 2^f$ is even and $|\Omega| = q^{n/2-1}(q^{n/2}-\epsilon)$. Let r be an odd prime divisor of $q^{n/2}-\epsilon$ such that r is a primitive prime divisor of $q^j - 1$ for some $j \geqslant 1$. Note that if $\epsilon = -$ then j divides n but not $n/2$, so j is even and n/j is odd. Similarly if $\epsilon = +$ then j divides $n/2$, so n/j is even. Take $x = \hat{x}Z \in G_0$ to be an element of order r such that

$$\hat{x} := \begin{cases} [(\Lambda, \Lambda^{-1})^{(n/2j)}] & \epsilon = + \text{ and } j \text{ is odd} \\ [\Lambda^{n/j}] & \text{otherwise} \end{cases}.$$

Then x does not fix a 1-space, so is a derangement. Therefore we may assume that $q^{n/2} - \epsilon = r^l$ for some odd prime r and $l \geqslant 1$. It follows by Lemma 2.4.1 that one of the following is satisfied:

(i) $\epsilon = +$ and $r = 2^{fn/2} - 1$ is a Mersenne prime; or

(ii) $\epsilon = -$ and $r = 2^{fn/2} + 1$ is a Fermat prime, $n = 2^w$ for some $w \geqslant 3$ and $f = 2^u$ for some $u \geqslant 0$.

Suppose (i) holds. Then in particular $j = n/2$ is prime and $f = 1$, so $\mathrm{Aut}(G_0) = \mathrm{PGO}_n^+(q)$. It follows that G_0 contains $(r-1)/(n/4) = (2^{(n/2+2)} - 8)/n \geqslant 2$ distinct G-classes of derangements of order r. Thus we conclude that G is not almost elusive.

Now suppose that (ii) holds. Then $j = n = 2^w$ for some $w \geqslant 3$ and $f = 2^u$ for some $u \geqslant 0$. Thus G_0 contains $(r-1)/n = 2^{(2^k - w)}$ distinct $\mathrm{PGO}_n^-(q)$-classes of derangements

of order r, where $k = w + u - 1$. Now $|\operatorname{Aut}(G_0) : \mathrm{PGO}_n^-(q)| = f$ so we conclude that G_0 contains at least $(r-1)/fn = 2^{2^k-(k+1)}$ distinct G-classes of derangements of order r. It is straightforward to check that $k \geqslant 3$ and so $2^{2^k-(k+1)} \geqslant 2$. Therefore G is not almost elusive. □

In Propositions 4.2.49, 4.2.50 and 4.2.51 we handle the cases in which H is the stabiliser of a decomposition $V = U \perp W$ of the natural module, where W is a non-degenerate $(n-1)$-dimensional space of type $\epsilon \in \{+, -, \circ\}$. Note that in all of these cases $q = p^f$ is odd. Additionally if $x = \hat{x}Z \in H_0$ is an element of order p then $\hat{x} \in \Omega_{n-1}^{\epsilon}(q)$, and so the Jordan form of x must contain at least one Jordan 1-block.

Proposition 4.2.49. *Theorem 4.1 holds for Case* O4 *in Table A3 and Case* XVII *in Table A1.*

Proof. In both cases $G_0 = \mathrm{P}\Omega_n^+(q)$ with q odd and H is of type $\mathrm{O}_1(q) \perp \mathrm{O}_{n-1}(q)$. Assume first we are in Case O4. Then $n \equiv 2 \pmod 4$ and any nontrivial element in G_0 of order $r_{n/2}$ is a derangement by Lemma 2.1.25 (since $r_{n/2} \in \alpha(G_0) \setminus \alpha(H_0)$). Take $x \in G_0$ to be an element of order p with Jordan form $[J_3^2, J_2^{(n-6)/2}]$ on V. Then x is a derangement since it does not contain a Jordan 1-block. Thus G is not almost elusive.

We may assume for the remainder of the proof that we are in Case XVII, so in particular $n \equiv 0 \pmod 4$. Take r to be a primitive prime divisor of $q^{n/2} - 1$ (note that by Proposition 4.2.1 r always exists) and let $x = \hat{x}Z \in G_0$ be an element of order r such that $\hat{x} = [\Lambda^2]$. Then x is a derangement. Suppose $n \geqslant 12$ and take $y \in G_0$ to be an element of order p with Jordan form $[J_3^4, J_2^{(n-12)/2}]$ on V. Then $y \notin H_0$ since the Jordan form does not contain a Jordan 1-block, so we conclude that G is not almost elusive. Finally suppose $n = 8$. If $p \geqslant 5$ then any element in G_0 of order p with Jordan form $[J_5, J_3]$ on V is a derangement. Thus we may assume $p = 3$ and by Proposition 4.2.1 $q \neq 3$. Take s to be a primitive prime divisor of $q^2 - 1$ and let $y = \hat{y}Z \in G_0$ be an element of order s such that $\hat{y} = [\Lambda^4]$. Then y is a derangement, so again G is not almost elusive. □

Proposition 4.2.50. *Theorem 4.1 holds for Case* O14 *in Table A3.*

Proof. Here $(G_0, i) = (\mathrm{P}\Omega_n^-(q), n)$ and H is of type $\mathrm{O}_1(q) \perp \mathrm{O}_{n-1}(q)$. Suppose first that $n > 8$. Let $x \in G_0$ be an element of order p with Jordan form $[J_3^2, J_2^{(n-6)/2}]$ if $n \equiv 2 \pmod 4$ and $[J_3^4, J_2^{(n-12)/2}]$ if $n \equiv 0 \pmod 4$. Then x is a derangement since there are no Jordan 1-blocks in its Jordan form on V. Thus G_0 contains both unipotent and semisimple derangements. Finally assume $n = 8$. By Proposition 4.2.1 we may assume

$q \geqslant 5$, so $r_8 \geqslant 32f + 1$ by Lemma 2.4.15. Therefore G_0 contains $(r_8 - 1)/8 = 4f$ distinct $\mathrm{PGO}_n^-(q)$-classes of elements of order r_8 (see [9, Propositions 3.5.4 and 3.5.8]). Since $|\operatorname{Aut}(G_0) : \mathrm{PGO}_n^-(q)| = f$ there are at least $(r_8 - 1)/8f \geqslant 4$ distinct G-classes of elements of order r_8 in G_0, so G is not almost elusive. □

Proposition 4.2.51. *Theorem 4.1 holds for Cases* O17 *and* O18 *in Table A3 and Case* XXII *in Table A1.*

Proof. Here $G_0 = \Omega_n(q)$ and H is the stabiliser of a non-degenerate $(n-1)$-space of type $\epsilon \in \{+, -\}$. Assume $n \geqslant 9$ when $\epsilon = +$ and take $x = \hat{x}Z \in G_0$ to be an element of order p with the following Jordan form:

	$n \equiv 1 \pmod 4$	$n \equiv 3 \pmod 4$
$\epsilon = +$	$[J_3^3, J_2^{(n-9)/2}]$	$[J_3, J_2^{(n-3)/2}]$
$\epsilon = -$	$[J_2^{(n-1)/2}, J_1]$	$[J_3, J_2^{(n-3)/2}]$

By [9, Proposition 3.5.12] if $\hat{x} \in \Omega_{n-1}^-(q)$ is an element of order p with Jordan form $[J_p^{a_p}, \ldots, J_1^{a_1}]$, then $a_i > 1$ for some odd i. Thus x is a derangement. It follows that in Case O17 with $n \geqslant 9$ or in Case O18, G_0 contains both semisimple and unipotent derangements and we are done.

Suppose we are in Case O17 with $n = 7$. Then $\epsilon = +$ and by assumption G_0 contains semisimple derangements. If $p \geqslant 5$ then any element in G_0 with Jordan form $[J_3, J_2^2]$ is a derangement, so we may assume $p = 3$. By Proposition 4.2.1 we may additionally assume $q \geqslant 9$, so $r_i = r_6 \geqslant 24f + 1$ by Lemma 2.4.15. Thus continuing in the usual manner, G_0 contains $4f$ distinct $\mathrm{PGO}_7(q)$-classes of order r_6, and since $|\operatorname{Aut}(G_0) : \mathrm{PGO}_7(q)| = f$, G_0 contains at least 4 distinct G-classes of elements of order r_6. Thus the result follows.

Finally assume we are as in Case XXII, then $\epsilon = -$ and $n \equiv 1 \pmod 4$. Let s be a primitive prime divisor of $q^{(n-1)/2} - 1$ and take $x = \hat{x}Z \in G_0$ to be an element of order s such that $\hat{x} = [\Lambda^2, I_1]$. Now suppose that x fixes a non-degenerate $(n-1)$-space W of type $\epsilon = -$. Then $\hat{x}$ acts nontrivially on W since $\dim C_V(\hat{x}) = 1 < n - 1$, so we obtain a decomposition $W = W_1 \perp W_2$ where W_1 and W_2 are elliptic $(\frac{n-1}{2})$-spaces. This forces W to be a hyperbolic space (of type $\epsilon = +$) which is a contradiction, so we conclude that x is a derangement. Thus G is not almost elusive. □

The last three propositions deal with the cases in which H is the stabiliser of a decomposition $V = U \perp W$ of the natural module, where W is a non-degenerate 2-dimensional space of type $\epsilon \in \{+, -\}$.

Proposition 4.2.52. *Theorem 4.1 holds for Cases* O5 *and* O6 *in Table A3.*

Proof. Here $G_0 = \mathrm{P}\Omega_n^+(q)$, $n \equiv 0 \,(\mathrm{mod}\, 4)$ and H stabilises a non-degenerate 2-space of type $\epsilon \in \{+, -\}$. Let s be a primitive prime divisor $q^{n/2} - 1$ and note that by Proposition 4.2.1 we assume $(n, q) \neq (12, 2)$, so s always exists. Take $x = \hat{x}Z \in G_0$ to be an element of order s such that $\hat{x} = [\Lambda^2]$. Then x does not fix a 2-space, so x is a derangement. Thus G_0 contains derangements of order r_i and order s, so the result follows. □

Proposition 4.2.53. *Theorem 4.1 holds for Cases* O7 *and* O15 *in Table A3.*

Proof. Here $G_0 = \mathrm{P}\Omega_n^{\pm}(q)$ with $n \equiv 2 \,(\mathrm{mod}\, 4)$ and we note in both cases all elements of H stabilise an $(n-2)$-dimensional non-degenerate elliptic (of type $\epsilon = -$) space. For the case when $(n, q) \neq (14, 2)$, we refer the reader to the final paragraph in the proof of Proposition 4.2.51 since the proof here is similar.

Now assume $(n, q) = (14, 2)$. Take (G_0, H, i) to be as in Case O7 (respectively Case O15), then any element in G_0 of order $r_7 = 127$ (resp. $r_{14} = 43$) is a derangement. The elements $x = \hat{x}Z \in G_0$ of order r_7 (resp. r_{14}) have the form $\hat{x} = [(\Lambda, \Lambda^{-1})]$ (resp. $[\Lambda]$). Therefore by [9, Proposition 3.5.4] there are 9 (resp. 3) distinct $\bar{G} = \mathrm{PGO}_{14}^+(2)$ (resp. $\mathrm{PGO}_{14}^-(2)$)-classes of derangements of order r_7 (resp. r_{14}) in G_0. Therefore since $\mathrm{Aut}(G_0) = \bar{G}$ we conclude that G is not almost elusive. □

Proposition 4.2.54. *Theorem 4.1 holds for Cases* O19 *in Table A3.*

Proof. Here $G_0 = \Omega_n(q)$ with $n \equiv 1 \,(\mathrm{mod}\, 4)$ and H is of type $\mathrm{O}_2^{\epsilon}(q) \perp \mathrm{O}_{n-2}(q)$ with $\epsilon \in \{+, -\}$. Recall that any element in G_0 of order r_{n-1} is a derangement, where r_{n-1} is the unique primitive prime divisor of $q^{n-1} - 1$. Let s be a primitive prime divisor of $q^{(n-1)/2} - 1$ and take $x = \hat{x}Z \in G_0$ to be an element of order s such that $\hat{x} = [\Lambda^2, I_1]$. Then x does not fix a non-degenerate 2-space of type ϵ, so G_0 contains derangements of order r_{n-1} and s, implying that G is not almost elusive. □

This completes the proof of Theorem 4.1 for subspace subgroups. In particular, in view of Propositions 4.2.1 and 4.2.28, this completes the proof of Theorem 4.1 entirely.

4.3 The quasiprimitive case

In this section we prove Theorem 2 for classical groups. Throughout this section we let G be an almost simple classical group with socle $G_0 \in \mathcal{A}$ and let H be a core-free non-maximal subgroup of G such that $G = G_0H$. Recall, $\mathcal{A}$ is defined as in Notation 2.3.2. The content of this section is made up of work in [45, Section 4]. We prove the following result:

Theorem 4.2. *The pair (G, H) is almost elusive only if one of the following holds:*

(i) *$G_0 = \mathrm{U}_n(q)$ and H stabilises a 1-dimensional non-degenerate subspace of the natural module, where q is even and $n \geqslant 5$ is a prime divisor of $q + 1$.*

(ii) *$G_0 = \mathrm{L}_2(p)$ with $p \geqslant 5$ prime and (G, H) is recorded in Table Q1.*

(iii) *(G, H) is recorded in Table Q2.*

Remark 4.3.1. Here we provide some remarks on Theorem 4.2.

(a) Suppose that (G, H) is as in Case (i) of Theorem 4.2. Then $H < M$, where M is the stabiliser of a 1-dimensional non-degenerate subspace of the natural module. In particular, (G, M) arises in Case 1 of Table P1, with the relevant conditions on n and q provided in Remark 8.2(a). As discussed in Remark 4.2.43 we expect that there are no examples that satisfy all the number-theoretic conditions. That is no genuine almost elusive examples arise in this case, which would allow us to eliminate Case (i) in Theorem 4.2.

(b) In part (ii), if (G, H) is a case recorded in Table Q1, then (G, K) is almost elusive for any subgroup K of G isomorphic to H. See Proposition 4.3.8.

(c) For part (iii), let (G, H) be any of the cases recorded in Table Q2. Then G has a subgroup K with $H \cong K$ such that (G, K) is almost elusive. In the table, we record the total number of G-classes of subgroups isomorphic to H such that $G = G_0H$, together with the number of these G-classes that give almost elusive examples. We note that all of these groups can easily be constructed with the aid of Magma [5]. See Chapter 8 and Remark 8.3 for more details on these cases.

Recall that we may embed H in a core-free maximal subgroup M of G. By Lemma 2.1.30, we may assume that (G, M) is found in Table P1 or P2.

We begin by proving Theorem 4.2 in some small cases. For this let

$$\mathcal{K} = \{\mathrm{L}_2(q), \mathrm{L}_3^\epsilon(q'), \mathrm{U}_4(q'), \mathrm{PSp}_4(q'), \mathrm{U}_5(2),\ \mathrm{U}_6(2),\ \mathrm{PSp}_6(2)\},$$

where $q \leqslant 49$ and $q' \leqslant 8$.

Proposition 4.3.2. *Theorem 4.2 holds for $G_0 \in \mathcal{K}$.*

Proof. Let M denote a core-free maximal subgroup of G such that $H < M$. Then by Lemma 2.1.30, (G, M) is recorded in Table P1 or P2. As in Proposition 4.2.1 we can use Magma to obtain the groups G and M such that (G, M) is recorded in Tables P1 or P2. We then use the same method outlined in the proof of Proposition 3.2.2 to complete the proof. □

Proposition 4.3.2 handles all the cases with (G, M) in Table P2, so we may now assume that (G, M) is as in Cases 1-5 in Table P1, with $G_0 \notin \mathcal{K}$. We go through each of these cases in turn, using the labels in Table P1 to denote the cases. Recall that $\alpha(X)$ is the set of prime divisors of $|X|$, and $\pi(X) = |\alpha(X)|$. Additionally, we remind the reader that $H_0 = H \cap G_0$.

We begin with a remark on Case 1 in Table P1, this case corresponds to part (i) of Theorem 4.2. Here we use the notation in Notation 2.1.2. For example, we say that the pair (G, M) contains a derangement if G contains a derangement with respect to the natural action of G on G/M.

Remark 4.3.3. As discussed in Remarks 4.2.43 and 8.2(a), we do not anticipate that any primitive almost elusive groups arise in Case 1 of Table P1. Thus we do not expect any quasiprimitive almost elusive groups in this case either. However the existence (or otherwise) of an imprimitive quasiprimitive example in this setting has not been investigated.

In order to handle Cases 2-5 in Table P1, we first discuss the conjugacy classes of prime order semisimple elements when $G_0 = \mathrm{L}_2(q)$. Recall from Section 4.1.1 that in $G = \mathrm{PGL}_2(q)$, where $q = p^f$ is a prime power and p is odd, there are 2 distinct classes of involutions, represented by t_1 and t_1', and $G_0 = \mathrm{L}_2(q)$ has a unique class of involutions. More precisely, $t_1 \in G_0$ if $q \equiv 1 \pmod 4$, and $t_1' \in G_0$ if $q \equiv 3 \pmod 4$. See [9, Section 3.2.2] for more details.

Now let $x \in G$ be a semisimple element of odd prime order r, so $x \in G_0$. Then either r divides $q - 1$ or $q + 1$. Set $k = 1$ if r divides $q - 1$ and $k = 2$ otherwise. Take $x \in G$ to be an element of order r. Then x lifts to an element $\hat{x} \in \mathrm{GL}_2(q)$ that is diagonalisable

over $\mathbb{F}_{q^k}$, with eigenvalues $[\lambda^i, \lambda^{-i}]$ if $k = 1$ and $[\lambda^i, \lambda^{qi}]$ if $k = 2$, where λ is a nontrivial r^{th} root of unity in $\mathbb{F}_{q^k}$ and $1 \leqslant i \leqslant (r-1)/2$. The G-classes of elements of order r are uniquely determined by these eigenvalue sets, so there are $(r-1)/2$ such G-classes of elements of order r in G. We abuse notation and write representatives of these G-classes as $[\Lambda]Z$, where $\Lambda = [\lambda^i, \lambda^{-i}]$ if $k = 1$ and $[\lambda^i, \lambda^{qi}]$ otherwise, with Z the centre of $\mathrm{GL}_2(q)$. See [9, Section 3.2.1] for more details.

Lemma 4.3.4. *Let $L = \mathrm{L}_2(q)$ be a simple group and let K be a subgroup of L. Suppose $r \neq p$ is an odd prime divisor of $|K|$ and let $x \in L$ be an element of order r. Then $x^L \cap K \neq \emptyset$.*

Proof. Here $|L| = \frac{q}{(2,q-1)}(q-1)(q+1)$, so r divides $q-1$ or $q+1$. The two cases are very similar, so we only provide details in the case where r divides $q-1$. Let $y \in K$ be an element of order r. Then without loss of generality, we can assume $y \in ([\lambda, \lambda^{-1}]Z)^L$. This implies that $y^t \in ([\lambda^t, \lambda^{-t}]Z)^L$ for all $1 \leqslant t \leqslant (r-1)/2$, so $\langle y \rangle$ intersects all L-classes of elements of order r and the result follows. □

Corollary 4.3.5. *Let $G \leqslant \mathrm{PGL}_2(q)$ be an almost simple group with socle $\mathrm{L}_2(q)$. Let H be a core-free subgroup of G and suppose $r \neq p$ is an odd prime divisor of $|H|$. Then (G, H) contains no derangements of order r.*

We are now in a position to handle Cases 2-5 in Table P1.

Proposition 4.3.6. *Theorem 4.2 holds for (G, M) as in Cases 2 or 3 in Table P1.*

Proof. Here $G_0 = \mathrm{L}_2(p)$ and $M = C_p{:}C_{k(p-1)/2}$ is a P_1 parabolic subgroup of G (that is, M is a Borel subgroup of G), where $k = |G : G_0| \in \{1, 2\}$ and $p = 2^m - 1$ is a Mersenne prime in Case 2, and $p = 2.3^a - 1$ is a prime with $a \geqslant 2$ in Case 3.

We begin by handling Case 2, so $G = G_0$ or $\mathrm{PGL}_2(p)$. Here we show that (G, H) is almost elusive only if it is recorded in Case II or III of Table Q1. Set $M_0 = M \cap G_0 = C_p{:}C_{(p-1)/2}$. We note that $|M_0|$ is odd since $p \equiv 3 \pmod 4$, so $\alpha(G_0) \setminus \alpha(M_0) = \{2\}$. Therefore every involution in G_0 is a derangement, we recall that G_0 has a unique class of involutions. Assume (G, H) is almost elusive. Again from the discussion above, we recall that $\mathrm{PGL}_2(p)$ contains two distinct classes of involutions. One class consists of the involutions in G_0, each of which is a derangement, and the other comprises the involutions in $\mathrm{PGL}_2(p) \setminus G_0$. Thus $|H|$ must be even when $G = \mathrm{PGL}_2(p)$. Next we note that $\pi(M_0) = \pi(H_0)$ by Lemma 2.1.27, which is equivalent to the condition $\alpha(M_0) = \alpha(H_0)$

since $H_0 \leqslant M_0$. Therefore, since $p \equiv 3 \pmod 4$ and $|H|$ is even when $k = 2$, we must have $H = C_p{:}C_d$, where d is a proper divisor of $k(p-1)/2$ and $\alpha(d) = \alpha(k(p-1)/2)$.

Finally we turn to Case 3. Here $G = G_0$ and we need to show that (G, H) is almost elusive only if it is recorded in Case IV of Table Q1. Assume (G, H) is almost elusive. Then as above we have $\alpha(M_0) = \alpha(H_0)$, so $H = C_p{:}C_d$ where d is a proper divisor of $(p-1)/2$ and $\alpha(d) = \alpha((p-1)/2)$. The result follows. □

Proposition 4.3.7. *Theorem 4.2 holds for (G, M) as in Case 4 or 5 in Table P1.*

Proof. Here $G = \mathrm{PGL}_2(p)$, where $p = 2^m + \epsilon$ is a prime and $M = D_{2(p+\epsilon)}$ with $\epsilon = \pm 1$. We note that $p + \epsilon \equiv 2 \pmod 4$ and we set $M_0 = M \cap G_0 = D_{p+\epsilon}$. Additionally we note that $\alpha(G) \setminus \alpha(M) = \{p\}$. Therefore every element of order p in G is a derangement and there is a unique G-class of such elements (see [9, Proposition 3.2.6]). We need to show that (G, H) is almost elusive only if it is recorded in Case I of Table Q1.

Assume that (G, H) is almost elusive. We note that by Lemma 2.1.27 we may assume that $\pi(H_0) = \pi(M_0)$, which is equivalent to $\alpha(H_0) = \alpha(M_0)$ since $H_0 \leqslant M_0$. Here the possibilities for H are as follows:

(i) $H = C_d$ such that d divides $p + \epsilon$, or

(ii) $H = D_{2d}$ such that d is a proper divisor of $p + \epsilon$.

Assume that H is as in Case (i). If $d = 2$, then every odd prime divisor of $p + \epsilon$ divides $|M_0|$ and not $|H_0|$. Additionally, if $d \neq 2$, then $H_0 = C_{d/2}$ and so 2 divides $|M_0|$ and not $|H_0|$, since $p + \epsilon \equiv 2 \pmod 4$. Thus we have that $\pi(H_0) \neq \pi(M_0)$, which is a contradiction, so we may assume H is as in Case (ii). Using similar reasoning, we reduce down to the case $H = D_{2d}$ and d is a proper divisor of $p + \epsilon$ with $\alpha(d) = \alpha(k(p+\epsilon)/2)$, where we set $k = 2$ if d is even and 1 otherwise (note that $H_0 = D_{2d/k}$, since $H \not\leqslant G_0$). If d is odd, then H has a unique conjugacy class of involutions, but we recall that there are two such classes in G, so d must be even. That is $\alpha(d) = \alpha(p + \epsilon)$ and the result follows. □

We now justify the statement in Remark 4.3.1(b).

Proposition 4.3.8. *If (G, H) is a case recorded in Table Q1, then (G, K) is almost elusive for any subgroup K of G isomorphic to H.*

Proof. First take (G, H) as in Case I of Table Q1. Here $G = \mathrm{PGL}_2(p)$ and $H = D_{2d}$, where $p = 2^m + \epsilon$ is a prime and d is a proper divisor of $p + \epsilon$ with $\alpha(d) = \alpha(p + \epsilon)$.

Note that $|G : H| = 2^{m-1}p(p+\epsilon)/d$. By Corollary 4.3.5, there are no derangements of order r for any odd prime divisor r of $p+\epsilon$. Since d is even and $H_0 = D_d$, we see that $H \setminus H_0$ contains involutions and so every involution in G has a fixed point. Finally, since $p \notin \alpha(H)$ and G contains a unique conjugacy class of elements of order p, we conclude that (G, H) is almost elusive.

Next take (G, H) to be as in Case II or III. Here $G = G_0 = \mathrm{L}_2(p)$ or $\mathrm{PGL}_2(p)$ with $p = 2^m - 1$ a Mersenne prime, and $H = C_p{:}C_d$, where d is a proper divisor of $k(p-1)/2$ and $\alpha(d) = \alpha(k(p-1)/2)$, where $k = |G : G_0|$. Then $|G : H| = 2^{m-1}k(p-1)/d$. By Corollary 4.3.5, there are no derangements of order r for any odd prime divisor r of $p-1$. Since $|H|$ is even when $k = 2$ and $|H_0|$ is odd, there exists a unique class of involutory derangements in G. Thus (G, H) is almost elusive.

A very similar argument applies in Case IV. Here $G = \mathrm{L}_2(p)$ and $H = C_p{:}C_d$, where $p = 2.3^a - 1 \geqslant 17$ is a prime and d is a proper divisor of $(p-1)/2$ with $\alpha(d) = \alpha((p-1)/2)$. Then $|G : H| = 3^a(p-1)/d$. By Corollary 4.3.5, there are no derangements of order r for any odd prime divisor r of $p-1$. Since $3 \notin \alpha(H)$ and there exists a unique class of elements of order 3 in G (see [9, Proposition 3.2.1]), we conclude that (G, H) is almost elusive. □

This completes the proof of Theorem 4.2.

CHAPTER

5

EXCEPTIONAL GROUPS

In this chapter we prove Theorems 1 and 2 for the exceptional groups of Lie type. We remind the reader that we use $\mathcal{B}$ to denote the set of all simple exceptional groups of Lie type over $\mathbb{F}_q$ (see Notation 2.3.2). In addition, recall that we consider the Tits group ${}^2F_4(2)'$ as an exceptional group of Lie type, rather than a sporadic group. We remind the reader that throughout this thesis we may assume that all groups taken are finite, unless stated otherwise. Our main result is the following.

Theorem 5.1. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a quasiprimitive permutation group with point stabiliser H and socle $G_0 \in \mathcal{B}$. Then G is almost elusive if and only if either*

(i) $(G, H) = (G_2(4), J_2)$, $({}^2F_4(2), 5^2{:}4S_4)$*; or*

(ii) $(G_0, H \cap G_0) = ({}^2F_4(2)', \mathrm{L}_2(25))$.

In particular, G is almost elusive only if G is primitive.

The content of this chapter can be found in [13, Sections 4.3 and 4.4] and [45, Section 2]. We begin by stating some preliminary results.

5.1 Preliminaries

We begin with a result regarding the group $G_2(q)$. Let $G = G_2(q)$ with $q \geqslant 3$ and let V denote the minimal module for $G_2(q)$, so V is irreducible and $\dim V = 7 - \delta_{2,p}$ (recall we write $q = p^f$ where p is a prime and f is a positive integer). Now $M = \mathrm{SL}_3^\epsilon(q)$:2 is a maximal subgroup of G (see [6, Tables 8.30, 8.41 and 8.42] for example) and we let $H = \mathrm{SL}_3^\epsilon(q) < M$. For matrices $A_1, \ldots, A_n$ we use $[A_1, \ldots, A_n]$ to denote a block-diagonal matrix with blocks $A_1, \ldots, A_n$, while A_i^{-T} denotes the inverse-transpose of A_i.

Lemma 5.1.1. *Let $G = G_2(q)$ with $q \geqslant 3$ and let V be the minimal module for G. Take $x \in H = \mathrm{SL}_3^\epsilon(q)$ such that x acts as the matrix A on the natural H-module. Then up to conjugacy, x acts on V as*

$$\begin{cases} [A, A^{-T}] & \text{if } q \text{ is even} \\ [A, A^{-T}, 1] & \text{otherwise} \end{cases}.$$

Proof. We work with the algebraic groups $\bar{G} = G_2(k)$ and $\bar{H} = \mathrm{SL}_3(k)$, where k is the algebraic closure $\bar{\mathbb{F}}_p$. Let $\bar{V} = V \otimes k$ denote the minimal module of $\bar{G}$ and $\bar{W}$ the natural $\bar{H}$-module. Then $\dim \bar{V} = 7 - \delta_{2,p}$ and

$$\bar{V} \downarrow \bar{H} = \begin{cases} \bar{W} \oplus \bar{W}^* & \text{if } q \text{ is even} \\ \bar{W} \oplus \bar{W}^* \oplus 0 & \text{otherwise} \end{cases},$$

where $\bar{W}^*$ denotes the dual of $\bar{W}$ and 0 denotes the trivial $\bar{H}$-module. The result now follows immediately since x acts as the matrix A on $\bar{W}$ and so x acts as A^{-T} on $\bar{W}^*$. $\square$

We now present two technical results on the conjugacy classes of certain prime order elements in exceptional groups of Lie type.

Proposition 5.1.2. *Let $G = G_2(q)$ with $q \geqslant 3$ and for $i \in \{3, 6\}$ let s_i denote a primitive prime divisor of $q^i - 1$. Then G contains at least $\frac{s_i - 1}{6}$ distinct classes of elements of order s_i.*

Proof. The proof for $i = 6$ and $i = 3$ are similar, so we only provide details in the case $i = 6$. We may view G as a subgroup of $\mathrm{GL}(V)$, where V is the minimal module for $G_2(q)$. Let $M = \mathrm{SU}_3(q)$:2, which is a maximal subgroup of G (see [6, Tables 8.30, 8.41 and 8.42], for example). Define $H := \mathrm{SU}_3(q) < M$ with natural module W and take $x \in H$ to be an element of order s_6. The conjugacy of semisimple elements in H of order s_6 is uniquely determined by the set of eigenvalues of the elements acting on the natural

module of H (over the extension field $\mathbb{F}_{q^6}$). By [9, Proposition 3.3.2], there are $(s_6-1)/3$ distinct H-classes of elements of order s_6, each represented by an eigenvalue set $[\Lambda_j]$, where $\Lambda_j = \{\lambda_j, \lambda_j^{q^2}, \lambda_j^{q^4}\}$ and $\lambda_j \in \mathbb{F}_{q^6}$ is an s_6^{th} root of unity (note $\Lambda_j \neq \Lambda_j^{-1}$). Now $M = H.\langle\psi\rangle$, where ψ is an automorphism acting as the inverse-transpose, so the H-classes represented by $[\Lambda_j]$ and $[\Lambda_j^{-1}]$ are fused in M. In particular, there are $(s_6-1)/6$ distinct M-classes of elements of order s_6. By applying Lemma 5.1.1, it follows that there are at least $(s_6-1)/6$ distinct $\mathrm{GL}(V)$-classes of such elements and the result follows. □

Proposition 5.1.3. *Let $G \in \{F_4(q), {}^3D_4(q)\}$ and assume that $q^4-q^2+1 = r$ is prime. Then there are $(q^4-q^2)/\alpha$ distinct G-classes of elements of order r in G, where $\alpha = 4$ if $G = {}^3D_4(q)$ and $\alpha = 12$ if $G = F_4(q)$.*

Proof. We inspect the relevant tables in [25, 75, 76]. First assume $G = {}^3D_4(q)$. As described in [25, Table 2.1] each semisimple class can be represented by a 4-tuple of scalars in an appropriate extension field of $\mathbb{F}_q$. The elements labeled s_{14} are represented by $(t, t^{q^3+1}, t^q, t^{q^2})$ with $t \neq 1$ and $t^{q^4-q^2+1} = 1$. In terms of the notation of the table, these elements have order $q^4-q^2+1 = r$, and by inspecting the table, we conclude that these are the only elements of order r. Then turning to [25, Table 4.4], we see that G contains precisely $\frac{1}{4}(q^4-q^2)$ distinct G-classes of elements of order r. Next let us assume that $G = F_4(q)$ and q is even. Then [75, Table II] shows that the elements labeled h_{76} are the only semisimple elements of order r, and there are $\frac{1}{12}(q^4-q^2)$ such G-classes. Similarly, for $G = F_4(q)$ and q odd, inspection of [76, Tables 8 and 9] shows the required elements are labeled by h_{99} and the result follows. □

5.2 Proof of Theorem 5.1

We begin by handling some small groups with the aid of Magma [5].

Proposition 5.2.1. *Let G be an almost simple group with socle G_0 in the set*

$$\{G_2(3), G_2(4), G_2(5), {}^2F_4(2)', {}^3D_4(2)\}$$

and let H be a core-free subgroup of G, such that $G = G_0H$. Then (G,H) is almost elusive if and only if either

(i) $(G,H) = (G_2(4).2, \mathrm{J}_2.2)$, $({}^2F_4(2), 5^2{:}4S_4)$; *or*

(ii) $(G_0, H \cap G_0) = ({}^2F_4(2)', \mathrm{L}_2(25))$.

Proof. The method for the calculations here is the same as in the proof of Propositions 3.2.2 and 4.2.1. □

We recall that (G, H) is almost elusive only if $\pi(G_0) - \pi(H_0) \leqslant 1$. Thus Theorem 2.5.1 reduces the proof of Theorem 5.1 to the Cases R1, G1-G7, D1-D7, F1 and F1′-F3′ listed in Table B1. In addition, we note that Cases G2-G4, D5-D7 and F1′-F3′ are covered by Proposition 5.2.1.

Proposition 5.2.2. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive permutation group with point stabiliser H and socle G_0 as in Case* R1 *of Table B1. Then G is not almost elusive.*

Proof. Here $G_0 = {}^2G_2(q)$ and $H_0 = 2 \times \mathrm{L}_2(q)$, so $|\Omega| = q^2(q^2 - q + 1)$ and $H_0 = C_{G_0}(x)$ for an involution $x \in G_0$. We are assuming there is a unique primitive prime divisor r of $q^6 - 1$, and we note that every element in G_0 of order r is a derangement (since r divides $|G_0|$ and not $|H_0|$). We observe that there exists an element $y \in G_0$ of order 3 with $|C_{G_0}(y)| = q^3$ (see [64, Table 22.2.7], for example); since $|C_{G_0}(y)|$ is odd, it follows that y does not commute with an involution, so y is a derangement and we conclude that G is not almost elusive. □

In the following proposition we prove Theorem 5.1 for Cases G1, G5-G7 in Table B1. First we remind the reader of our notation for unipotent elements in $\mathrm{GL}(V) = \mathrm{GL}_n(q) = M$, where $q = p^f$ (see Section 4.1.2). Let $x \in M$ be an element of order p. Up to conjugacy, x is a block-diagonal matrix of the form

$$x = [J_p^{a_p}, \ldots, J_1^{a_1}],$$

where J_k is a standard unipotent Jordan block of size k and a_k is its multiplicity (note $n = \sum_{i=1}^{p} i a_i$). In particular, if $x, y \in M$, then x and y are conjugate in M if and only if they have the same Jordan form on V (see [9, Lemma 3.1.14], for example).

Proposition 5.2.3. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive permutation group with point stabiliser H and socle G_0 as in Case* G1*,* G5*,* G6 *or* G7 *in Table B1. Then G is not almost elusive.*

Proof. Here $G_0 = G_2(q)$ and by Proposition 4.2.1 we may assume $q \geqslant 7$. We note that in all cases there exists a unique primitive prime divisor of $q^i - 1$, say r_i, where $i = 6$ for Cases G1 and G5, and $i = 3$ for Cases G6 and G7. We note that r_i is also a primitive prime

divisor of $p^{fi}-1$, so by Lemma 2.4.10 we may write $r_i = ifd_i + 1$, where d_i is a positive integer. Additionally, we note that every element in G_0 of order r_i is a derangement.

By Proposition 5.1.2, G_0 contains at least $ifd_i/6$ conjugacy classes of derangements of order r_i. Since $|\operatorname{Aut}(G_0) : G_0| = (1+\delta_{(3,p)})f$, it follows by Lemma 4.1.1 that G contains at least β distinct classes of derangements of order r_i, where

$$\beta = \begin{cases} id_i/12 & \text{if } p = 3 \\ id_i/6 & \text{otherwise} \end{cases}.$$

By Lemma 2.4.15, $\beta \geqslant 2$ if and only if $(q,i) \neq (8,6),(19,6)$. Thus we conclude G is not almost elusive for Cases G1, G6, G7, and for Case G5 with $q \neq 8, 19$. It remains to handle the final cases for G5, where $H_0 = \mathrm{SL}_3(q)$:2 and $q = 8$ or 19.

Assume first that $q = 19$. Suppose $x \in H_0$ is an element of order 19. Then $x \in \mathrm{SL}_3(q)$ must have Jordan form $[J_2, J_1]$ or $[J_3]$ on the natural 3-dimensional module. Thus by Lemma 5.1.1, x has Jordan form $[J_2^2, J_1^3]$ or $[J_3^2, J_1]$ on the 7-dimensional minimal module V for G_0. By inspecting [55, Table 1], the elements in G_0 of order 19 are in the class labeled $\tilde{A}_1$, and they have Jordan form $[J_3, J_2^2]$ on V. Therefore, G contains derangements of order 19.

Finally assume $q = 8$, so 3 is the unique primitive prime divisor of $q^2 - 1$. By [9, Proposition 3.2.1] there is a unique class of elements of order 3 in H_0. It is easy to check using Magma [5] that there are two distinct classes of elements of order 3 in G_0, so Lemma 2.1.24 implies that G_0 contains derangements of order 3. □

Proposition 5.2.4. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive permutation group with point stabiliser H and socle G_0 in Cases* D1-D4 *in Table B1. Then G is not almost elusive.*

Proof. By Proposition 5.2.1 we may assume $q \geqslant 3$. Here we are assuming $q^4 - q^2 + 1 = r$ is prime and every element in G_0 of order r is a derangement (since r divides $|G_0|$ but not $|H_0|$). By Proposition 5.1.3 there are $(q^4-q^2)/4$ distinct G_0-classes of derangements of order r in G_0. Since $|\operatorname{Aut}(G_0) : G_0| = 3f$, by Lemma 4.1.1 there are at least $(q^4-q^2)/12f$ distinct G-classes of derangements of order r. It is easy to check that $(q^4-q^2)/12f \geqslant 2$ for all $q \geqslant 3$. □

Proposition 5.2.5. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive permutation group with point stabiliser H and socle G_0 in Case* F1 *in Table B1. Then G is not almost elusive.*

Proof. Here $G_0 = F_4(q)$, $H_0 = (2, q-1).\Omega_9(q)$ and we may assume that G contains no graph automorphisms by [61] (also see [24, Tables 7.1 and 7.2]). For $q = 2$ we proceed as in the proof of Proposition 5.2.1, so we may assume $q \geqslant 3$. The conditions for case F1 imply that $q^4 - q^2 + 1 = r$ is a prime and thus any element in G_0 of order r is a derangement. By Proposition 5.1.3 there are $(q^4 - q^2)/12$ distinct G_0-classes of elements of order r in G_0. Since $|G : G_0| \leqslant f$, there are at least $(q^4 - q^2)/12f \geqslant 2$ distinct G-classes of derangements. The result follows. □

This completes the proof of Theorem 5.1 for the primitive cases. In particular, by Lemmas 2.1.29 and 2.1.30, this completes the proof of Theorem 5.1 for all quasiprimitive groups.

CHAPTER

6

AFFINE GROUPS

We recall that Theorem 2.2.1 shows that a finite quasiprimitive permutation group is almost elusive only if it is almost simple or a 2-transitive affine group. Here we prove Theorems 1 and 2 for the affine groups. We begin by recalling the definition of an affine group.

Let p be a prime and let $V = (\mathbb{F}_p)^d$ be a d-dimensional vector space over $\mathbb{F}_p$. An *affine transformation* of V is a map $t_{h,v} : V \longrightarrow V$ with $h \in \mathrm{GL}(V)$ and $v \in V$ such that $t_{h,v}(u) := hu + v$. These affine transformations form the *affine general linear group*, which is denoted $\mathrm{AGL}(V)$ or $\mathrm{AGL}_d(p)$, which we can view as a permutation group on V. The socle of $\mathrm{AGL}(V)$ may be identified with the additive group of V, which is isomorphic to $(C_p)^d$, and we say G is an *affine permutation group* if

$$V \trianglelefteqslant G = V{:}H \leqslant \mathrm{AGL}(V),$$

where $H \leqslant \mathrm{GL}(V)$ is the stabiliser of the zero vector in V.

Our main theorem is Theorem 6.1. In part (iii) we write $\mathcal{P}(n, i)$ for the i^{th} primitive group of degree n in the *Database of Primitive Groups* in Magma [5]. For example, $\mathcal{P}(2^4, 17) = 2^4{:}\mathrm{Sp}_4(2)'$. Additionally, we write $\Gamma\mathrm{L}_m(q)$ for the general semilinear group of dimension m over $\mathbb{F}_q$, where q is a p-power. We remind the reader that, unless stated otherwise, we assume that all groups are finite.

Theorem 6.1. *Let $G = V{:}H \leqslant \mathrm{AGL}(V)$ be a quasiprimitive affine permutation group of degree $|V| = n = p^d$, with p prime and $d \geqslant 1$. Then G is almost elusive if and only if G is 2-transitive and one of the following holds:*

(i) $H \leqslant \Gamma\mathrm{L}_1(p^d)$.

(ii) $\mathrm{SL}_2(q) \trianglelefteqslant H \leqslant \Gamma\mathrm{L}_2(q)$, *where $p = 2$, d is even and $q = 2^{d/2}$.*

(iii) $G = \mathcal{P}(n, i)$, *where (n, i) is contained in Table P3.*

Assume that the hypothesis of Theorem 6.1 holds. If $H \leqslant \Gamma\mathrm{L}_1(p^d)$, then the exact structure of the 2-transitive groups can be found in [47, Theorem XII.7.3]. Additionally, if $\mathrm{SL}_2(q) \trianglelefteqslant H \leqslant \Gamma\mathrm{L}_2(q)$, then G is always 2-transitive (see [26, pg. 55]).

We note that an affine group G is quasiprimitive if and only if H is an irreducible subgroup of $\mathrm{GL}(V)$ (hence, every quasiprimitive affine group is primitive). In addition, Theorem 2.2.1 implies that a primitive affine group G is almost elusive only if G is 2-transitive, so the proof for Theorem 2 is trivial in the affine case. Hence, for the remainder of this chapter, we will assume that $G = V{:}H \leqslant \mathrm{AGL}(V)$ is a 2-transitive affine group and we will use (v, h) to denote the elements of G where $v \in V$ and $h \in H$. The content of this chapter is taken from [45, Section 3].

6.1 Preliminaries

Throughout this section we let $V^* = V \setminus \{0\}$. We begin by discussing the prime order derangements in affine groups. Note that $|V| = p^d$, so every prime order derangement has order p. Any element of the form $(v, 1) \in G$ such that $v \in V^*$ is a derangement of order p, since it acts as a translation by v on V. Additionally, every element in H has fixed points. In fact, we can precisely determine when an element of G is a prime order derangement.

Lemma 6.1.1. *An element $(v, h) \in G$ is a derangement of order p if and only if all the following conditions are satisfied:*

(i) $h^p = 1$,

(ii) $v \in \ker(h^{p-1} + \cdots + h + 1)$,

(iii) $v \notin \mathrm{im}(h - 1)$.

Proof. Let $g = (v, h)$ be a nontrivial element of G. Since G acts on V via affine transformations it is easy to see that g is a derangement if and only if $u \neq hu + v$ for all $u \in V$.

Table 6.1: Groups arising in Hering's Theorem.

	n	H	Conditions
I	p^d	$H \leqslant \Gamma\mathrm{L}_1(p^d)$	
II	q^a	$\mathrm{SL}_a(q) \trianglelefteqslant H \leqslant \Gamma\mathrm{L}_a(q)$	$a \geqslant 2$
III	q^a	$\mathrm{Sp}_a(q) \trianglelefteqslant H$	$a \geqslant 4$ even
IV	q^6	$\mathrm{G}_2(q)' \trianglelefteqslant H$	q even
V	$5^2, 7^2, 11^2, 23^2$	$\mathrm{SL}_2(3) \trianglelefteqslant H$	
VI	3^4	$2^{1+4} \trianglelefteqslant H$	
VII	$3^4, 11^2, 19^2, 29^2, 59^2$	$\mathrm{SL}_2(5) \trianglelefteqslant H$	
VIII	2^4	A_6, A_7	
IX	3^6	$\mathrm{SL}_2(13)$	

That is $v \notin \mathrm{im}(h-1)$. Now, $g^p = (v + hv + h^2v + \cdots + h^{p-1}v, h^p)$, so g has order p if and only if $h^p = 1$ and $(h^{p-1} + \cdots + h + 1)(v) = 0$, where $h^{p-1} + \cdots + h + 1 \in \mathrm{Hom}(V, V)$. That is, $v \in \ker(h^{p-1} + \cdots + h + 1)$. The result follows. □

The 2-transitive affine groups have been determined by Hering [46]. Other convenient sources for this result are [57, Appendix 1] and [17, Section 7.3].

Theorem 6.1.2 (Hering's Theorem)**.** *Let $G = V{:}H$ be a 2-transitive affine group of degree $n = p^d$. Then (n, H) is one of the cases in Table 6.1.*

For the remainder of Section 6.1 we will establish some results regarding the Jordan form of elements of order p in H. We note that will use the same notation for Jordan form as described in Section 4.1.2. These results will be particularly useful when H belongs to one of the infinite families in Hering's Theorem (see cases I-IV in Table 6.1). For these infinite families we show that there are no almost elusive examples for cases III and IV in Hering's Theorem (see Propositions 6.2.4 and 6.2.5), but that there do exist almost elusive groups for cases I and II (see Propositions 6.2.2 and 6.2.3). Note that every subgroup appearing in II of Table 6.1 is 2-transitive (see [26, pg. 55]), and detailed information on the exact structure of the 2-transitive groups in case I can be found in [47, Theorem XII.7.3]. Additionally, for the groups in cases V-IX we use computational methods in Magma, see Proposition 6.2.1.

Proposition 6.1.3. *Let $h \in H$ be an element of order p with Jordan form $[J_p^{a_p}, \ldots, J_1^{a_1}]$*

on V. Then there exists an element $v \in V^*$ such that $(v, h) \in G$ is a derangement of order p if and only if $a_i > 0$ for some $1 \leqslant i \leqslant p-1$.

Proof. Fix an $\mathbb{F}_p$-basis $\{v_1, \ldots, v_d\}$ of V such that $h = [J_p^{a_p}, \ldots, J_1^{a_1}]$. By Lemma 6.1.1, there exists a $v \in V^*$ such that $(v, h) \in G$ is a derangement of order p if and only if there exists a $v \in V^*$ such that $v \in \ker(h^{p-1} + \cdots + h + 1)$ and $v \notin \mathrm{im}(h-1)$.

We note that we can write any $v \in V^*$ as $v = c_1 v_1 + \cdots + c_d v_d$ for some $c_1, \ldots, c_d \in \mathbb{F}_p$, and that $h^i = [(J_p^i)^{a_p}, \ldots, (J_1^i)^{a_1}]$, with

$$J_k^i = \begin{pmatrix} 1 & \binom{i}{1} & \binom{i}{2} & \cdots & \binom{i}{k-1} \\ 0 & 1 & \binom{i}{1} & \cdots & \binom{i}{k-2} \\ 0 & 0 & 1 & \cdots & \binom{i}{k-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix},$$

where we take $\binom{a}{b} = 0$ if $a < b$ or $b \leqslant 0$.

Since $\sum_{i=t}^{p-1} \binom{i}{t} = \binom{p}{t+1}$ is divisible by p for all $1 \leqslant t \leqslant p-2$, it is easy to show that $v \in \ker(h^{p-1} + \cdots + h + 1)$ if and only if either $a_p = 0$, or $c_{kp} = 0$ for all $1 \leqslant k \leqslant a_p$. Similarly, $v \in \mathrm{im}(h-1)$ if and only if for all $1 \leqslant i \leqslant p$ either $a_i = 0$, or $c_{ki+t} = 0$ for all $1 \leqslant k \leqslant a_i$, where

$$t = \begin{cases} \sum_{j=i+1}^{p} a_j j & \text{if } i < p \\ 0 & \text{if } i = p \end{cases}.$$

Thus it is clear to see that $\ker(h^{p-1} + \cdots + h + 1) \geqslant \mathrm{im}(h-1)$ with equality if and only if $a_i = 0$ for all $1 \leqslant i \leqslant p-1$. That is there exists $v \in V^*$ such that $v \in \ker(h^{p-1} + \cdots + h + 1)$ and $v \notin \mathrm{im}(h-1)$ if and only if $a_i > 0$ for some $1 \leqslant i \leqslant p-1$. Thus the result follows. □

Corollary 6.1.4. *Let $G = V{:}H$ be a 2-transitive affine group of degree p^d. Then G is almost elusive if and only if one of the following holds:*

(i) *$|H|$ is indivisible by p; or*

(ii) *Both $|H|$ and d are divisible by p, and every $h \in H$ of order p has Jordan form $[J_p^{d/p}]$ on V.*

Next we briefly discuss the embedding of $\mathrm{GL}_{d/k}(q^k)$ in $\mathrm{GL}_d(q)$, where $k \geqslant 1$ is a divisor of d. Let $V_\#$ be a d/k-dimensional vector space over $\mathbb{F}_{q^k}$. Then we may view $V_\#$ as a d-dimensional vector space V over $\mathbb{F}_q$. Additionally, any $\mathbb{F}_{q^k}$-linear transformation of $V_\#$ is

also an $\mathbb{F}_q$-linear transformation of V, which yields an embedding of $\mathrm{GL}_{d/k}(q^k)$ in $\mathrm{GL}_d(q)$. We state the following lemma, which is a direct consequence of the normal basis theorem (see, for instance, [56, Theorem 2.35]).

Lemma 6.1.5. *Let d and k be positive integers, such that k divides d. Consider the vector spaces $V = (\mathbb{F}_q)^d$ and $V_\# = (\mathbb{F}_{q^k})^{d/k}$, where $q = p^f$ with p prime and $f \geqslant 1$. Fix an $\mathbb{F}_{q^k}$-basis $\{v_1, \ldots, v_{d/k}\}$ of $V_\#$. Then there exists a scalar $\lambda \in \mathbb{F}_{q^k} \setminus \mathbb{F}_q$ such that*

$$\{\lambda v_1, \lambda^q v_1, \ldots\ldots, \lambda^{q^{k-1}} v_1, \ldots, \lambda v_{d/k}, \lambda^q v_{d/k}, \ldots, \lambda^{q^{k-1}} v_{d/k}\}$$

is an $\mathbb{F}_q$-basis for V.

The following result is [9, Lemma 5.3.2].

Lemma 6.1.6. *Let d and k be positive integers, such that k divides d. Let $h \in \mathrm{GL}_{d/k}(p^k)$ be an element of order p with Jordan form $[J_p^{a_p}, \ldots, J_1^{a_1}]$ on $V_\# = (\mathbb{F}_{p^k})^{d/k}$. Then h has Jordan form $[J_p^{ka_p}, \ldots, J_1^{ka_1}]$ on $V = (\mathbb{F}_p)^d$.*

Proof. Fix an $\mathbb{F}_{p^k}$-basis $\{v_1, \ldots, v_{d/k}\}$ of $V_\#$ such that $h = [J_p^{a_p}, \ldots, J_1^{a_1}] \in \mathrm{GL}_{d/k}(p^k)$. Then by Lemma 6.1.5 there is an $\mathbb{F}_p$-basis for V,

$$\beta = \{\lambda v_1, \lambda^p v_1, \ldots\ldots, \lambda^{p^{k-1}} v_1, \ldots, \lambda v_{d/k}, \lambda^p v_{d/k}, \ldots, \lambda^{p^{k-1}} v_{d/k}\},$$

such that $\lambda \in \mathbb{F}_{p^k} \setminus \mathbb{F}_p$. Since we know how h acts on the basis vectors in $\{v_1, \ldots, v_{d/k}\}$ and h is linear over $\mathbb{F}_{p^k}$, it is easy to see how h acts on the basis vectors in β. Then with respect to an appropriate ordering of the basis β, we have $h = [J_p^{ka_p}, \ldots, J_1^{ka_1}]$ as required. □

The final results of this preliminary section concern the general semilinear group. We begin by discussing the structure of this group. Let d and k be positive integers and fix a prime p. Let $\{u_1, \ldots, u_d\}$ be a basis for the natural module $U = (\mathbb{F}_{p^k})^d$ of $\mathrm{GL}_d(p^k)$. We can define a map, $\gamma : U \to U$, where

$$\gamma : \sum_i \lambda_i u_i \mapsto \sum_i \lambda_i^p u_i.$$

Then γ induces a field automorphism, $\phi : \mathrm{GL}_d(p^k) \to \mathrm{GL}_d(p^k)$, where $(a_{ij})^\phi = (a_{ij}^p)$ for all $(a_{ij}) \in \mathrm{GL}_d(p^k)$. The general semilinear group is defined to be $\Gamma\mathrm{L}_d(p^k) = \mathrm{GL}_d(p^k){:}\langle\phi\rangle$ and we write the elements of $\Gamma\mathrm{L}_d(p^k)$ as (g, ϕ^l) where $g \in \mathrm{GL}_d(p^k)$ and $\phi^l \in \langle\phi\rangle$. We refer to the map ϕ as a standard field automorphism of order k in $\mathrm{GL}_d(p^k)$. In general, we say an element in $\Gamma\mathrm{L}_d(p^k)\backslash\mathrm{GL}_d(p^k)$ is a field automorphism and note that they have the form

(g, ϕ^l) such that $1 \leqslant l \leqslant k-1$. Additionally, we recall that if k divides d then $\mathrm{GL}_{d/k}(p^k)$ embeds in $\mathrm{GL}_d(p)$. Therefore since the map γ acts as an $\mathbb{F}_p$-linear map, $\Gamma\mathrm{L}_{d/k}(p^k)$ embeds in $\mathrm{GL}_d(p)$.

Lemma 6.1.7. *Let $G = \Gamma\mathrm{L}_{d/k}(p^k)$ where p is a prime and $k = pf$ for some $f \geqslant 1$. Let $x = (1, \psi) \in G$ be an element of order p. Then x has Jordan form $[J_p^{d/p}]$ on V.*

Proof. We begin by noting that the standard field automorphism ϕ has order $k = pf$ and so $\psi = \phi^{if}$ for some $1 \leqslant i \leqslant p-1$. Fix an $\mathbb{F}_{p^k}$-basis $\{v_1, \ldots, v_{d/k}\}$ for $V_\# = (\mathbb{F}_{p^k})^{d/k}$, such that it is compatible with ϕ as in the discussion above. By Lemma 6.1.5 there is an $\mathbb{F}_p$-basis for V,

$$\beta = \{\lambda v_1, \lambda^p v_1, \ldots, \lambda^{p^{k-1}} v_1, \ldots, \lambda v_{d/k}, \lambda^p v_{d/k}, \ldots, \lambda^{p^{k-1}} v_{d/k}\}$$

such that $\lambda \in \mathbb{F}_{p^k} \backslash \mathbb{F}_p$. Note that ψ acts on the vectors of β as follows, $\psi(\lambda^{p^l} v_m) = \lambda^{p^{l+if}} v_m$ for all $0 \leqslant l \leqslant k-1$ and $1 \leqslant m \leqslant d/k$. We can partition the set β into d/k sets of size k, namely the sets $\{\lambda v_1, \lambda^p v_1, \ldots \lambda^{p^{k-1}} v_1\}, \ldots, \{\lambda v_{d/k}, \lambda^p v_{d/k}, \ldots \lambda^{p^{k-1}} v_{d/k}\}$. On each of these d/k sets ψ acts as f disjoint p-cycles. For example, on the first set an example of such a p-cycle is $(\lambda v_1, \lambda^{p^{if}} v_1, \ldots, \lambda^{p^{(p-1)if}} v_1)$. Thus ψ acts on β as a product of d/p disjoint p-cycles. It then follows that $(1, \psi)$ has Jordan form $[J_p^{d/p}]$ on V. □

We are now in a position to state results regarding the Jordan form of field automorphisms of order p in the general semilinear group $\Gamma\mathrm{L}_{d/k}(p^k)$. We remind the reader that for positive integers a and b, we use the notation (a, b) to denote the greatest common divisor of a and b.

Lemma 6.1.8. *Let d be a positive integer and let p be a prime divisor of d. Let $x \in \Gamma\mathrm{L}_1(p^d)$ be a field automorphism of order p. Then x has Jordan form $[J_p^{d/p}]$ on $V = (\mathbb{F}_p)^d$.*

Proof. Recall $H = \Gamma\mathrm{L}_1(p^d) = \mathrm{GL}_1(p^d){:}\langle\phi\rangle$, where ϕ is the standard field automorphism of order d. We write $x = (a, \psi)$ where $a \in \mathrm{GL}_1(p^d)$ and $\psi = \phi^j$ for some integer $1 \leqslant j < d$. Additionally we write $d = pk$ for some $k \geqslant 1$. Since x has order p, this implies that ψ has order p and $a\psi(a) \ldots \psi^{p-1}(a) = 1$. In particular, $j = ik$ with $1 \leqslant i \leqslant p-1$.

We claim that x is H-conjugate to $(1, \psi)$ and so the result follows from Lemma 6.1.7. In order to prove this claim we first note that an element $(b, \phi^t) \in H$ is H-conjugate to $(1, \psi)$ only if $\phi^t = \psi$. Thus we proceed by showing that $|(1, \psi)^H|$ is equal to the number of order p elements in H of the form (b, ψ).

We recall that $(b, \psi) \in H$ has order p if and only if

$$b\psi(b)\dots\psi^{p-1}(b) = b\phi^{ik}(b)\dots\phi^{(p-1)ik}(b) = 1.$$

Using Lemma 2.4.4 we can show that for each $1 \leqslant z \leqslant p-1$ there exists a unique $1 \leqslant y \leqslant p-1$ such that $zik \equiv yk \pmod{d}$. Thus since ϕ has order d the equation above is exactly equivalent to

$$b\phi^{k}(b)\dots\phi^{(p-1)k}(b) = b^{1+p^k+\dots+p^{(p-1)k}} = 1.$$

Since $\mathrm{GL}_1(p^d)$ is a cyclic group of order p^d-1 there are

$$(p^d-1, 1+p^k+\dots+p^{(p-1)k}) = 1+p^k+\dots+p^{(p-1)k}$$

many elements $b \in \mathrm{GL}_1(p^d)$ such that (b, ψ) has order p.

An element $(b, \phi^t) \in C_H((1,\psi))$ if and only if $b = \psi(b)$ which is equivalent to $b^{p^{ik}-1} = 1$. There are exactly $(p^d-1, p^{ik}-1) = p^k-1$ such elements $b \in \mathrm{GL}_1(p^d)$. Thus $|C_H((1,\psi))| = (p^k-1)d$, so

$$|(1,\psi)^H| = (p^d-1)d/(p^k-1)d = 1+p^k+\dots+p^{(p-1)k},$$

and the claim follows. The result now follows by applying Lemma 6.1.7. □

Lemma 6.1.9. *Let p, k and d be integers such that p is a prime, d is divisible by k with $d/k \geqslant 2$ and k is divisible by p. Let $x \in \Gamma\mathrm{L}_{d/k}(p^k)$ be a field automorphism of order p. Then x has Jordan form $[J_p^{d/p}]$ on $V = (\mathbb{F}_p)^d$.*

Proof. Let ϕ denote the standard field automorphism of order p in $\Gamma\mathrm{L}_{d/k}(p^k)$. We note that all field automorphisms of order p are contained in a coset $\mathrm{GL}_{d/k}(p^k)\phi^i$ for some $1 \leqslant i \leqslant p-1$. Thus $x \in \mathrm{GL}_{d/k}(p^k)\sigma$, where $\sigma = \phi^i$ for some $1 \leqslant i \leqslant p-1$. By the theory of Shintani descent (see [12, Section 3.4] for more details for example) there is a bijective correspondence between the set of $\mathrm{GL}_{d/k}(p^k)$:$\langle\sigma\rangle$-classes in the coset $\mathrm{GL}_{d/k}(p^k)\sigma$ and the set of conjugacy classes in $\mathrm{GL}_{d/k}(p^{k/p})$. In particular, the classes of elements of order p in $\mathrm{GL}_{d/k}(p^k)\sigma$ correspond to classes of elements of order 1 in $\mathrm{GL}_{d/k}(p^{k/p})$ (see [12, Lemma 3.20] for a proof of this). We conclude there is a unique $\mathrm{GL}_{d/k}(p^k)$:$\langle\sigma\rangle$-class of elements of order p in $\Gamma\mathrm{L}_{d/k}(p^k)$. Therefore we may assume that $x = (1,\sigma) = (1,\phi^i)$, so by Lemma 6.1.7 the result follows. □

6.2 Proof of Theorem 6.1

We now turn to the proof of Theorem 6.1. We remind the reader of the notation we will use throughout this section: $G = V{:}H \leqslant \mathrm{AGL}(V)$ with $V = (\mathbb{F}_p)^d$ and H is an irreducible subgroup of $\mathrm{GL}(V)$. Additionally, we recall that we may also assume that G is 2-transitive. Thus we approach the proof by inspecting the cases in Hering's Theorem (see Theorem 6.1.2 and Table 6.1).

Proposition 6.2.1. *Theorem 6.1 holds for G as in Cases V-IX of Table 6.1.*

Proof. This is a simple calculation using the *Database of Primitive Groups* in Magma [5], which records the primitive groups up to degree 4095. The command `PrimitiveGroups` outputs the groups with our desired degree. We can then use the `Classes` command to obtain all the conjugacy classes in G of elements of prime order. Using the `Fix` command, which outputs the set of fixed points of an element of our group, for each G-class we can find the number of fixed points of the element. If there is a unique G-class of elements of prime order with no fixed points then we conclude the group is almost elusive. □

It now remains to handle the infinite families in Hering's theorem, namely cases I-IV in Table 6.1. We recall that the non-zero vectors in V form a single class of derangements of order p. Thus G is almost elusive if there exist no derangements of the form $(v, h) \in G$, where both v and h are nontrivial.

Proposition 6.2.2. *Assume G is a 2-transitive group as in Case I of Table 6.1. Then G is almost elusive.*

Proof. Here $n = p^d$ and $H \leqslant \Gamma\mathrm{L}_1(p^d) = \mathrm{GL}_1(p^d){:}d \leqslant \mathrm{GL}_d(p)$. If p does not divide d, then p does not divide $|H|$ and thus G is almost elusive by Lemma 6.1.1. Now assume that p divides d. Any element of order p in $\Gamma\mathrm{L}_1(p^d)$ must be a field automorphism, so the result follows by Lemma 6.1.8 and Corollary 6.1.4. □

Proposition 6.2.3. *Assume G is as in Case II of Table 6.1. Then G is almost elusive if and only if $p = a = 2$.*

Proof. Here $\mathrm{SL}_a(q) \trianglelefteq H \leqslant \Gamma\mathrm{L}_a(q)$ and $n = p^d = q^a$ with $a \geqslant 2$. We recall that $\Gamma\mathrm{L}_a(q) = \Gamma\mathrm{L}_{d/k}(p^k) < \mathrm{GL}_d(p)$, where $k = d/a$. Define $V_\# = (\mathbb{F}_q)^a$, an a-dimensional vector space over $\mathbb{F}_q$ (the natural module of $\mathrm{GL}_a(q)$). Assume first that $a \geqslant 3$ and take $h \in \mathrm{SL}_a(q) \leqslant H$ to be an element of order p with Jordan form $[J_2, J_1^{a-2}]$ on $V_\#$. Then by Lemma 6.1.6, h

has Jordan form $[J_2^k, J_1^{k(a-2)}]$ on V. Thus Corollary 6.1.4 implies G is not almost elusive. Finally assume that $a = 2$. Take $h \in \mathrm{GL}_2(q)$ to be an element of order p. Then h has Jordan form $[J_2]$ on $V_\#$ and $[J_2^{d/2}]$ on V. Suppose first $p \geqslant 3$. Then G is not almost elusive by Corollary 6.1.4. Finally suppose $p = 2$. Then using Lemma 6.1.9 we see that every element of order 2 in $\Gamma\mathrm{L}_2(q)$ has Jordan form $[J_2^{d/2}]$ on V. Thus the result follows by Corollary 6.1.4. □

Proposition 6.2.4. *Assume G is as in Case III of Table 6.1. Then G is not almost elusive.*

Proof. In this case $\mathrm{Sp}_a(q) \trianglelefteqslant H$ and $p^d = q^a$ with $a \geqslant 4$ even. Define $V_\# = (\mathbb{F}_q)^{a/2}$ and let $h \in \mathrm{Sp}_a(q)$ be an element of order p with Jordan form $[J_2, J_1^{a-2}]$ on $V_\#$. Then h has Jordan form $[J_2^k, J_1^{k(a-2)}]$ on V, where $d = ak$. Thus by Corollary 6.1.4, G is not almost elusive. □

Proposition 6.2.5. *Assume G is as in Case IV of Table 6.1. Then G is not almost elusive.*

Proof. Here $p = 2$ and $G_2(q)' \trianglelefteqslant H$ with $2^d = q^6$. We note that we can handle the case $d = 6$ easily in Magma using the same method outlined in the proof of Proposition 6.2.1. Thus we may assume that $d \geqslant 12$ and $G_2(q) \trianglelefteqslant H$.

Note that $\mathrm{SL}_3(q)$:2 is a maximal subgroup of $G_2(q)$ (see [6, Table 8.30] for example). Let W denote the natural $\mathrm{SL}_3(q)$ module and let $V_\# = (\mathbb{F}_q)^6$ denote the minimal module of $G_2(q)$ over $\mathbb{F}_q$. Take $h \in \mathrm{SL}_3(q) \leqslant H$ to be an element of order 2 with Jordan form $[J_2, J_1]$ on W. Then by Lemma 5.1.1, h has Jordan form $[J_2^2, J_1^2]$ on $V_\#$ and thus h has Jordan form $[J_2^{d/3}, J_1^{d/3}]$ on V. Therefore Corollary 6.1.4 implies that G is not almost elusive. □

In view of Propositions 6.2.1 - 6.2.5, the proof of Theorem 6.1 is complete.

CHAPTER

7

CONCLUSIONS AND FUTURE DIRECTIONS

In this penultimate chapter we finalise the proofs of our main results (Theorems 1 and 2), and we provide proofs of Corollaries 3 and 4. We also briefly discuss some further research directions relating to the topic of this thesis.

7.1 Proof of the main results

We begin by noting that the proofs of Theorems 1 and 2 have now been completed. Here we provide a helpful guide to the proofs.

- For Theorem 1, we combine the following results
  - Theorem 2.2.1 (the reduction to almost simple and 2-transitive affine groups)
  - Theorem 3.1 (alternating groups)
  - Theorem 3.3 (sporadic groups)
  - Theorem 4.1 (classical groups)
  - Theorem 5.1 (exceptional groups)

  - Theorem 6.1 (affine groups)

- For Theorem 2, we combine the following results
  - Theorem 2.2.1 (the reduction to almost simple and 2-transitive affine groups)
  - Theorem 3.2 (alternating groups)
  - Theorem 3.3 (sporadic groups)
  - Theorem 4.2 (classical groups)
  - Theorem 5.1 (exceptional groups)

(Note that every quasiprimitive affine group is primitive.) We note that the proofs of Corollaries 3 and 4 can be found in [45, Section 5].

7.1.1 Proof of Corollary 3

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a quasiprimitive almost elusive permutation group with socle G_0 and point stabiliser H. Assume that G has derangements of prime order s. Here we prove that either s is the largest prime divisor of $|\Omega|$ or it is one of the cases outlined in the statement of Corollary 3.

The result for affine groups is trivial. Thus in view of Theorems 1 and 2 we may assume that G is an almost simple group such that (G, H) is one of the cases recorded in Tables P1, P2, Q1 or Q2 . The cases in Table P2 and Q2 can be handled easily using computational methods in Magma [5] to calculate the degree of G. Thus it remains to handle the cases in Tables P1 and Q1. Let s be the order of the elements in the unique G-class of derangements of prime order.

Suppose (G, H) is recorded in Table P1. The proof is similar in all cases so we will only show the details for Cases 1, 4 and 7 (we note that we use [54, Chapters 3 and 4] for the orders of the classical groups).

First assume (G, H) is as in Case 1 in Table P1. Here $G = \mathrm{U}_n(q).[2f]$ such that $q = 2^f$ is even, $n \geqslant 5$ is a prime divisor of $q + 1$ and $s = 2nf + 1$ is the unique primitive prime divisor of $q^{2n} - 1$. Additionally, H is the stabiliser of a 1-dimensional non-degenerate subspace of the natural module. By [54, Proposition 4.1.4] we have

$$|G_0| = \frac{1}{n} q^{n(n-1)/2} \prod_{i=2}^{n} (q^i - (-1)^i) \text{ and } |H_0| = \frac{1}{n} q^{(n-1)(n-2)/2} \prod_{i=1}^{n-1} (q^i - (-1)^i).$$

Since s is the unique primitive prime divisor of $q^{2n} - 1$, by Remark 2.4.17 we deduce that

$$|\Omega| = q^{n-1} \frac{q^n + 1}{q + 1} = q^{n-1}.n.s^l$$

for some $l \geqslant 1$. Thus the result follows since $s = 2nf + 1 > n$.

Next assume that (G, H) is as in Case 4 of Table P1. Then $G = \mathrm{PGL}_2(p)$ and $H = D_{2(p-1)}$ where $s = p = 2^m - 1$ is a Mersenne prime. Here $|G| = 2^m p(p-1)$ and $|H| = 2(p-1)$. Thus $|\Omega| = 2^{m-1}p$. The result follows since $p \geqslant 7$. Finally let us assume that (G, H) is as in Case 7 of Table P1. Then $G = S_n$ and $H = S_{n-2} \times S_2$ with $n = 2^m = s + 1$. Thus $|\Omega| = (n(n-1))/2 = 2^{m-1}s$. The result follows since $s > 2$.

Finally suppose that (G, H) is recorded in Table Q1. Assume first that (G, H) is as in Case II or III. Then $G = \mathrm{L}_2(p)$ or $\mathrm{PGL}_2(p)$ with $p = 2^m - 1$ a Mersenne prime and $H = C_p{:}C_d$, where d is a proper divisor of $k(p-1)/2$ and $\alpha(d) = \alpha(k(p-1)/2)$ with $k = |G : G_0|$. Here $s = 2$ and $|\Omega| = 2^{m-1}k(p-1)/d$. Thus 2 is not the largest prime divisor of $|\Omega|$ since $(p-1)/d$ is divisible by an odd prime. Next assume that (G, H) is as in Case I. Then $G = \mathrm{PGL}_2(p)$ where $s = p = 2^m + \epsilon$ is a prime and $\epsilon = \pm 1$. Additionally, $H = D_{2d}$ where d is a proper divisor of $p + \epsilon$ and $\alpha(d) = \alpha(p + \epsilon)$. Thus $|\Omega| = 2^{m-1}p(p + \epsilon)/d$. Since all prime divisors of $p + \epsilon$ must be less than p we conclude that p is the largest prime divisor of $|\Omega|$. Finally assume that (G, H) is as in Case IV. Here $G = \mathrm{L}_2(p)$ where $p = 2.3^a - 1$ is a prime such that $a \geqslant 2$ and $H = C_p{:}C_d$ such that d is a proper divisor of $(p-1)/2$ and $\alpha(d) = \alpha((p-1)/2)$. In this case $s = 3$ and $|\Omega| = 3^a.(p-1)/d$. Thus it is clear to see that 3 is not the largest prime divisor of $|\Omega|$ if and only if $(p-1)/d$ has an odd prime divisor. □

7.1.2 Proof of Corollary 4

Let G be an almost simple group with socle G_0 and let H be a core-free subgroup of G such that $G = G_0H$ and (G, H) is almost elusive. We begin by recalling the set up of Corollary 4.

We define the *depth of* H, denoted $d_G(H)$, to be the longest possible chain of subgroups

$$G > L_1 > \cdots > L_{\ell-1} > L_\ell = H, \tag{7.1}$$

such that (G, L_i) is almost elusive for all $1 \leqslant i \leqslant \ell$. Here we refer to ℓ as the length of the chain in (7.1). We define the *almost elusive depth* of G to be

$$D_G = \max d_G(H)$$

where we take the maximum over all core-free subgroups H of G such that $G = G_0H$ and (G, H) is almost elusive. Additionally we remind the reader that we use $\omega(n)$ and $\pi(n)$ to

denote the total number of prime divisors and the number of distinct prime divisors of a positive integer n, respectively.

Here we aim to describe D_G for $D_G \geqslant 2$. In view of Theorem 2, we may assume that G is one of the groups recorded in Table Q1 or Q2.

First consider the cases in Table Q2. In each case we can use MAGMA to compute D_G precisely, applying similar techniques used in the proof of Proposition 4.3.2. Finally let us assume G is one of the groups in Table Q1. The analysis of these cases is very similar, so we only provide details when $G = \mathrm{PGL}_2(p)$ and $p = 2^m - 1$ is a Mersenne prime. In this case (G, H) is almost elusive only if $H = D_{2d}$ or $C_p{:}C_d$, where d is a proper divisor of $p-1$ and $\alpha(d) = \alpha(p-1)$. In both cases, it is easy to see that

$$d_G(H) = \omega(p-1) - \omega(d) + 1.$$

For example, take $H = C_p{:}C_d < M = C_p{:}C_{p-1}$, where M is a Borel subgroup of G. We can compute the depth of H by constructing a chain of subgroups starting with M and then repeatedly taking prime index subgroups, where each subgroup in the chain is of the form $C_p{:}C_t$, where t is a proper divisor of $p-1$ and $\alpha(t) = \alpha(p-1)$. Thus

$$D_G = \max d_G(H) = d_G(D_{2e}) = d_G(C_p{:}C_e)$$

where e is the product of the distinct prime divisors of $p-1$. That is $\omega(e) = \pi(p-1)$, and we conclude that $D_G = \omega(p-1) - \pi(p-1) + 1$ as in part (ii) of the corollary. □

7.2 Future research directions

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group of a finite set Ω. We will use $\mathcal{K}_{pr}(G)$ to denote the number of conjugacy classes of derangements of prime order in G. Additionally we define $\beta_{pr}(G)$ to be the set of primes r such that G contains a derangement of order r in G.

7.2.1 k-almost elusive groups

There is a very natural way to extend the concept of almost elusivity. For $k \geqslant 1$, we say that G is *k-almost elusive* if it has exactly k conjugacy classes of derangements of prime order (i.e $\mathcal{K}_{pr}(G) = k$).

Problem 7.2.1. *For $k \geqslant 1$, can we classify the k-almost elusive quasiprimitive permutation groups?*

In this thesis we have completed the classification of the quasiprimitive 1-almost elusive groups, but the analogous problem for $k \geqslant 2$ seems to be far more complicated, mainly due to hard number-theoretic problems that arise. We can divide Problem 7.2.1 into two subproblems:

Problem 7.2.2. *For $k \geqslant 2$, can we classify the k-almost elusive quasiprimitive permutation groups with $|\beta_{pr}(G)| = 1$.*

Problem 7.2.3. *For $k \geqslant 2$, can we classify the k-almost elusive quasiprimitive permutation groups with $|\beta_{pr}(G)| \geqslant 2$.*

Here we will use examples to exhibit some of the difficulties that arise here.

Example 7.2.4. Take $G = S_n$ or A_n acting on the set of 2-element subsets of $\{1, \ldots, n\}$ with $n \geqslant 6$ even. Then $x \in G$ is a derangement of prime order if and only if it has cycle shape $[r^{n/r}]$ or $[r^{(n-1)/r}, 1]$ where r is an odd prime. In particular, for each odd prime divisor of n or $n-1$ there is a unique S_n-class of derangements of that prime order. We know that G is 1-almost elusive if and only if $G = S_n$ and $r = n-1 = 2^m - 1$ is a Mersenne prime (see Lemma 3.1.4).

Let us now assume that G is k-almost elusive with $k \geqslant 2$. Then there exist exactly k conjugacy classes of derangements of prime order $x_1^G, \ldots, x_k^G$, where $|x_i| = r_i$ is an odd prime. Without loss of generality, we may assume that $r_1 \leqslant r_2 \leqslant \ldots \leqslant r_k$.

Let us first assume that $r_1 = \cdots = r_k$. Since $n \geqslant 6$ is even, there always exists an odd prime divisor r of $n-1$ and any element with the cycle shape $[r^{(n-1)/r}, 1]$ is a derangement of prime order. Thus we conclude that $r = r_1$ and $n-1 = r^a$ for some $a \geqslant 1$. Additionally, if s is an odd prime divisor of n then $[s^{n/s}]$ is a derangement of prime order. Since $r \neq s$ we may assume that $n = 2^m$ for some $m \geqslant 1$. Then by Lemma 2.4.1, we must have $r = n - 1 = 2^m - 1$ is a Mersenne prime. We note that this forces there to be a unique cycle shape for derangements of prime order. Thus we can answer Problem 7.2.2 in this case. In particular, G is k-almost elusive with $k \geqslant 2$ if and only if $G = A_n$, $n - 1$ is a Mersenne prime and $k = 2$.

Now we turn to Problem 7.2.3. Without loss of generality we may assume that $r_1 < r_2 < \cdots < r_t = \cdots = r_k$ for some $2 \leqslant t \leqslant k$. Recall that each r_i must divide either n or $n - 1$, which leads us to a variety of possible Diophantine equations. For example, take $k = 2$. Then using similar reasoning as above we get the following possible equations:

(i) $n = 2^m r_1^b$ and $n - 1 = r_2^a$ (i.e. $2^m r_1^b - 1 = r_2^a$); or

(ii) $n = 2^m$ and $n - 1 = r_1^b r_2^a$ (i.e. $2^m - 1 = r_1^b r_2^a$),

where $m, b, a \geqslant 1$. Determining the solutions to these equations is a very difficult number theoretic problem, which is far out of reach with current methods. For example, all primes of the form $r_2 = 2r_1 - 1$ are solutions to (i) and we do not currently know if there are infinitely many primes of this form or not. More complicated equations arise for $k > 2$, making Problem 7.2.3 increasingly more difficult to solve.

For the following example, we remind the reader that we use P_q^n to denote the set of primitive prime divisors of $q^n - 1$. We also write (a, b) for the greatest divisor of positive integers a and b (see Section 2.4).

Example 7.2.5. Take $G = \mathrm{L}_2(q)$, where $q = p^f \geqslant 4$ such that p is a prime and $f \geqslant 1$, and take H to be a maximal subgroup of type P_1. That is $H = C_p^f{:}C_{(q-1)/d}$ where $d = (2, q-1)$. In particular,

$$|G| = \frac{1}{d}q(q-1)(q+1) \text{ and } |H| = \frac{1}{d}q(q-1).$$

The only possible primes for prime order derangements are the prime divisors of $|\Omega| = q+1$. We note that if r is an odd prime divisor of $q+1$ then every element in G of order r is a derangement since r divides $|G|$ but not $|H|$. Additionally we note that r is an odd prime divisor of $q+1$ if and only if r is a primitive prime divisor of $q^2 - 1$. Thus there are $(r-1)/2$ distinct G-classes of derangements of order r in G (see [9, Proposition 3.2.1]). In fact these are the only derangements of prime order in G unless $q \equiv 3 \pmod 4$. To see this note that if q is even then $q+1$ is not divisible by 2 so there are no involutory derangements. Additionally if q is odd then 2 divides $|G|$, and $|H|$ is divisible by 2 if and only if $q \equiv 1 \pmod 4$. Thus since G has a unique class of involutions, we conclude that G contains an involutory derangement if and only if $q \equiv 3 \pmod 4$.

Assume that G is k-almost elusive such that $k \geqslant 2$ (the case $k = 1$ was handled in Proposition 4.2.33). By the above discussion we may immediately assume that $|P_q^2| \leqslant k$. Suppose first that $|P_q^2| = 0$. Then by the discussion above this forces $k = 1$ (see also Proposition 4.2.33). Finally let us suppose that $|P_q^2| = t \geqslant 1$. That is $P_q^2 = \{r_1, \ldots, r_t\}$ such that $r_i = 2d_i + 1$ for some $d_i \geqslant 1$. Then again by the discussion above there are exactly d_i distinct G-classes of derangements of order r_i in G and so G contains exactly $\sum_i d_i + \gamma$ conjugacy classes of derangements of prime order, where $\gamma = 1$ if $q \equiv 3 \pmod 4$ and $\gamma = 0$ otherwise. Thus for both Problems 7.2.2 and 7.2.3 we need to know when $\sum_i d_i + \gamma = k$. We note that finding the values of q such that this equation is satisfied

is an incredibly difficult number theoretic problem for similar reasons to those discussed in Section 2.4.2. In particular these problems lead to complicated Diophantine equations that do not have full integer solution sets at this current time. We will discuss some of the refinements and detailed difficulties for each problem.

To answer Problem 7.2.2 we will assume that $|\beta_{pr}(G)| = 1$. Note that if $q \equiv 3 \pmod 4$ then we must have $|P_q^2| = 0$ and so $k = 1$. Thus we may assume that $q \not\equiv 3 \pmod 4$. In this case we reduce down to the problem of classifying the values of q such that $2k+1$ is the unique primitive prime divisor of $q^2 - 1$ with $k \geqslant 2$. In particular, we want to classify all values of q that satisfy the following equation:

$$q + 1 = 2^a(2k+1)^b,$$

where $b \geqslant 1$, $a = 0$ if q is even and $a = 1$ if q is odd (since $q \not\equiv 3 \pmod 4$). By using Proposition 2.4.11 we reduce down to the cases $q = 8$, $f = 1$, $f = 2^t$ for some $t \geqslant 1$, or f is an odd prime and p is a Mersenne prime. Assume first that $q = 8$, in this case it is clear to see that $k = 1$ (see also Proposition 4.2.1). Now assume that $f = 2^t$ for some $t \geqslant 1$. Then we can use Lemma 2.4.1 and Theorem 2.4.14 to show that either $(p, f, k) = (239, 2, 6)$ or $q+1 = 2(2k+1)^b$ where $b \in \{1, 2\}$. For a given k we can now use computational methods to find the remaining solutions. For example if $k \leqslant 6$ then the only remaining solutions are $(k, q) = (2, 7), (2, 9)$ and $(6, 25)$. Next assume that $f = 1$. In this case we are left with the Diophantine equation $p + 1 = 2(2k+1)^b$ where $b \geqslant 1$ (recall that $q \geqslant 4$). This type of Diophantine equation does not have a full integer solution set for similar reasons to the equation in (i) from Example 7.2.4 and finding solutions to this is a difficult number theoretic problem. A similar issue arises for the case when f is an odd prime and p is a Mersenne prime.

For Problem 7.2.3 since all of the r_i are distinct we may assume without loss of generality that $r_1 < \ldots < r_t$. Thus $d_1 < \ldots < d_t$ and so $d_i \geqslant i$. Therefore $\sum_i d_i \geqslant \sum_i i = t(t+1)/2$. This means that t must be such that $t(t+1)/2+\gamma \leqslant k$. In particular, $t \leqslant k/2+1$. However with this reduction we are still left with the problem of finding solutions to the Diophantine equation

$$q + 1 = 2^a r_1^{a_1} \ldots r_t^{a_t}$$

where $a \geqslant 0$ and $a_1, \ldots, a_t \geqslant 1$.

As we have seen in both of the examples above, the current inability to find full integer solution sets to certain complicated Diophantine equations is a huge obstacle in answering

both Problems 7.2.2 and 7.2.3. However it may be possible to provide solutions to these problems in terms of some number theoretic constraints, particularly in the cases when k is small.

7.2.2 The minimal number of conjugacy classes of derangements of prime order

We recall that the O'Nan-Scott theorem [73] allows us to partition the primitive permutation groups into 5 different families based on the socles of the groups. These families are the affine, almost simple, diagonal-type, product-type and the twisted wreath product groups. We recall that if G is elusive then $\mathcal{K}_{pr}(G) = 0$ and if G is almost elusive then $\mathcal{K}_{pr}(G) = 1$. Due to the work of Giudici [37] the only primitive O'Nan-Scott families that contain elusive groups are the almost simple groups and the product type groups. Additionally due to work in this thesis, namely Theorem 2.2.1, the only families that contain almost elusive groups are the affine groups and the almost simple groups. Thus it is clear that the following result holds

Lemma 7.2.6. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive permutation group. Then either G is elusive or exactly one of the following holds*

(i) *G is an almost simple or an affine group and $\mathcal{K}_{pr}(G) \geqslant 1$; or*

(ii) *$\mathcal{K}_{pr}(G) > 1$*

An interesting question to pose for the remaining families (diagonal type, product type and twisted wreath product groups) is can we improve the bound in (ii). In particular we pose the following problem

Problem 7.2.7. *For the non-elusive primitive diagonal type, product type and twisted wreath product groups can we obtain strict lower bounds on $\mathcal{K}_{pr}(G)$ for these families? If so can we determine precisely which groups obtain these bounds?*

Here we will provide a small discussion on the product type groups. First we remind the reader of some of the properties of product type groups. Take $G \leqslant \mathrm{Sym}(\Omega)$ to be a primitive permutation group of product type. Then the socle $G_0 = T^k$, is a direct product of k copies of a simple group T where $k = mr$ with $r > 1$. There exists a primitive nonregular group $U \leqslant \mathrm{Sym}(\Gamma)$ with socle T^m such that U is almost simple or diagonal type and G is isomorphic to a subgroup of $U \wr S_r$ with the product action. We say that $T^k \leqslant G \leqslant U \wr S_r$ and that $G_0 = T^k$. Note $\Omega = \Gamma^k$.

There do exist examples of product type groups for which $\mathcal{K}_{pr}(G) = 2$. For example, take $U = A_5$ with its action on the right cosets of D_{10}. Then $G = U \wr S_2$ has two conjugacy classes of derangements of prime order. We note that in this case $\mathcal{K}_{pr}(G) = k$. Thus it is natural to wonder if we may be able to find a lower bound for the product type groups with socle T^k in terms of k. It turns out that we can.

Proposition 7.2.8. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive permutation group of product type with socle T^k and $\Omega = \Gamma^k$ as described above. Suppose that T is not elusive with its action on Γ. Then $\mathcal{K}_{pr}(G) \geqslant k$.*

Proof. Let $x \in T$ be a derangement of prime order with respect to the action of T on Γ. Then the elements $(x, 1, \ldots, 1)$, $(x, x, \ldots, 1)$, $\ldots$, $(x, x, \ldots, x) \in T^k$ are k pairwise non-conjugate elements in G. Additionally these elements are all derangements in G. To see this we will show that $y = (x, 1, \ldots, 1)$ is a derangement and note that the proof for the other elements is similar. Take $(\gamma_1, \ldots, \gamma_k) \in \Omega = \Gamma^k$. Then $(\gamma_1, \ldots, \gamma_k)^y = (\gamma_1^x, \gamma_2, \ldots, \gamma_k)$. Since x is a derangement we have that $\gamma_1^x \neq \gamma_1$, so y is a derangement in T^k with respect to the action on Ω. □

We hope that it may be possible to find similar lower bounds for the other remaining O'Nan-Scott families.

7.2.3 Anti-elusive groups

We recall that due to a theorem of Fein, Kantor and Schacher [29], every nontrivial finite transitive permutation group contains a derangement of prime power order. Additionally we recall that the existence of derangements of prime order is not guaranteed, and we call a transitive permutation group elusive if it contains no derangements of prime order. Motivated by these ideas we provide the following definition,

Definition 7.2.9. We say a transitive permutation group G is *anti-elusive* if the only derangements in G are of prime order.

For example, take $G = A_5$ acting naturally on the points $\{1, ..., 5\}$. To see that this is anti-elusive we note that an element of G is a derangement if and only if its cycle shape does not contain a 1-cycle. Thus the only order for a derangement is 5, and so G is anti-elusive. In [48], Isaccs et al. describe the finite transitive groups in which every derangement is an involution. By [48, Theorem A], such a group is either an elementary abelian 2-group or

a Frobenius group with kernel an elementary abelian 2-group. In particular, these groups are examples of anti-elusive groups. We pose the following problem.

Problem 7.2.10. *Can we classify the finite transitive anti-elusive permutation groups?*

We focus the remainder of our discussion on the primitive case. Note that we have already seen an example of an anti-elusive almost simple primitive group earlier in this section. In [16], Burness and Tong-Viet classify the primitive permutation groups in which every derangement is of r-power order for some fixed prime r. Frequently throughout the analysis in [16] the proofs of various results inadvertently show that certain groups are not anti-elusive. In fact in some cases they show necessary and sufficient conditions for a group to be anti-elusive. For example, the proof of [16, Lemma 4.4] shows the following result.

Lemma 7.2.11. *Take $G = \mathrm{L}_2(q)$ with $q = 2^f \geqslant 8$ even and with point stabiliser H. Assume that G is primitive. Then G is anti-elusive if and only if one of the following holds:*

(i) *$q+1$ is a Fermat prime and $H = P_1$ or $D_{2(q-1)}$*

(ii) *$q-1$ is a Mersenne prime and $H = D_{2(q+1)}$*

This result in particular implies that there exist some potentially infinite families of anti-elusive groups. We conclude this section by handling certain families of primitive almost simple groups with alternating socle. For the remainder of this section we will take $G \leqslant \mathrm{Sym}(\Omega)$ to be an almost simple primitive permutation group with point stabiliser H and socle A_n such that $n \geqslant 5$.

Lemma 7.2.12. *Suppose $n \leqslant 20$. Then G is anti-elusive if and only if one of the following holds*

(i) *$G = A_5$ and $H = S_3$, D_{10} or A_4,*

(ii) *$G = A_6$ and $H = S_4$ or $3^2{:}4$,*

(iii) *$G = \mathrm{M}_{10}$ and $H = SD_{16}$, or*

(iv) *$G = A_7$ and $H = C_3{:}S_4$ or S_5.*

Proof. This is a straightforward computation in Magma [5], using similar techniques to those used in the proof of Proposition 3.1.1. □

Lemma 7.2.13. *Suppose $n > 20$ and H acts intransitively on $\{1, \ldots, n\}$. That is $H = (S_k \times S_{n-k}) \cap G$ for some $1 \leqslant k < n/2$. Then G is not anti-elusive.*

Proof. We note that since $n > 20$ we may assume that $G = A_n$ or S_n. Here H is the stabiliser of a k element subset of $\{1, \ldots, n\}$ (a k-set). Suppose first that n is not prime. If $G = S_n$, or $G = A_n$ with n odd, then any element with cycle shape $[n]$ is a derangement. Thus we may assume now that $G = A_n$ with n even. If $k \neq 2$ then any element with cycle shape $[n-2, 2]$ is a derangement not of prime order. Additionally if $k = 2$ then all elements with cycle shape $[n-3, 3]$ are derangements not of prime order, since $n - 3 > 3$. Thus we conclude that G is not anti-elusive.

Finally suppose that n is prime. Assume first that $k \notin \{2, 4\}$. Then any element in G with cycle shape $[n-4, 2^2]$ is a derangement not of prime order. Finally assume that $k = 2, 4$. In this case if $n \equiv 1 \pmod 4$ then any element with cycle shape $[(\frac{n-3}{2})^2, 3]$ is a derangement not of prime order. Similarly if $n \equiv 3 \pmod 4$ then any element with cycle shape $[(\frac{n-5}{2})^2, 5]$ is a derangement not of prime order. Thus G is not anti-elusive. □

Intuitively the case in which the point stabiliser H acts transitively but imprimitively on $\{1, \ldots, n\}$ should have a vaguely similar result and proof to that of Lemma 7.2.13. Additionally on first inspection the case in which the point stabiliser H acts primitively on $\{1, \ldots, n\}$ seems slightly harder to handle. This is primarily due to the fact that Ω does not have a nice description in terms of a partition of $\{1, \ldots, n\}$ unlike the other two cases.

CHAPTER

8

TABLES

In this final chapter we present the main tables we have referenced throughout this thesis. The content of this chapter is taken from [13, Section 1], [44, Sections 1 and 2] and [45, Sections 1, 2.2 and 6].

8.1 Remarks on the tables

We begin by noting that in view of the isomorphisms outlined in (2.1) the tables are complete. We remind the reader of these isomorphisms here.

$$\mathrm{L}_2(4) \cong \mathrm{L}_2(5) \cong A_5,\ \mathrm{L}_2(7) \cong \mathrm{L}_3(2),$$

$$\mathrm{L}_2(9) \cong \mathrm{PSp}_4(2)' \cong A_6,\ \mathrm{L}_4(2) \cong A_8,\ \mathrm{U}_4(2) \cong \mathrm{PSp}_4(3),$$

$$G_2(2)' \cong \mathrm{U}_3(3),\ {}^2G_2(3)' \cong \mathrm{L}_2(8).$$

We now provide a little information on how to read Tables P1, P2 and P3.

Remark 8.1. Firstly consider Tables P1 and P2. Here $G \leqslant \mathrm{Sym}(\Omega)$ is an almost simple primitive permutation group with socle G_0 and point stabiliser H.

(a) In both tables we record the *type of* H. For the alternating groups this describes the exact structure of H. In the case where G_0 is a classical group we additionally

record the Aschbacher collection containing H. For the geometric collections (those in the collections $\mathcal{C}_1, \ldots, \mathcal{C}_8$) and the novelty collection (denoted as $\mathcal{N}$) the type gives the approximate structure of $H \cap \mathrm{PGL}(V)$, where V is the natural module of G_0, and for the non-geometric collection (denoted as $\mathcal{S}$) the type of H denotes the socle of H. For example, take $G = \mathrm{L}_n(q)$ and H to be of type $\mathrm{GL}_1(q) \wr S_n$. Then H is the stabiliser of a direct sum decomposition of $V = V_1 \oplus \cdots \oplus V_n$ where $\dim V_i = 1$ for all $1 \leqslant i \leqslant n$. In addition, we adopt the standard notation and use P_i to denote a maximal parabolic subgroup, which is the stabiliser in G of an i-dimensional totally singular subspace of V (see Section 2.3.2 for more information). In all other cases the type of H describes the structure of $H \cap G_0$.

(b) The column labeled G records the groups G for which (G, H) is almost elusive. Additionally, the conditions stated in the tables are in addition to any conditions required for simplicity of G_0 and maximality of H (see [54, Section 3.5] for conditions for the classical groups of Lie type).

(c) In the final column, we describe the unique conjugacy class of derangements of prime order in G. If there is a unique G-class of elements of the given prime order in G, then we represent this class with the prime. However, if there are multiple classes of the given prime order then we describe the precise class. For example, 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 shown in the table, the Jordan form on V of the derangements is $[J_2, J_1]$, where J_i denotes a standard unipotent block of size i.

Similarly if $G = \mathrm{U}_4(2).2$ and H is of type $\mathrm{Sp}_4(2)$, then G has three G-classes of elements of order 3, labeled 3A, 3C and 3D with $|3\mathrm{A}| = 80$, $|3\mathrm{C}| = 240$ and $|3\mathrm{D}| = 480$; the derangements are in 3A. Something similar occurs in the cases where $G_0 = \mathrm{PSp}_6(2)$ with H of type $\mathrm{O}_6^+(2)$ and $G_0 = {}^2F_4(2)'$ with H of type $\mathrm{L}_2(25)$. In Case 2 of Table P1 the class 2A of involutory derangements in G is precisely the unique class of involutions in G_0.

Finally for the alternating and symmetric groups we represent the conjugacy class by the cycle structure of the element. For example, in the case $(G, H) = (A_6, \mathrm{L}_2(5))$ the elements in the unique class of derangements of prime order have cycle shape $[3, 1^3]$.

Finally in Table P3 we record n and i such that $G = \mathcal{P}(n, i)$ is almost elusive, where we

write $\mathcal{P}(n,i)$ for the i^{th} primitive group of degree n in the *Database of Primitive Groups* in Magma [5].

Remark 8.2. Here we provide some additional remarks on the cases arising in Tables P1 and P2.

(a) For case 1 in Table P1 there are additional conditions. Firstly, we note that $G_0 = \mathrm{U}_n(q)$ with number theoretic restrictions, namely $q = 2^f$ is even, $n \geqslant 5$ is a prime divisor of $q+1$ and $2nf+1$ is the unique primitive prime divisor of $q^{2n}-1$. Additionally, $G = G_0.J$ where $J \leqslant \mathrm{Out}(G_0) = \langle\ddot{\delta}\rangle{:}\langle\ddot{\phi}\rangle$, $J \cap \langle\ddot{\delta}\rangle = 1$ and J projects onto $\langle\ddot{\phi}\rangle$. Here we use δ and ϕ to denote a diagonal automorphism of order n and a field automorphism of order $2f$ respectively in $\mathrm{Aut}(G_0)$ (see [6, Section 1.7]), and following [54] for any element $x \in \mathrm{Aut}(G_0)$ we use $\ddot{x}$ to denote the coset $G_0x \in \mathrm{Out}(G_0) = \mathrm{Aut}(G_0)/G_0$. As explained in Remark 4.2.43 we do not anticipate any genuine examples arise in this case due to the heavy number theoretic restrictions required.

(b) For the cases with $G_0 = \mathrm{L}_3(4)$ in Table P2 the recorded groups in the column labeled G are defined using Atlas notation [82]. That is $G_0.2_1 = \mathrm{L}_3(4).\langle\iota\phi\rangle$, $G_0.2_2 = \mathrm{L}_3(4).\langle\phi\rangle$, $G_0.2_3 = \mathrm{L}_3(4).\langle\iota\rangle$ and $G_0.2^2 = \mathrm{L}_3(4).\langle\iota,\phi\rangle$, where ι denotes the inverse-transpose graph automorphism and ϕ denotes a field automorphism of order 2. Similarly for the case with $G_0 = \mathrm{U}_4(3)$ in Table P2. Here $G_0.2_2 = \mathrm{U}_4(3).\langle\gamma\rangle$, where γ is an involutory graph automorphism and $C_{G_0}(\gamma) = \mathrm{PSp}_4(3)$. Finally in the case where $G = {}^2F_4(2)$ and H is of type $\mathrm{L}_2(25)$, we note that $H = \mathrm{L}_2(25).2_3$. We use $\mathrm{L}_2(25).2_3$ to denote $\mathrm{L}_2(25).\langle\delta\phi\rangle$ where δ and ϕ are standard involutory diagonal and field automorphisms respectively (see [6, Section 1.7] for example).

Remark 8.3. Here we remark on Tables Q1 and Q2.

(a) For both tables, in the column labeled G we record the almost simple groups of interest. The column labeled H records the core-free non-maximal subgroups of G up to isomorphism for which (G,H) is almost elusive. Additionally, the column labeled x gives the unique conjugacy class of derangements of prime order. Note this is denoted by the relevant prime, r, since in all cases there is a unique conjugacy class in G of elements of order r.

(b) In Table Q2, the column labeled a records the number of G-classes of subgroups K of G such that $G = G_0K$ and $H \cong K$, b records the number of these G-classes

such that (G, K) is almost elusive and $c = d_G(H)$ denotes the depth of H (see Corollary 4). Additionally, in the column labeled M we record representatives of the G-classes of maximal subgroups of G that contain at least one subgroup K of G with $G = G_0K$, $H \cong K$ such that (G, K) is almost elusive. We note that each case can be constructed in MAGMA [5].

(c) For Table Q1, $p \geqslant 5$ is a prime and we remind the reader that for a positive integer t we use $\alpha(t)$ to denote the set of distinct prime divisors of t.

(d) In Case I of Table Q1, d is a divisor of $p+\epsilon$ such that $\alpha(d) = \alpha(p+\epsilon)$. Additionally in Cases II-IV in Table Q1, d is a divisor of $(p-1)/k$ such that $\alpha(d) = \alpha((p-1)/k)$ and $k = |G : G_0|$.

(e) In Table Q2 the † denotes the fact that the relevant A_5 or S_5 subgroup of H is a primitive subgroup of the corresponding A_6 or S_6 subgroup of M.

(f) In Table Q2, we write $G = \mathrm{L}_2(49).2_3 = \mathrm{L}_2(49).\langle\delta\phi\rangle$, where δ and ϕ denote standard involutory diagonal and field automorphisms of G_0, respectively (see [6, Section 1.7]).

Remark 8.4. Here we provide some remarks on the remaining tables (Tables A1-A3 and B1) .

(a) The column in Table A3 and B1 labeled i indicates the extra condition that there exists a unique primitive prime divisor r_i of $q^i - 1$. In particular, r_i is the unique prime that divides $|G_0|$ and not $|H_0|$. In Table B1 r_i is recorded in the column labeled r. We note that if $i = 6$ and $q \neq 19$ then $r_i = q^2 - q + 1$, and if $i = 12$ then $r_i = q^4 - q^2 + 1$ (this can be shown using Theorem 2.4.13 and is in fact shown within the proof of Lemma 2.4.15).

(b) For (G_0, H) in Tables A1-A3 we additionally record the *type* of H. See Remark 8.1(a).

(c) The conditions presented for the cases in Tables A1, A3 and B1 are in addition to the conditions given for existence and maximality in [54, Tables 3.5.A-F] and [6, Section 8.2].

(d) The cases recorded in Table A2 are specific cases in which $\pi(G_0) - \pi(H_0) = 1$ and either (G_0, H) does not appear in Table A3, or it appears in Table A3 but there does not exist a primitive prime divisor of $q^i - 1$.

(e) In Table A2 the second column is labeled (n, q, r). Here r indicates the unique prime that divides $|G_0|$ but not $|H_0|$. In the final five rows we have some potentially infinite families. We note that for the first two of these $q = p$ is a Mersenne prime and for the third $q = p$ is a Fermat prime. Additionally the † indicates that $q^2 - 1 = 2^a 3^b 5^c$ for some $a, b, c \geqslant 0$ and $q \neq 9$.

(f) For Cases L6, S7 and O10 in Table A3, we specifically require that there is a unique primitive prime divisor of $(q^{1/2})^{2i} - 1$. For i even this is equivalent to there being a unique primitive prime divisor of $q^i - 1$ (see Lemma 2.4.11).

(g) In Case U3 of Table A3 we have

$$i := \begin{cases} n & n \equiv 0 \pmod 4 \\ n/2 & n \equiv 2 \pmod 4 \\ 2n & \text{otherwise} \end{cases}.$$

8.2 The tables

Table P1: Primitive almost elusive almost simple groups: Part I

Case	G_0		Type of H	G	Conditions	x
1	$\mathrm{U}_n(q)$	$\mathcal{C}_1$	$\mathrm{GU}_1(q) \perp \mathrm{GU}_{n-1}(q)$	$G_0.J$	see Remark 8.2(a)	$2nf+1$
2	$\mathrm{L}_2(q)$	$\mathcal{C}_1$	P_1	$\mathrm{PGL}_2(q)$, G_0	$q=p=2^m-1$	2A
3				G_0	$q=p$, $p+1=2.3^a$, $a\geqslant 2$	3
4		$\mathcal{C}_2$	$\mathrm{GL}_1(q)\wr S_2$	$\mathrm{PGL}_2(q)$	$q=p=2^m-1$	p
5		$\mathcal{C}_3$	$\mathrm{GL}_1(q^2)$	$\mathrm{PGL}_2(q)$	$q=p=2^m+1$, $m\geqslant 3$	p
6	A_n		S_{n-1}	S_n	$n=r^a$, $a\geqslant 1$	$[r^{n/r}]$
7			$S_{n-2}\times S_2$	S_n	$n=2^m=r+1$	$[r,1]$
8				S_n	$n=2^m+1=r$	$[r]$
9			A_{n-1}	A_n	$n=r^a$, $a\geqslant 2$	$[r^{n/r}]$
10				A_n	$n=2r^a$, $r\geqslant 3$, $a\geqslant 2$	$[r^{n/r}]$

Table P2: Primitive almost elusive almost simple groups: Part II

G_0		Type of H	G	x
$\mathrm{L}_3(4)$	$\mathcal{C}_1$	$\mathrm{GL}_1(4) \oplus \mathrm{GL}_2(4)$	$G_0.2_1$, $G_0.2_3$, $G_0.2^2$	7
	$\mathcal{C}_5$	$\mathrm{GL}_3(2)$	$G_0.2_1$, $G_0.2_2$, $G_0.2^2$	5
	$\mathcal{S}$	A_6	$G_0.2_3$	7
$\mathrm{L}_2(49)$	$\mathcal{C}_1$	P_1	$G_0.2$	5
$\mathrm{L}_2(8)$	$\mathcal{C}_1$	P_1	$G_0.3$, G_0	3
	$\mathcal{C}_2$	$\mathrm{GL}_1(q) \wr S_2$	$G_0.3$, G_0	3
	$\mathcal{C}_3$	$\mathrm{GL}_1(q^2)$	$G_0.3$	7
$\mathrm{U}_6(2)$	$\mathcal{C}_5$	$\mathrm{Sp}_6(2)$	$G_0.2$	11
	$\mathcal{S}$	$\mathrm{U}_4(3)$	$G_0.2$	11
$\mathrm{U}_5(2)$	$\mathcal{C}_1$	$\mathrm{GU}_1(2) \perp \mathrm{GU}_4(2)$	$G_0.2$	11
	$\mathcal{C}_2$	$\mathrm{GU}_1(2) \wr S_5$	$G_0.2$	11
$\mathrm{U}_4(3)$	$\mathcal{C}_1$	P_2	$G_0.2_2$	7
$\mathrm{U}_4(2)$	$\mathcal{C}_1$	P_1	$G_0.2$, G_0	5
	$\mathcal{C}_2$	$\mathrm{GU}_1(2) \wr S_4$	$G_0.2$, G_0	5
	$\mathcal{C}_5$	$\mathrm{Sp}_4(2)$	$G_0.2$	3A
$\mathrm{U}_3(3)$	$\mathcal{C}_1$	P_1	$G_0.2$	7
	$\mathcal{S}$	$\mathrm{L}_2(7)$	$G_0.2$, G_0	$[J_2, J_1]$
$\mathrm{U}_3(4)$	$\mathcal{C}_1$	$\mathrm{GU}_2(q) \times \mathrm{GU}_1(q)$	$G_0.4$	13
	$\mathcal{C}_2$	$\mathrm{GU}_1(q) \wr S_3$	$G_0.4$	13
$\mathrm{U}_3(8)$	$\mathcal{C}_1$	$\mathrm{GU}_2(q) \times \mathrm{GU}_1(q)$	$G_0.6$	19
$\mathrm{PSp}_6(2)$	$\mathcal{C}_1$	$\mathrm{Sp}_2(2) \perp \mathrm{Sp}_4(2)$	G_0	7
	$\mathcal{C}_8$	$\mathrm{O}_6^+(2)$	G_0	3B
	$\mathcal{C}_8$	$\mathrm{O}_6^-(2)$	G_0	7
$\mathrm{PSp}_4(7)$	$\mathcal{C}_1$	P_2	$G_0.2$, G_0	5
${}^2F_4(2)'$		$\mathrm{L}_2(25)$	$G_0.2$, G_0	2A
		$5^2{:}4A_4$	$G_0.2$	13
$G_2(4)$		J_2	$G_0.2$	13
A_{10}		$(S_7 \times S_3) \cap G$	G_0	$[5^2]$
A_9		$(S_7 \times S_2) \cap G$	$G_0.2, G_0$	$[3^3]$

To be continued

Table P2 (Continued)

G_0	Type of H	G	x
	$(S_6 \times S_3) \cap G$	$G_0.2, G_0$	$[7, 1^2]$
A_6	$S_3 \wr S_2$	$G_0.2 = S_6$	$[5, 1]$
	$\mathrm{L}_2(5)$	G_0	$[3, 1^3]$
	D_{20}	$G_0.2 = \mathrm{PGL}_2(9)$	3
	5:4	$G_0.2 = \mathrm{M}_{10}$	3
	$3^2{:}Q_8$	$G_0.2 = \mathrm{M}_{10}$	5
A_5	D_{10}	G_0	$[3, 1^2]$

Table P3: The almost elusive affine groups $G = \mathcal{P}(n, i)$

n	i	n	i
2^4	17, 19	11^2	36, 38, 42, 43, 44
3^4	44, 68, 69, 70, 90, 99	19^2	73, 80
3^6	145, 198, 239, 240, 366	23^2	49, 51
5^2	12, 14, 17, 19	29^2	97, 103, 104
7^2	22, 23, 29	59^2	79, 84

Table Q1: Some quasiprimitive almost elusive groups

Case	G	H	Conditions	$\alpha(d)$	x
I	$\mathrm{PGL}_2(p)$	D_{2d}	$p = 2^m + \epsilon$, $m > 2$	$\alpha(p + \epsilon)$	p
II		$C_p{:}C_d$	$p = 2^m - 1$	$\alpha(p - 1)$	2
III	$\mathrm{L}_2(p)$	$C_p{:}C_d$	$p = 2^m - 1$	$\alpha(\frac{p-1}{2})$	2
IV		$C_p{:}C_d$	$p = 2.3^a - 1$, $a \geqslant 2$	$\alpha(\frac{p-1}{2})$	3

Table Q2: Sporadic quasiprimitive almost elusive groups

G	H	M	a	b	c	x
M_{10}	$3^2{:}4$	$3^2{:}Q_8$	2	2	2	5
A_9	$(A_5 \times 3){:}2^\dagger$	$(A_6 \times 3){:}2$	2	1	2	7
S_9	$S_5 \times S_3{}^\dagger$	$S_6 \times S_3$	2	1	2	7
$\mathrm{L}_2(8).3$	$S_3 \times 3$	$D_{18}{:}3$	1	1	2	7
$\mathrm{L}_2(49).2_3$	$7^2{:}(3 \times Q_8)$	$7^2{:}(3 \times Q_{16})$	2	2	2	5
	$7^2{:}12$	$7^2{:}(3 \times Q_{16})$	2	2	3	5
$\mathrm{U}_3(3).2$	$3.(S_3 \wr 2)$	$(3^{1+2}{:}8).2$	1	1	2	7
	$3.S_3^2$	$(3^{1+2}{:}8).2$	1	1	3	7
	S_3^2	$(3^{1+2}{:}8).2$	1	1	4	7
$\mathrm{U}_4(2)$	$S_3^2{:}S_3$	$3^3.S_4$	1	1	2	5
	$3 \times S_3^2$	$3^3.S_4$	1	1	3	5
	$6 \times S_3$	$3^3.S_4,\ 2^{1+4}{:}\mathrm{SU}_2(2){:}3$	1	1	4	5
	$\mathrm{SL}_2(3){:}A_4$	$2^{1+4}{:}\mathrm{SU}_2(2){:}3$	1	1	2	5
$\mathrm{U}_4(2).2$	$S_3 \times (S_3 \wr 2)$	$3^3{:}S_4 \times 2$	1	1	2	5
	S_3^3	$3^3{:}S_4 \times 2$	2	1	3	5
	$2 \times S_3^2$	$3^3{:}S_4 \times 2,\ 2^3{:}A_4.D_{12}$	3	1	4	5
	$2^{1+4}{:}\mathrm{SU}_2(2){:}3$	$2^3{:}A_4.D_{12}$	1	1	2	5
$\mathrm{U}_5(2).2$	$S_3 \times S_6$	$(3 \times \mathrm{SU}_4(2)){:}2$	1	1	2	11
$\mathrm{PSp}_6(2)$	$S_5 \times \mathrm{Sp}_2(2)^\dagger$	$S_6 \times \mathrm{Sp}_2(2)$	2	1	2	7

Table A1: Cases with $\pi(G_0) = \pi(H_0)$

Case	G_0		Type of H	Conditions
I	$\mathrm{L}_n(q)$	$\mathcal{C}_1$	P_1	$(n,q) = (6,2)$
II			$\mathrm{GL}_1(q) \oplus \mathrm{GL}_{n-1}(q)$	$(n,q) = (6,2)$
III		$\mathcal{S}$	A_7	$(n,q) = (4,2)$
IV		$\mathcal{S}$	A_5	$(n,q) = (2,9)$
V	$\mathrm{U}_n(q)$	$\mathcal{C}_1$	P_2	$(n,q) = (4,2)$
VI		$\mathcal{C}_5$	$\mathrm{Sp}_n(q)$	$(n,q) = (4,2)$
VII		$\mathcal{S}$	M_{22}	$(n,q) = (6,2)$
VIII			$\mathrm{L}_2(11)$	$(n,q) = (5,2)$
IX			$\mathrm{L}_2(7)$	$(n,q) = (3,3)$
X			$\mathrm{L}_3(4)$	$(n,q) = (4,3)$
XI			A_7	$(n,q) = (3,5), (4,3)$
XII	$\mathrm{PSp}_n(q)$	$\mathcal{C}_3$	$\mathrm{Sp}_{n/2}(q^2)$	$n = 4$
XIII		$\mathcal{C}_8$	$\mathrm{O}_n^-(q)$	$n \equiv 0 \pmod 4$
XIV			$\mathrm{O}_n^+(q)$	$(n,q) = (6,2)$
XV		$\mathcal{S}$	A_7	$(n,q) = (4,7)$
XVI	$\mathrm{P}\Omega_n^+(q)$	$\mathcal{C}_1$	P_m	$(n,q,m) = (8,2,1), (8,2,4)$
XVII			$\mathrm{O}_1(q) \perp \mathrm{O}_{n-1}(q)$	$n \equiv 0 \pmod 4$
XVIII			$\mathrm{Sp}_{n-2}(q)$	$n \equiv 0 \pmod 4$
XIX		$\mathcal{S}$	$\Omega_7(q)$	$n = 8$ and $p \neq 2$
XX			$\mathrm{Sp}_6(q)$	$n = 8$ and $p = 2$
XXI			A_9	$(n,q) = (8,2)$
XXII	$\Omega_n(q)$	$\mathcal{C}_1$	$\mathrm{O}_1(q) \perp \mathrm{O}_{n-1}^-(q)$	$n \equiv 1 \pmod 4$

Table A2: Cases with $\pi(G_0) = \pi(H_0) + 1$: Classical groups part I

G_0	Case	(n, q, r)	Type of H
$\mathrm{L}_n(q)$		$(7, 2, 127)$	P_2, $\mathrm{GL}_2(q) \oplus \mathrm{GL}_5(q)$, $P_{1,6}$
		$(6, 2, 31)$	P_2, $\mathrm{GL}_2(q) \oplus \mathrm{GL}_4(q)$, $P_{1,5}$
		$(5, 3, 13)$	M_{11}
		$(4, 4, 17)$	$\mathrm{GL}_4(q^{1/2})$
		$(3, 8, 73)$	$\mathrm{GL}_1(q) \wr S_3$, $\mathrm{GL}_3(q^{1/3})$
		$(3, 4, 7)$	A_6
		$(3, 4, 5)$	$\mathrm{GL}_3(q^{1/2})$
		$(2, 5, 5)$	$2_-^{1+2}.\mathrm{O}_2^-(2)$
		$(2, 7, 7)$	$2_-^{1+2}.\mathrm{O}_2^-(2)$
		$(2, 17, 17)$	$2_-^{1+2}.\mathrm{O}_2^-(2)$
		$(2, 9, 3)$	$\mathrm{GL}_1(q^2)$
$\mathrm{U}_n(q)$		$(6, 2, 11)$	$\mathrm{U}_4(3)$
		$(5, 2, 11)$	P_2, $\mathrm{GU}_1(q) \wr S_5$
		$(4, 5, 13)$	$\mathrm{U}_4(2)$, A_7
		$(4, 3, 7)$	$2^4.\mathrm{Sp}_4(2)$
		$(4, 2, 5)$	P_1, $\mathrm{GU}_1(q) \wr S_4$
		$(3, 9, 73)$	$\mathrm{GU}_1(q) \wr S_3$
		$(3, 5, 7)$	A_6
		$(3, 5, 5)$	$\mathrm{L}_2(7)$
		$(3, 4, 13)$	$\mathrm{GU}_1(q) \wr S_3$
		$(3, 3, 7)$	$\mathrm{GU}_1(q) \wr S_3$
$\mathrm{PSp}_n(q)$		$(8, 2, 17)$	P_1, P_4, $\mathrm{Sp}_2(q) \perp \mathrm{Sp}_6(q)$, A_{10}
		$(8, 2, 7)$	$\mathrm{Sp}_4(q^2)$
		$(6, 3, 5)$	$\mathrm{L}_2(13)$
		$(6, 2, 7)$	P_1, $\mathrm{Sp}_2(q) \perp \mathrm{Sp}_4(q), \mathrm{O}_6^-(2)$
		$(6, 2, 5)$	P_3
		$(4, 8, 3)$	${}^2B_2(q)$
		$(4, 7, 7)$	$2^{1+4}.\mathrm{O}_4^-(2)$
		$(4, 5, 13)$	$2^{1+4}.\mathrm{O}_4^-(2)$, A_6

To be continued

Table A2 (Continued)

G_0	Case	(n, q, r)	Type of H
$\mathrm{P}\Omega_n^+(q)$		$(10, 2, 17)$	P_5, $\mathrm{GL}_5(q).2$
		$(8, 3, 13)$	$\mathrm{O}_1(q) \wr S_8$, $2_+^{1+6}.\mathrm{O}_6^+(2)$, $\Omega_8^+(2)$
		$(8, 2, 7)$	$\mathrm{O}_4^-(q) \wr S_2$, $\mathrm{O}_4^+(q^2)$
		$(8, 2, 5)$	P_3, $\mathrm{GL}_1(q) \times \mathrm{GL}_3(q)$
$\mathrm{P}\Omega_n^-(q)$		$(10, 2, 17)$	A_{10}, M_{12}
		$(8, 2, 17)$	$\mathrm{O}_2^-(2) \perp \mathrm{O}_6^+(2)$
		$(8, 2, 7)$	$\mathrm{O}_4^-(q^2)$
$\Omega_n(q)$		$(7, 3, 13)$	$\mathrm{O}_1(q) \wr S_7$, $\mathrm{Sp}_6(2)$, A_9
$\mathrm{L}_n(q)$	I	$(2, 2^k - 1, 2)$	P_1
	II	$(2, 2^k - 1, 2^k - 1)$	$\mathrm{GL}_1(q) \wr S_2$
	III	$(2, 2^k + 1, 2^k + 1)$	$\mathrm{GL}_1(q^2)$
	IV	$(2, 2^f, 2^f - 1)$	$\mathrm{GL}_1(q^2)$
	V	$(2, q, p)^\dagger$	A_5

Table A3: Cases with $\pi(G_0) = \pi(H_0) + 1$: Classical groups part II

Case	G_0		Type of H	Conditions	i
L1	$\mathrm{L}_n(q)$	$\mathcal{C}_1$	P_1		n
L2			$\mathrm{GL}_1(q) \oplus \mathrm{GL}_{n-1}(q)$		n
L3			$P_{1,n-1}$	$n = 3, q = p$ Mersenne	n
L4		$\mathcal{C}_2$	$\mathrm{GL}_1(q) \wr S_n$	$(n, p) = (2, 2)$	n
L5		$\mathcal{C}_3$	$\mathrm{GL}_{n/2}(q^2)$	$n = 4, 6$	$n - 1$
L6		$\mathcal{C}_5$	$\mathrm{GL}_n(q^{1/2})$	$n = 2$	n
L7		$\mathcal{C}_8$	$\mathrm{Sp}_n(q)$	$n = 4, 6$	$n - 1$
L8			$\mathrm{O}^\epsilon_n(q)$	$(\epsilon, n) = (\circ, 3), (-, 4)$	3
U1	$\mathrm{U}_n(q)$	$\mathcal{C}_1$	$P_{n/2}$	$n = 4, 6$	$2n - 2$
U2			P_1	$n = 3$	$2n$
U3			$\mathrm{GU}_1(q) \perp \mathrm{GU}_{n-1}(q)$		See Remark 8.4(g)
U4		$\mathcal{C}_2$	$\mathrm{GL}_{n/2}(q^2).2$	$n = 4, 6$	$2n - 2$
U5		$\mathcal{C}_5$	$\mathrm{Sp}_n(q)$	$n = 4, 6$	$2n - 2$
U6			$\mathrm{O}^-_n(q)$	$n = 4$	$2n - 2$
U7			$\mathrm{O}_n(q)$	$n = 3$	$2n$
S1	$\mathrm{PSp}_n(q)$	$\mathcal{C}_1$	P_1	$n \equiv 0 \pmod 4$	n
S2			P_2	$n = 4$	n
S3			$\mathrm{Sp}_2(q) \perp \mathrm{Sp}_{n-2}(q)$	$n \equiv 0 \pmod 4$	n
S4		$\mathcal{C}_2$	$\mathrm{GL}_{n/2}(q).2$	$n = 4$	n
S5			$\mathrm{Sp}_{n/2}(q) \wr S_2$	$n = 4$	n
S6		$\mathcal{C}_3$	$\mathrm{Sp}_{n/3}(q^3)$	$n = 6$	$n - 2$
S7		$\mathcal{C}_5$	$\mathrm{Sp}_n(q^{1/2})$	$n = 4$	n
S8		$\mathcal{C}_8$	$\mathrm{O}^+_n(q)$		n
S9			$\mathrm{O}^-_n(q)$	$n \equiv 2 \pmod 4$	$n/2$
S10		$\mathcal{S}$	$\mathrm{G}_2(q)$	$n = 6$	$n - 2$
S11			$\mathrm{L}_2(q)$	$n = 4$	n
O1	$\mathrm{P}\Omega^+_n(q)$	$\mathcal{C}_1$	P_1	$n \equiv 0 \pmod 4$	$n - 2$
O2			P_4	$n = 8$	$n - 2$
O3			$\mathrm{Sp}_{n-2}(q)$	$n \equiv 2 \pmod 4$	$n/2$

To be continued

Table A3 (Continued)

Case	G_0		Type of H	Conditions	i
O4			$\mathrm{O}_1(q) \perp \mathrm{O}_{n-1}(q)$	$n \equiv 2 \pmod 4$	$n/2$
O5			$\mathrm{O}_2^+(q) \perp \mathrm{O}_{n-2}^+(q)$	$n \equiv 0 \pmod 4$	$n-2$
O6			$\mathrm{O}_2^-(q) \perp \mathrm{O}_{n-2}^-(q)$	$n \equiv 0 \pmod 4$	$(n-2)/2$
O7			$\mathrm{O}_2^-(q) \perp \mathrm{O}_{n-2}^-(q)$	$n \equiv 2 \pmod 4$	$n/2$
O8		$\mathcal{C}_2$	$\mathrm{GL}_{n/2}(q).2$	$n = 8$	$n-2$
O9		$\mathcal{C}_3$	$\mathrm{GU}_{n/2}(q)$	$n = 8$	$(n-2)/2$
O10		$\mathcal{C}_5$	$\mathrm{O}_n^-(q^{1/2})$	$n = 8$	$n-2$
O11		$\mathcal{N}$	$G_2(q)$	$n = 8$	$n/2$
O12	$\mathrm{P}\Omega_n^-(q)$	$\mathcal{C}_1$	P_1	$n \equiv 2 \pmod 4$	n
O13			$\mathrm{Sp}_{n-2}(q)$		n
O14			$\mathrm{O}_1(q) \perp \mathrm{O}_{n-1}(q)$		n
O15			$\mathrm{O}_2^+(q) \perp \mathrm{O}_{n-2}^-(q)$	$n \equiv 2 \pmod 4$	n
O16	$\Omega_n(q)$	$\mathcal{C}_1$	P_1	$n \equiv 1 \pmod 4$	$n-1$
O17			$\mathrm{O}_1(q) \perp \mathrm{O}_{n-1}^+(q)$		$n-1$
O18			$\mathrm{O}_1(q) \perp \mathrm{O}_{n-1}^-(q)$	$n \equiv 3 \pmod 4$	$(n-1)/2$
O19			$\mathrm{O}_2^\mu(q) \perp \mathrm{O}_{n-2}(q)$	$n \equiv 1 \pmod 4$	$n-1$
O20		$\mathcal{S}$	$\mathrm{G}_2(q)$	$n = 7$	$n-3$

Table B1: Cases in which $\pi(G_0) = \pi(H_0) + 1$: Exceptional groups

Case	G_0	H_0	Conditions	i	r
R1	${}^2G_2(q)$	$2 \times \mathrm{L}_2(q)$		6	r
G1	$G_2(q)$	J_1	$q = 11$	6	37
G2		J_2	$q = 4$	6	13
G3		$\mathrm{L}_2(13)$	$q = 4$	2	5
G4		$2^3.\mathrm{L}_3(2)$	$q = 3$	3	13
G5		$\mathrm{SL}_3(q)$:2		6	r
G6		$\mathrm{SU}_3(q)$:2		3	r
G7		${}^2G_2(q)$	$q = 3^f, f$ is odd	3	r
D1	${}^3D_4(q)$	$[q^9]$:$(\mathrm{SL}_2(q^3) \circ (q-1)).(2, q-1)$		12	r
D2		$G_2(q)$		12	r
D3		$\mathrm{L}_2(q^3) \times \mathrm{L}_2(q)$	q even	12	r
D4		$(\mathrm{SL}_2(q^3) \circ \mathrm{SL}_2(q)).2$	q odd	12	r
D5		$[2^{11}]$:$(7 \circ \mathrm{SL}_2(q))$	$q = 2$	12	13
D6		$(7 \circ \mathrm{SL}_3(2)).7.2$	$q = 2$	12	13
D7		$7^2.\mathrm{SL}_2(3)$	$q = 2$	12	13
F1	$F_4(q)$	$(2, q-1).\Omega_9(q)$		12	r
F1′	${}^2F_4(2)'$	$\mathrm{L}_3(3)$:2		4	5
F2′		$A_6.2^2$		12	13
F3′		5^2:$4A_4$		12	13

BIBLIOGRAPHY

[1] M. Aschbacher, *On the maximal subgroups of the finite classical groups*, Invent. Math. **76** (1984),469–514.

[2] M. Aschbacher and G. M. Seitz, *Involutions in Chevalley groups over fields of even order*, Nagoya Math. J. **63** (1976), 1–91.

[3] M. W. Baldoni, C. Ciliberto and G. M. Piacentini Cattaneo, *Elementary Number Theory, Cryptography and Codes,* D. A. Gewurz (trans.), Springer-Verlag, Berlin (2009).

[4] M. A. Bennett and A. Levin, *The Nagell-Ljunggren equation via Runge's method*, Monatsh. Math. **177** (2015), no. 1, 15–31.

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

[6] 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.

[7] T. Breuer, *Manual for the GAP Character Table Library, Version 1.3.6*, RWTH Aachen, 2023.

[8] T. C. Burness, *Topics in Permutation Group Theory*, Young Algebraists' Conference, Lausanne, 2014.

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

[10] T. C. Burness and M. Giudici, *Locally elusive classical groups*, Israel J. Math. **225** (2018), no.1, 343–402.

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

[12] T. C. Burness, R. M. Guralnick and S. Harper, *The spread of a finite group*, Ann. of Math. (2) **193** (2021), no.2, 619–687.

[13] T. C. Burness and E. V. Hall, *Almost elusive permutation groups*, J. Algebra **594** (2022), 519–543.

[14] T. C. Burness and A. R. Thomas, *The Classification of Extremely Primitive Groups*, Int. Math. Res. Not. IMRN **2022** (2022), no. 13, 10148–10248.

[15] 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.

[16] T. C. Burness and H. P. Tong-Viet, *Primitive permutation groups and derangements of prime power order*, Manuscripta Math. **105** (2016), 255–291.

[17] P. J. Cameron, *Permutation groups*, London Mathematical Society Student Texts, **45**, Cambridge University Press, Cambridge, 1999.

[18] 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.

[19] A. M. Cohen, M. W. Liebeck, J. Saxl and G. M. Seitz, *The local maximal subgroups of exceptional groups of Lie type*, Proc. London Math. Soc. **64** (1992), 21–48.

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

[21] D. A. Craven, *Alternating subgroups of exceptional groups of Lie type*, Proc. Lond. Math. Soc. **115** (2017), 449–501.

[22] D. A. Craven, *On medium-rank Lie primitive and maximal subgroups of exceptional groups of Lie type*, arXiv:2102.11096, 2021.

[23] D. A. Craven, *Maximal* PSL_2 *subgroups of exceptional groups of Lie type*, Mem. Amer. Math. Soc. **276** (2022), no. 1355.

[24] D. A. Craven, *The maximal subgroups of the exceptional groups* $F_4(q)$, $E_6(q)$ *and* ${}^2E_6(q)$ *and related almost simple groups*, arXiv:2103.04869, 2021.

[25] D. I. Deriziotis and G. O. Michler, *Character table and blocks of finite simple triality groups* ${}^3D_4(q)$, Trans. Amer. Math. Soc. **303** (1987), no. 1, 39–70.

[26] J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics, **163**. Springer-Verlag, New York, 1996.

[27] E. F. Ecklund and R.B. Eggleton, *Prime factors of consecutive integers*, Amer. Math. Monthly **79** (1972), 1082–1089.

[28] 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.

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

[30] 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.

[31] J. Fulman and R.M. Guralnick, *Derangements in subspace actions of finite classical groups*, Trans. Amer. Math. Soc. **369** (2017), 2521–2572.

[32] 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.

[33] 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.

[34] P. X. Gallagher, *The number of conjugacy classes in a finite group* Math. Z. **118** (1970), 175–179.

[35] É. Galois, *Oeuvres mathématiques: Lettre de Galois à M. Auguste Chevalier (29 Mai 1832)*. J. Math. Pures Appl. (Liouville) **11** (1846), 408–415.

[36] M. Giudici, *New constructions of groups without semiregular subgroups*, Comm. Algebra **35** (2007), 2719–2730.

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

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

[39] 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.

[40] D. Gorenstein, R. Lyons and R. Solomon, *The Classification of the Finite Simple Groups. Number 3,* Mathematical Surveys and Monographs, vol. 40. American Mathematical Society, Providence, RI (1998).

[41] R. M. Guralnick, *Conjugacy classes of derangements in finite transitive groups*, Proc. Steklov Inst. Math. **292** (2016), 112–117.

[42] R. M. Guralnick, *Subgroups of prime power index in a simple group*, J. Algebra **81** (1983), 304–311.

[43] R. M. Guralnick, T. Penttila, C. Praeger, J. Saxl, *Linear groups with orders having certain large prime divisors*, Proc. Lond. Math. Soc. **78** (1999) 167–214.

[44] E. V. Hall, *Almost elusive classical groups*, J. Pure Appl. Algebra **226** (2022), no.11, Paper No.107086.

[45] E. V. Hall, *The quasiprimitive almost elusive groups*, arXiv:2301.05569, 2023.

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

[47] B. Huppert and N. Blackburn, *Finite Groups III*, Springer-Verlag, Berlin, 1982.

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

[49] C. Jordan, *Sur la limite de transitivité des groupes non alternés*, Bull. Soc. Math. France **1** (1872/1873), 40–71.

[50] C. Jordan, *Recherches sur les substitutions*, J. Math. Pures Appl. (Liouville) **17** (1872), 351–367.

[51] P. B. Kleidman, *The maximal subgroups of the Steinberg triality groups* ${}^3D_4(q)$ *and of their automorphism groups*, J. Algebra **115** (1988), no. 1, 182–199.

[52] 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), no. 1, 30–71.

[53] P. B. Kleidman, *The maximal subgroups of the finite 8-dimensional orthogonal groups* $\mathrm{P}\Omega_8^+(q)$ *and of their automorphism groups*, J. Algebra **110** (1) (1987) 173–242.

[54] 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.

[55] R. Lawther, *Jordan block sizes of unipotent elements in exceptional algebraic groups,* Comm. Algebra **23** (1995), no. 11, 4125–4156.

[56] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, **20**. Cambridge University Press, Cambridge, 1997.

[57] M. W. Liebeck, *The affine permutation groups of rank three,* Proc. London Math. Soc. (3) **54** (1987), no. 3, 477–516.

[58] M. W. Liebeck, C. E. Praeger and J. Saxl, *A classification of the maximal subgroups of the finite alternating and symmetric groups*, J. Algebra **111** (1987), no. 2, 365–383.

[59] M. W. Liebeck, C. E. Praeger and J. Saxl, *On the O'Nan-Scott theorem for finite primitive permutation groups*, J. Austral. Math. Soc. **44** (1988), 389–396.

[60] M. W. Liebeck, C. E. Praeger and J. Saxl, *Transitive subgroups of primitive permutation groups*, J. Algebra **234** (2000), 291–361.

[61] M. W. Liebeck, J. Saxl and G. M. Seitz, *Subgroups of maximal rank in finite exceptional groups of Lie type*, Proc. London Math. Soc. **65** (1992), 297–325.

[62] M. W. Liebeck and G. M. Seitz, *A survey of maximal subgroups of exceptional groups of Lie type*, Groups, combinatorics & geometry (Durham, 2001), 139–146, World Sci. Publ., River Edge, NJ, 2003.

[63] M. W. Liebeck and G. M. Seitz, *On finite subgroups of exceptional algebraic groups*, J. reine angew. Math. **515** (1999), 25–72.

[64] M. W. Liebeck and G. M. Seitz, *Unipotent and Nilpotent Classes in Simple Algebraic Groups and Lie Algebras*, Mathematical Surveys and Monographs, vol. 180. AMS, New York (2012).

[65] A. J. Litterick, *On non-generic finite subgroups of exceptional algebraic groups*, Mem. Amer. Math. Soc. **253** (2018), no. 1207, v+156 pp.

[66] G. Malle, *The maximal subgroups of* ${}^2F_4(q^2)$, J. Algebra **139** (1991), no. 1, 52–69.

[67] G. Malle and D. Testerman, *Linear algebraic groups and finite groups of Lie type*, Cambridge Studies in Advanced Mathematics, **133**. Cambridge University Press, Cambridge, 2011.

[68] 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.

[69] P. Mihăilescu, *New bounds and conditions for the equation of Nagell-Ljunggren*, J. Number Theory **124** (2007), 380–395.

[70] 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.

[71] 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.

[72] S. Ramanujan, *A proof of Bertrand's postulate*, J. Indian Math. Soc. **XI** (1919), 181–182.

[73] L. L. Scott, *Representations in characteristic p*, The Santa Cruz Conference on Finite Groups, Proceedings of Symposia in Pure Mathematics, **37** (1980), 319–331.

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

[75] K. Shinoda, *The conjugacy classes of Chevalley groups of type* (F_4) *over finite fields of characteristic 2*, J. Fac. Sci. Univ. Tokyo Sect. I A Math. **21** (1974), 133–159.

[76] T. Shoji, *The conjugacy classes of Chevalley groups of type* (F_4) *over finite fields of characteristic* $p \neq 2$, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **21** (1974), 1–17.

[77] R. Steinberg, *Lectures on Chevalley Groups*, Department of Mathematics, Yale University (1968).

[78] M. Suzuki, *On a class of doubly transitive groups*, Annals of Math. **75** (1962), 105–145.

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

[80] 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.

[81] R. A. Wilson, *The finite simple groups*, Graduate Texts in Math. vol. 251. Springer-Verlag London, 2009.

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

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

[84] H. Zhu, M. Le and A. Togbé, *On the exponential Diophantine equation* $x^2 + p^{2m} = 2y^n$, Bull. Aust. Math. Soc. **86** (2012), 303–314.

[85] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Für Math. u. Phys. **3** (1892) 265–284.