1
Introduction

The study of derangements in transitive permutation groups has a long and rich history, which can be traced all the way back to the origins of probability theory in the early eighteenth century. In 1708, the French mathematician Pierre de Montmort wrote one of the first highly influential books on probability, entitled *Essay d'Analyse sur les Jeux de Hazard* [106], in which he presents a systematic combinatorial analysis of games of chance that were popular at the time. Through studying the card game *treize* (and variations), he calculates the proportion of derangements in the symmetric group S_{13} in its natural action on 13 points, and he proposes the general formula

$$\frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}$$

for the natural action of S_n. In a second edition, published in 1713, he reports on his correspondence with Nicolaus Bernoulli, who proved the above formula using the inclusion-exclusion principle (see [117] for further details). In particular, it follows that the proportion of derangements in S_n tends to $1/e$ as n tends to infinity.

In the context of permutation group theory, derangements have been widely studied since the days of Jordan in the nineteenth century, finding a range of interesting applications and connections in diverse areas such as graph theory, number theory and topology. In more recent years, following the Classification of Finite Simple Groups, the subject has been reinvigorated and our understanding of derangements has advanced greatly. As we shall see, many new results on the proportion of derangements in various families of groups have been obtained, and there has been a focus on studying the existence of derangements with special properties.

In the first three sections of this introductory chapter we will briefly survey some of these results and applications, focusing in particular on derangements

https://doi.org/10.1017/CBO9781139059060.002 Published online by Cambridge University Press

of prime order. Given a fixed prime number r, we will see that the problem of determining the existence of a derangement of order r in a finite transitive permutation group G can essentially be reduced to the case where G is a primitive almost simple group of Lie type. In this book, we aim to provide a detailed analysis of derangements of prime order in classical groups; the basic problem is introduced in Section 1.4, and we present a brief summary of our main results in Section 1.5 (with more detailed results given later in the text).

1.1 Derangements

We start by recalling some basic notions. We refer the reader to the books by Cameron [35], Dixon and Mortimer [48] and Wielandt [120] for excellent introductions to the theory of permutation groups.

Let G be a permutation group on a set Ω, so G is a subgroup of $\mathrm{Sym}(\Omega)$, the group of all permutations of Ω. We will use exponential notation for group actions, so α^g denotes the image of $\alpha \in \Omega$ under the permutation $g \in G$. The cardinality of Ω is called the *degree* of G.

We say that G is *transitive* on Ω if for all $\alpha, \beta \in \Omega$ there exists an element $g \in G$ such that $\alpha^g = \beta$. The *stabiliser in G of α*, denoted by G_α, is the subgroup of G consisting of all the permutations that fix α. The familiar Orbit-Stabiliser Theorem implies that if G is transitive then Ω can be identified with the set of (right) cosets of G_α in G. Moreover, the action of G on Ω is equivalent to the natural action of G on this set of cosets by right multiplication.

Given a subgroup H of G, we will write H^g to denote the conjugate subgroup $g^{-1}Hg = \{g^{-1}hg \mid h \in H\}$. It is easy to see that $G_{\alpha^g} = (G_\alpha)^g$ for all $\alpha \in \Omega$, $g \in G$. In particular, if G is transitive then G_α and G_β are conjugate subgroups for all $\alpha, \beta \in \Omega$.

The notion of primitivity is a fundamental indecomposability condition in permutation group theory. We say that a transitive group G is *imprimitive* if Ω admits a nontrivial G-invariant partition (there are two trivial partitions, namely $\{\Omega\}$ and $\{\{\alpha\} \mid \alpha \in \Omega\}$), and *primitive* otherwise. Equivalently, G is primitive if and only if G_α is a maximal subgroup of G. The finite primitive groups are the basic building blocks of all finite permutation groups.

Notice that if N is a normal subgroup of G, then the set of orbits of N on Ω forms a G-invariant partition of Ω. Thus, if G is primitive, every nontrivial normal subgroup of G is transitive. We can generalise the notion of primitivity by defining a group to be *quasiprimitive* if every nontrivial normal subgroup is transitive.

Definition 1.1.1 Let G be a group acting on a set Ω. An element of G is a *derangement* (or *fixed-point-free*) if it fixes no point of Ω. We write $\Delta(G)$ for the set of derangements in G. In addition, if G is finite then $\delta(G) = |\Delta(G)|/|G|$ denotes the proportion of derangements in G.

Note that if G is transitive with point stabiliser H then

$$\Delta(G) = G \setminus \bigcup_{g \in G} H^g \tag{1.1.1}$$

so an element $x \in G$ is a derangement if and only if $x^G \cap H$ is empty, where $x^G = \{g^{-1}xg \mid g \in G\}$ is the conjugacy class of x in G. We also observe that $\Delta(G)$ is a normal subset of G.

Let G be a finite group acting transitively on a set Ω with $|\Omega| \geqslant 2$. By the Orbit-Counting Lemma we have

$$\frac{1}{|G|} \sum_{x \in G} |\mathrm{fix}_\Omega(x)| = 1$$

where $\mathrm{fix}_\Omega(x) = \{\alpha \in \Omega \mid \alpha^x = \alpha\}$ is the set of fixed points of x on Ω. Since $|\mathrm{fix}_\Omega(1)| = |\Omega| \geqslant 2$, there must be an element $x \in G$ with $|\mathrm{fix}_\Omega(x)| = 0$ and thus G contains a derangement. This is a theorem of Jordan, which dates from 1872 (see [82]).

Theorem 1.1.2 *Let G be a finite group acting transitively on a set Ω with $|\Omega| \geqslant 2$. Then G contains a derangement.*

In particular, every nontrivial finite transitive permutation group contains a derangement. In view of (1.1.1), Jordan's theorem is equivalent to the fact that

$$G \neq \bigcup_{g \in G} H^g \tag{1.1.2}$$

for every proper subgroup H of a finite group G.

It is easy to see that Jordan's theorem does *not* extend to transitive actions of infinite groups:

(i) Let $\mathrm{FSym}(\Omega)$ be the *finitary symmetric group* on an infinite set Ω; it comprises the permutations of Ω with finite support (that is, the permutations that move only finitely many elements of Ω). Clearly, this transitive group does not contain any derangements.

(ii) Let V be an n-dimensional vector space over $\mathbb{C}$ and let $G = \mathrm{GL}(V)$ be the general linear group of all invertible linear transformations of V. Let Ω be the set of complete flags of V, that is, the set of subspace chains

https://doi.org/10.1017/CBO9781139059060.002 Published online by Cambridge University Press

$$\{0\} = V_0 \subset V_1 \subset V_2 \subset \cdots \subset V_{n-1} \subset V_n = V$$

where each V_i is an i-dimensional subspace of V. The natural action of G on V induces a transitive action of G on Ω. For each $x \in G$ there is a basis of V in which x is represented by a lower-triangular matrix (take the Jordan canonical form of x, for example), so x fixes a complete flag and thus G has no derangements.

(iii) More generally, consider a connected algebraic group G over an algebraically closed field K of characteristic $p \geqslant 0$, and let B be a Borel subgroup of G. Then every element of G belongs to a conjugate of B, so G has no derangements in its transitive action on the flag variety G/B. In fact, by a theorem of Fulman and Guralnick [55, Theorem 2.4], if G is a simple algebraic group acting on a coset variety G/H, then G contains no derangements if and only if one of the following holds:
   (a) H contains a Borel subgroup of G;
   (b) $G = \mathrm{Sp}_n(K)$, $H = \mathrm{O}_n(K)$ and $p = 2$;
   (c) $G = G_2(K)$, $H = \mathrm{SL}_3(K).2$ and $p = 2$.
   Moreover, if G is simple then [55, Lemma 2.2] implies that $\Delta(G)$ is a dense subset of G (with respect to the Zariski topology) if and only if H does not contain a maximal torus of G.

As observed by Serre, Jordan's theorem has some interesting applications in number theory and topology (see Serre's paper [113] for further details).

(i) *A number-theoretic application.* Let $f \in \mathbb{Z}[x]$ be an irreducible polynomial over $\mathbb{Q}$ with degree $n \geqslant 2$. Then f has no roots modulo p for infinitely many primes p.

(ii) *A topological application.* Let $f : T \to S$ be a finite covering of a topological space S, where f has degree $n \geqslant 2$ (so that $|f^{-1}(s)| = n$ for all $s \in S$) and T is path-connected and non-empty. Then there exists a continuous map $\varphi : \mathbb{S}_1 \to S$ from the circle $\mathbb{S}_1$ that cannot be lifted to the covering T.

In view of Jordan's theorem, two natural questions arise:

Question 1. *How abundant are derangements in transitive groups?*

Question 2. *Can we find derangements with special properties, such as a prescribed order?*

Both of these questions have been widely investigated in recent years, and in the next two sections we will highlight some of the main results.

Remark 1.1.3 We will focus on Questions 1 and 2 above. However, there are many other interesting topics concerning derangements that we will not discuss. Here are some examples:

(i) *Normal coverings.* Let G be a finite group and recall that if H is a proper subgroup of G then $\bigcup_{g\in G} H^g$ is a proper subset of G (see (1.1.2)). A collection of proper subgroups $\{H_1,\ldots,H_t\}$ is a *normal covering* of G if

$$G = \bigcup_{i=1}^{t} \bigcup_{g\in G} H_i^g$$

and we define $\gamma(G)$ to be the minimal size of a normal covering of G. By Jordan's theorem, $\gamma(G) \geqslant 2$, and this invariant has been investigated in several recent papers (see [15, 16, 42], for example). The connection to derangements is transparent: if $\{H_1,\ldots,H_t\}$ is a normal covering then each $x \in G$ has fixed points on the set of cosets G/H_i, for some i.

(ii) *Algorithms.* Given a set of generators for a subgroup $G \leqslant S_n$, it is easy to determine whether or not G is transitive. If G is transitive and $n \geqslant 2$, then Jordan's theorem implies that G contains a derangement, and there are efficient randomised algorithms to find a derangement in G. In a recent paper, Arvind [2] has presented the first elementary *deterministic* polynomial-time algorithm for finding a derangement.

(iii) *Thompson's question.* A finite transitive permutation group $G \leqslant \mathrm{Sym}(\Omega)$ is *Frobenius* if $|G_\alpha| > 1$ and $G_\alpha \cap G_\beta = 1$ for all distinct $\alpha,\beta \in \Omega$. By a theorem of Frobenius, $\{1\}\cup\Delta(G)$ is a normal transitive subgroup and thus $\Delta(G)$ is a transitive subset of G. The following, more general question, has been posed by J. G. Thompson.

Question. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group. Is $\Delta(G)$ a transitive subset of G?*

This is Problem 8.75 in the Kourovka Notebook [84]. It is easy to see that the primitivity condition here is essential; there are imprimitive groups G such that $\Delta(G)$ is intransitive. For instance, take the natural action of the alternating group A_4 on the set of 2-element subsets of $\{1,2,3,4\}$.

1.2 Counting derangements

Let G be a transitive permutation group on a finite set Ω with $|\Omega| = n \geqslant 2$. Recall that $\Delta(G)$ is the set of derangements in G, and $\delta(G) = |\Delta(G)|/|G|$ is the proportion of derangements. In general, it is difficult to compute $\delta(G)$

https://doi.org/10.1017/CBO9781139059060.002 Published online by Cambridge University Press

precisely. Of course, Jordan's theorem (Theorem 1.1.2) implies that $\delta(G) > 0$, and stronger lower bounds have been obtained in recent years. In [37], for example, Cameron and Cohen use the Orbit-Counting Lemma to show that $\delta(G) \geqslant 1/n$, with equality if and only if G is *sharply 2-transitive*, that is, either $(G,n) = (S_2,2)$, or G is a Frobenius group of order $n(n-1)$, with n a prime power. This has been extended by Guralnick and Wan (see [73, Theorem 1.3]).

Theorem 1.2.1 *Let G be a transitive permutation group of degree $n \geqslant 2$. Then one of the following holds:*

(i) $\delta(G) \geqslant 2/n$;
(ii) *G is a Frobenius group of order $n(n-1)$ with n a prime power;*
(iii) $G = S_n$ *and* $n \in \{2,4,5\}$.

It is worth noting that this strengthening of the lower bound on $\delta(G)$ from $1/n$ to $2/n$ requires the classification of the finite 2-transitive groups, which in turn relies on the Classification of Finite Simple Groups. As explained in [73], Theorem 1.2.1 has interesting applications in the study of algebraic curves over finite fields.

Inspired by Montmort's formula

$$\delta(S_n) = \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}$$

(with respect to the natural action of S_n), it is natural to consider the asymptotic behaviour of $\delta(G)$ when G belongs to an interesting infinite family of groups. From the above formula, we immediately deduce that $\delta(S_n)$ tends to $1/e$ as n tends to infinity. Similarly, we find that $\delta(A_n) \geqslant 1/3$ and $\delta(\mathrm{PSL}_2(q)) \geqslant 1/3$ for all $n,q \geqslant 5$, with respect to their natural actions of degree n and $q+1$ (see [12, Corollary 2.6 and Lemma 2.8]). In these two examples, we observe that G belongs to an infinite family of finite simple groups, and $\delta(G)$ is bounded away from zero by an absolute constant.

In fact, a deep theorem of Fulman and Guralnick [55, 56, 57, 58] shows that this is true for *any* transitive simple group.

Theorem 1.2.2 *There exists an absolute constant $\varepsilon > 0$ such that $\delta(G) \geqslant \varepsilon$ for any transitive finite simple group G.*

This theorem confirms a conjecture of Boston *et al.* [12] and Shalev. The asymptotic nature of the proof does not yield an explicit constant, although [57, Theorem 1.1] states that $\varepsilon \geqslant 0.016$ with at most finitely many exceptions. It is speculated in [12, p. 3274] that the optimal bound is $\varepsilon = 2/7$, which is realised by the standard actions of $\mathrm{PSL}_3(2)$ and $\mathrm{PSL}_3(4)$, of degree

7 and 21, respectively. In fact, it is easy to check that the action of the Tits group $G = {}^2F_4(2)'$ on the set of cosets of a maximal subgroup $2^2.[2^8].S_3$ yields $\delta(G) = 89/325 < 2/7$, and we expect 89/325 to be the optimal constant in Theorem 1.2.2.

Fulman and Guralnick also establish strong asymptotic results. For instance, they show that apart from some known exceptions, $\delta(G)$ tends to 1 as $|G|$ tends to infinity (the exceptions include $G = A_n$ acting on the set of k-element subsets of $\{1,\ldots,n\}$ with k bounded, for example). Further information on the limiting behaviour of the proportion of derangements in the natural action of S_n or A_n on k-sets is given by Diaconis, Fulman and Guralnick [44, Section 4], together with an interesting application to card shuffling.

As explained in [55, Section 6], one can show that the above theorem of Fulman and Guralnick does *not* extend to almost simple groups. For example, let p and r be primes such that r and $|\mathrm{PGL}_2(p)| = p(p^2-1)$ are coprime, and set $G = \mathrm{PGL}_2(p^r){:}\langle\phi\rangle$ and $\Omega = \phi^G$, where ϕ is a field automorphism of $\mathrm{PGL}_2(p^r)$ of order r. By [71, Corollary 3.7], the triple $(G, \mathrm{PGL}_2(p^r), \Omega)$ is *exceptional* and thus [71, Lemma 3.3] implies that every element in a coset $\mathrm{PGL}_2(p^r)\phi^i$ (with $1 \leqslant i < r$) has a unique fixed point on Ω. Therefore

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

and thus $\delta(G)$ tends to 0 as r tends to infinity.

It is worth noting that Theorem 1.2.2 indicates that the proportion of derangements in simple primitive groups behaves rather differently to the proportion of derangements in more general primitive groups. Indeed, by a theorem of Boston *et al.* [12, Theorem 5.11], the set

$$\{\delta(G) \mid G \text{ is a finite primitive group}\}$$

is dense in the open interval $(0,1)$.

In a slightly different direction, if G is a transitive permutation group of degree $n \geqslant 2$, then $\Delta(G)$ is a normal subset of G and we can consider the number of conjugacy classes in $\Delta(G)$, which we denote by $\kappa(G)$. Of course, Jordan's theorem implies that $\kappa(G) \geqslant 1$. In [31], the finite primitive permutation groups with $\kappa(G) = 1$ are determined (it turns out that G is either sharply 2-transitive, or $(G,n) = (A_5,6)$ or $(\mathrm{PSL}_2(8){:}3, 28)$), and this result is used to study the structure of finite groups with a nonlinear irreducible complex character that vanishes on a unique conjugacy class. We refer the reader to [31] for more details and further results.

An extension of the main theorem of [31] from primitive to transitive groups has recently been obtained by Guralnick [69]. He shows that every transitive group G with $\kappa(G) = 1$ is primitive, so no additional examples arise.

1.3 Derangements of prescribed order

In addition to counting the number of derangements in a finite permutation group, it is also natural to ask whether or not we can find derangements with special properties, such as a specific order.

1.3.1 Prime powers

The strongest result in this direction is the following theorem of Fein, Kantor and Schacher [52], which concerns the existence of derangements of prime power order.

Theorem 1.3.1 *Every nontrivial finite transitive permutation group contains a derangement of prime power order.*

This theorem was initially motivated by an important number-theoretic application, which provides another illustration of the utility of derangements in other areas of mathematics. Here we give a brief outline (see [52] and [87, Chapter III] for more details; also see [68] for further applications in this direction).

Let K be a field and let A be a central simple algebra (CSA) over K, so A is a simple finite-dimensional associative K-algebra with centre K. By the Artin–Wedderburn theorem, A is isomorphic to a matrix algebra $M_n(D)$ for some positive integer n and division algebra D. Under the *Brauer equivalence*, two CSAs A and A' over K are equivalent if $A \cong M_n(D)$ and $A' \cong M_m(D)$ for some n and m, and the set of equivalence classes forms an abelian group under tensor product. This is called the *Brauer group* of K, denoted $\mathscr{B}(K)$.

Let L/K be a field extension. The inclusion $K \subseteq L$ induces a group homomorphism $\mathscr{B}(K) \to \mathscr{B}(L)$, and the *relative Brauer group* $\mathscr{B}(L/K)$ is the kernel of this map. The connection to derangements arises from the remarkable observation that Theorem 1.3.1 is equivalent to the fact that $\mathscr{B}(L/K)$ is infinite for any nontrivial finite extension of global fields (where a *global field* is a finite extension of $\mathbb{Q}$, or a finite extension of $\mathbb{F}_q(t)$, the function field in one variable over a finite field $\mathbb{F}_q$).

In order to justify this equivalence, as explained in [52, Section 3], there is a reduction to the case where L/K is separable, and by a further reduction one can assume that $L = K(\alpha)$. Let E be a Galois closure of L/K, let Ω be the set of roots in E of the minimal polynomial of α over K, and let G be the Galois group $\mathrm{Gal}(E/K)$. Then G acts transitively on Ω, and [52, Corollary 3] states that $\mathscr{B}(L/K)$ is infinite if and only if G contains a derangement of prime power

order. More precisely, if r is a prime divisor of $|\Omega|$ then the r-torsion subgroup of $\mathscr{B}(L/K)$ is infinite if and only if G contains a derangement of r-power order.

Although the existence of derangements in Theorem 1.1.2 is an easy corollary of the Orbit-Counting Lemma, the extension to prime powers in Theorem 1.3.1 appears to require the full force of the Classification of Finite Simple Groups.

The basic strategy is as follows. First observe that if $G \leqslant \mathrm{Sym}(\Omega)$ is an imprimitive permutation group and every $x \in G$ of prime power order fixes a point, then x must also fix the set that contains this point in an appropriate G-invariant partition of Ω. Hence the primitive group induced by G on a maximal G-invariant partition also has no derangements of prime power order, so the existence problem is reduced to the primitive case. We now consider a minimal counterexample G. If N is a nontrivial normal subgroup of G, then N acts transitively on Ω (by the primitivity of G), so the minimality of G implies that $N = G$ and thus G is simple. The proof now proceeds by working through the list of finite simple groups provided by the Classification. It would be very interesting to know if there exists a Classification-free proof of Theorem 1.3.1.

Remark 1.3.2 The finite primitive permutation groups with the property that *every* derangement has r-power order, for some fixed prime r, are investigated in [32]. The groups that arise are almost simple or affine, and the almost simple groups with this extremal property are determined in [32, Theorem 2].

1.3.2 Isbell's Conjecture

Let G be a finite transitive permutation group. Although Theorem 1.3.1 guarantees the existence in G of a derangement of prime power order, the proof does not provide any information about the primes involved. However, there are some interesting conjectures in this direction. For example, it is conjectured that if a particular prime power dominates the degree of G, then G contains a derangement that has order a power of that prime. This is known as *Isbell's Conjecture*.

Conjecture 1.3.3 *Let p be a prime. There is a function $f(p,b)$ with the property that if G is a transitive permutation group of degree $n = p^a b$ with $(p,b) = 1$ and $a \geqslant f(p,b)$, then G contains a derangement of p-power order.*

The special case $p = 2$ arises naturally in the study of n-player games, and the conjecture dates back to work of Isbell on this topic in the late 1950s [77,

https://doi.org/10.1017/CBO9781139059060.002 Published online by Cambridge University Press

78, 79]. The formulation of the conjecture stated above is due to Cameron, Frankl and Kantor [38, p. 150].

Following [78], let us briefly explain the connection to n-player games. A *fair game* (or *homogeneous game*) is a method for resolving binary questions without giving any individual player an advantage. If such a game has n players, then it can be modelled mathematically as a family $\mathscr{W}$ of subsets of a set X of size n, called *winning sets*, with the following four properties:

(a) If $A \subseteq B \subseteq X$ and $A \in \mathscr{W}$ then $B \in \mathscr{W}$.
(b) If $A \in \mathscr{W}$ then $X \setminus A \notin \mathscr{W}$.
(c) If $A \notin \mathscr{W}$ then $X \setminus A \in \mathscr{W}$.
(d) If $G \leqslant \mathrm{Sym}(X)$ is the setwise stabiliser of $\mathscr{W}$, then G is transitive on X.

For example, if n is odd then 'majority rules', where $\mathscr{W}$ is the set of all subsets of X of size at least $n/2$, is a fair game.

We claim that the existence of a fair game with n players is equivalent to the existence of a transitive permutation group of degree n with no derangements of 2-power order (see [77, Lemma 1]).

To see this, suppose that $\mathscr{W}$ is a fair game with n players and associated group G. Clearly, if n is odd then G has no derangements of 2-power order, so let us assume that n is even. A derangement in G of 2-power order would map some subset A of size $n/2$ to its complement, but this is ruled out by (b) and (c) above.

Conversely, suppose $G \leqslant \mathrm{Sym}(X)$ is a transitive permutation group of degree n with no derangements of 2-power order. As noted above, if n is odd then G preserves the fair game 'majority rules', so let us assume that n is even. Consider the action of G on the set of subsets of X of size $n/2$, and suppose that G contains an element g that maps such a subset to its complement. Then g is a derangement. Moreover, if the cycles of g have length $n_1, \ldots, n_k$, then g^m is a derangement of 2-power order, where $m = [n_1', \ldots, n_k']$ is the least common multiple of the n_i', and n_i' is the largest odd divisor of n_i. This is a contradiction. Therefore, the orbits of G on the set of subsets of size $n/2$ can be labelled

$$\mathscr{O}_1, \ldots, \mathscr{O}_\ell, \mathscr{O}_1^c, \ldots, \mathscr{O}_\ell^c$$

where $\mathscr{O}_i^c = \{X \setminus A \mid A \in \mathscr{O}_i\}$. Then

$$\mathscr{W} = \{A \subseteq X \mid B \subseteq A \text{ for some } B \in \mathscr{O}_i,\ 1 \leqslant i \leqslant \ell\}$$

is preserved by G and so it models a fair game with n players. This justifies the claim.

Isbell's Conjecture remains an open problem, although some progress has been made in special cases. For example, Bereczky [8] has shown that if $n = p^a b$, where p is an odd prime, $a \geqslant 1$ and $p+1 < b < \frac{3}{2}(p+1)$, then G contains

a derangement of p-power order. An even more general version of Isbell's Conjecture, due to Cameron [35, p. 176], was refuted by Crestani and Spiga [43] for $p \geqslant 5$, and more recently by Spiga [114] for $p = 3$.

1.3.3 Semiregular elements

In view of Theorem 1.3.1, it is natural to ask whether or not every nontrivial finite transitive permutation group contains a derangement of *prime* order. In fact, it is not too difficult to see that there are transitive groups with no such elements, but examples appear to be somewhat rare. Following [39], we say that a transitive permutation group is *elusive* if it does not contain a derangement of prime order. For instance, the 3-transitive action of the smallest Mathieu group M_{11} on 12 points is elusive since M_{11} has a unique conjugacy class of involutions, and also a unique class of elements of order 3 (and moreover, the point stabiliser $\mathrm{PSL}_2(11)$ contains elements of order 2 and 3).

The first construction of an elusive group was given by Fein, Kantor and Schacher in [52]. Let p be a Mersenne prime, let G be the group

$$\mathrm{AGL}_1(p^2) = \{x \mapsto ax + b \mid a, b \in \mathbb{F}_{p^2}, a \neq 0\}$$

of affine transformations of $\mathbb{F}_{p^2}$ and let H be the subgroup of transformations with $a, b \in \mathbb{F}_p$. Then the natural action of G on the set of cosets of H gives a transitive permutation group of degree $p(p+1)$ with the property that all elements of order 2 and p have fixed points. Therefore, G is elusive. Generalisations of this construction are given in [39], producing elusive groups of degree $p^m(p+1)$ for all Mersenne primes p and positive integers m. In particular, this family of examples shows that the natural extension of Isbell's Conjecture, from prime-powers to primes, is false.

A nontrivial permutation is said to be *semiregular* if all of its cycles have the same length. Clearly, a derangement of prime order is semiregular, and since any power of a semiregular element is either trivial or semiregular, the existence of a semiregular element is equivalent to the existence of a derangement of prime order.

Determining the existence of semiregular elements is a classical problem with a long history. For example, Burnside [33, p. 343] showed that if G is a primitive permutation group of degree p^a, where p is a prime and $a > 1$, and G contains a cycle of length p^a, then G is 2-transitive. This was later extended by Schur [112], who proved that any primitive permutation group of composite degree n containing an n-cycle is 2-transitive. The complete list of such 2-transitive groups was later independently determined by Jones [80] and Li [90], following earlier work of Feit [53]. These results have found a wide range

of applications in combinatorics, including coding theory [9], Cayley graphs of cyclic groups (see [91], for example) and rotary embeddings of graphs on surfaces [92]. In a different direction, the existence of semiregular elements has also been used to study tame ramification in number fields [81].

1.3.4 The Polycirculant Conjecture

The notion of a semiregular permutation arises naturally in graph theory. In order to describe the connection, let us recall some standard terminology. A *digraph* Γ consists of a set $V\Gamma$ of vertices and a set $A\Gamma$ of ordered pairs of distinct elements of $V\Gamma$, called *arcs*. If Γ has the property that $(u,v) \in A\Gamma$ if and only if $(v,u) \in A\Gamma$, then Γ is called a *graph*. In this situation, the set of edges of Γ is denoted by $E\Gamma = \{\{u,v\} \mid (u,v) \in A\Gamma\}$, and we say that u is adjacent to v, denoted $u \sim v$, if $\{u,v\} \in E\Gamma$. An *automorphism* of a digraph Γ is a permutation g of $V\Gamma$ such that $(u,v) \in A\Gamma$ if and only if $(u^g, v^g) \in A\Gamma$. We denote the group of all automorphisms of Γ by $\mathrm{Aut}(\Gamma)$. If $\mathrm{Aut}(\Gamma)$ acts transitively on $V\Gamma$ then we say that Γ is *vertex-transitive*. Similarly, Γ is *arc-transitive* if $\mathrm{Aut}(\Gamma)$ acts transitively on $A\Gamma$, and *edge-transitive* if $\mathrm{Aut}(\Gamma)$ acts transitively on $E\Gamma$.

In 1981, Marušič [101, Problem 2.4] asked the following question.

Question. *Does every finite vertex-transitive digraph admit a semiregular automorphism?*

Note that in Marušič's terminology in [101], a digraph Γ is *galactic* if it has a semiregular automorphism. For any prime p, he showed that a transitive permutation group of p-power degree, or degree mp with $m \leqslant p$, has a derangement of order p. The same question for graphs has subsequently been posed by both Leighton [89] and Jordan [83], in 1983 and 1988, respectively.

The existence of a semiregular automorphism is closely related to the notion of a *Cayley digraph*. Given a group G and subset S with $1 \notin S$, the Cayley digraph $\mathrm{Cay}(G,S)$ is the digraph with vertex set G and the property that (g,h) is an arc if and only if $hg^{-1} \in S$. Note that $\mathrm{Cay}(G,S)$ is connected if and only if $G = \langle S \rangle$. If S is symmetric in the sense that $S = S^{-1} := \{s^{-1} \mid s \in S\}$, then (g,h) is an arc if and only if (h,g) is an arc, so in this situation we refer to the *Cayley graph* of G with respect to S. The group G acts on itself by right multiplication, mapping arcs to arcs, and so it induces a regular group of automorphisms of $\mathrm{Cay}(G,S)$ (in particular, $\mathrm{Cay}(G,S)$ is vertex-transitive). Sabidussi [110] showed that a digraph Γ is a Cayley digraph if and only if the full automorphism group of Γ contains a regular subgroup.

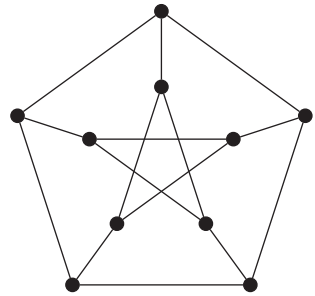

Figure 1.3.1 The Petersen graph

Clearly, every Cayley digraph admits a semiregular automorphism. However, not all vertex-transitive digraphs are Cayley digraphs. For example, it is easy to see that the familiar *Petersen graph* in Figure 1.3.1 is not a Cayley graph, but it visibly has a semiregular automorphism of order 5.

A Cayley digraph of a cyclic group is called a *circulant*. Notice that a circulant with n vertices admits a semiregular automorphism of order n. Similarly, a digraph Γ with n vertices is called a *bicirculant* if it has a semiregular automorphism of order $n/2$; for example, the Petersen graph has this property (with $n = 10$). Bicirculants have been studied by various authors in recent years, see [100] for example, and the notion has been extended to tricirculants, etc.

The existence of a semiregular automorphism of a graph Γ has other applications. For example, it facilitates a particularly succinct notation to describe the vertices and adjacency relation in Γ (see [10, 54], for example). Indeed, if $g \in \mathrm{Aut}(\Gamma)$ is semiregular, with r cycles of length m, then we can represent the graph Γ using only r vertices, with each vertex corresponding to one of the cycles of g. A label $m|k$ on a vertex corresponding to the m-cycle of g containing the vertices $v_1, v_2, \ldots, v_m$ of Γ indicates that each v_i is adjacent to v_{i+k}, where addition is calculated modulo m. Similarly, given two m-cycles $u_1, u_2, \ldots, u_m$ and $v_1, v_2, \ldots, v_m$, an unlabelled edge between the corresponding nodes signifies that u_i is adjacent to v_i, while an edge labelled by a positive integer k means that u_i is adjacent to v_{i+k}. This representation of Γ corresponds to the quotient of Γ by the partition of $V\Gamma$ determined by the cycles of g. This is called the *Frucht notation* for Γ. For instance, the representation of the Petersen graph is given in Figure 1.3.2. This notation can be adjusted appropriately for digraphs.

Semiregular automorphisms of graphs have also been used to construct Hamiltonian paths and cycles. As explained in [1], this can be done by lifting such a path or cycle in the quotient graph corresponding to the semiregular

Figure 1.3.2 Frucht notation for the Petersen graph

automorphism. These automorphisms have also played a role in the enumeration of all vertex-transitive graphs with a small number of vertices (see [103], for example).

The existence of elusive permutation groups implies that there are transitive groups that do not contain semiregular elements. However, not every transitive permutation group is the full automorphism group of a digraph. For example, $G = \mathrm{M}_{11}$ has a 2-transitive action on 12 points, so the only digraphs with 12 vertices that are preserved by G are the complete graph and the edgeless graph on 12 vertices, both of which admit semiregular automorphisms.

In order to generalise Marušič's question, we need the notion of 2-closure. Let G be a permutation group on a finite set Ω. The 2-*closure* of G, denoted by $G^{(2)}$, is the largest subgroup of $\mathrm{Sym}(\Omega)$ that preserves the orbits of G on $\Omega \times \Omega$. For instance, if G is 2-transitive then

$$\{(\alpha,\alpha) \mid \alpha \in \Omega\},\ \ \{(\alpha,\beta) \mid \alpha,\beta \in \Omega, \alpha \neq \beta\}$$

are the orbits of G on $\Omega \times \Omega$, so $G^{(2)} = \mathrm{Sym}(\Omega)$. We say that G is 2-*closed* if $G = G^{(2)}$. Note that the automorphism group $\mathrm{Aut}(\Gamma)$ of a finite digraph Γ is 2-closed: any permutation that fixes the orbits of $\mathrm{Aut}(\Gamma)$ on ordered pairs of vertices also fixes $A\Gamma$ setwise, and is therefore an automorphism of Γ. However, not every 2-closed group is the full automorphism group of a digraph. For example, the regular action of the Klein 4-group $C_2 \times C_2$ on four points is 2-closed, but it is not the full automorphism group of any digraph.

In 1997, Klin [34, Problem 282 (BCC15.12)] extended Marušič's question to 2-closed groups. This is now known as the *Polycirculant Conjecture*.

Conjecture 1.3.4 *Every nontrivial finite transitive* 2*-closed permutation group contains a derangement of prime order.*

One obvious way to attack this conjecture is to determine all elusive groups and show that none are 2-closed. Although elusive groups have been much studied in recent years (see [39, 51, 62] for some specific constructions), a

https://doi.org/10.1017/CBO9781139059060.002 Published online by Cambridge University Press

complete classification remains out of reach. However, the following result of Giudici [61] classifies the quasiprimitive elusive groups.

Theorem 1.3.5 *Let $G \leqslant \mathrm{Sym}(\Omega)$ be an elusive permutation group with a 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 $|\Delta| = 12$.*

The proof of Theorem 1.3.5 relies on the list of pairs (G,H) given in [95, Table 10.7], where G is a simple group and H is a maximal subgroup of G with the property that $|G|$ and $|H|$ have the same set of prime divisors.

None of the groups arising in Theorem 1.3.5 are 2-closed and so every minimal normal subgroup of a counterexample to the Polycirculant Conjecture must be intransitive.

Further progress in this direction has been made by Giudici and Xu in [65], where all the elusive biquasiprimitive permutation groups are determined. (A transitive permutation group is *biquasiprimitive* if it contains a nontrivial intransitive normal subgroup, and all nontrivial normal subgroups have at most two orbits.) As a corollary, it follows that every locally quasiprimitive graph has a semiregular automorphism. (A graph Γ with automorphism group G is *locally quasiprimitive* if for all vertices $v \in \mathrm{V}\Gamma$, the stabiliser G_v acts quasiprimitively on the set of vertices adjacent to v.) This family of graphs includes all arc-transitive graphs of prime valency, and all 2-arc transitive graphs.

Another approach to the Polycirculant Conjecture, and also the original question of Marušič, is to show that digraphs with additional properties must admit a semiregular automorphism. For instance, Marušič and Scapellato [102] showed that every vertex-transitive graph of valency 3, or with $2p^2$ vertices (p a prime), has a semiregular automorphism. Similarly, all vertex-transitive graphs of valency 4 [50], or with a square-free number of vertices [49], also have semiregular automorphisms. In fact, [64] reveals that any vertex-transitive group of automorphisms of a connected graph of valency at most 4 contains a semiregular element, and any vertex-transitive digraph of out-valency at most 3 admits a semiregular automorphism. By the main theorem of [88], all distance-transitive graphs have a semiregular automorphism. This remains an active area of current research.

1.3.5 Derangements of prime order

Let G be a transitive permutation group on a finite set Ω. Notice that G contains a derangement of prime order r only if r divides $|\Omega|$. One of the main aims of

this book is to initiate a quantitative study of derangements of prime order, motivated by the following basic question:

Question. *Let r be a prime divisor of $|\Omega|$. Does G contain a derangement of order r?*

This question leads us naturally to the following *local* notion of elusivity, which was introduced in [23].

Definition 1.3.6 Let G be a transitive permutation group on a finite set Ω and let r be a prime divisor of $|\Omega|$. Then G is *r-elusive* if it does not contain a derangement of order r.

In this terminology, G is elusive if and only if it is r-elusive for every prime divisor r of $|\Omega|$. Similarly, we say that G is *strongly r-elusive* if r divides $|\Omega|$ and G does not contain a derangement of r-power order.

Recall that G is primitive if a point stabiliser G_α is a maximal subgroup of G. The existence of a core-free maximal subgroup imposes restrictions on the abstract structure of G (for instance, it implies that G has at most two minimal normal subgroups). This is formalised in the statement of the O'Nan–Scott Theorem, which describes the structure of a finite primitive permutation group. This important theorem divides primitive groups into a certain number of classes according to the structure of the *socle* (the subgroup generated by the minimal normal subgroups) and the action of a point stabiliser. The precise number of classes depends on how fine a subdivision is required; for example, see [35, Section 4.5] for a subdivision into four classes, and [94] and [109, Section 6] for more refined subdivisions. Roughly speaking, the theorem states that a primitive group $G \leqslant \mathrm{Sym}(\Omega)$ either preserves some natural structure on Ω, for example a product structure, or the structure of an affine space, or there is a nonabelian simple group T such that

$$T \leqslant G \leqslant \mathrm{Aut}(T)$$

In the latter case, G is an *almost simple* group.

In many situations, the O'Nan–Scott Theorem can be used to reduce a general problem concerning primitive groups to the almost simple case. At this point, the Classification of Finite Simple Groups can be invoked to describe the possibilities for T (and thus G), and the vast literature on finite simple groups (in particular, information on their subgroup structure, conjugacy classes and representations) can be brought to bear on the problem.

For example, in order to determine all the r-elusive primitive permutation groups, the O'Nan–Scott Theorem was used in [23] to establish the following reduction theorem (see [23, Theorem 2.1]).

Theorem 1.3.7 *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group with socle N. Let r be a prime divisor of $|\Omega|$. Then one of the following holds:*

(i) *G is almost simple;*
(ii) *N contains a derangement of order r;*
(iii) *$G \leqslant H \wr S_k$ acting with its product action on $\Omega = \Delta^k$ for some $k \geqslant 2$, where $H \leqslant \mathrm{Sym}(\Delta)$ is primitive, almost simple and the socle of H is r-elusive.*

In view of Theorem 1.3.7, we may focus our attention on the almost simple primitive groups. Let G be such a group, with socle T. By the Classification of Finite Simple Groups, there are four cases to consider:

(a) T is an alternating group A_n of degree $n \geqslant 5$;
(b) T is one of 26 sporadic simple groups;
(c) T is a simple classical group;
(d) T is a simple group of exceptional Lie type.

By Theorem 1.3.5, the 3-transitive action of M_{11} on 12 points is the only almost simple primitive elusive group.

All the r-elusive groups in cases (a) and (b) are determined in [23]. For example, in case (a) the main theorem is the following (see [23, Section 3]).

Theorem 1.3.8 *Let $G = A_n$ or S_n be an almost simple primitive permutation group on a set Ω with point stabiliser H. Let r be a prime divisor of $|\Omega|$.*

(i) *If H acts primitively on $\{1,\ldots,n\}$, then G is r-elusive if and only if $r = 2$ and $(G,H) = (A_5, D_{10})$ or $(A_6, \mathrm{PSL}_2(5))$.*
(ii) *Let Ω be the set of partitions of $\{1,\ldots,n\}$ into b parts of size a with $a,b \geqslant 2$. Write $a \equiv \ell \pmod r$ and $b \equiv k \pmod r$ with $0 \leqslant \ell,\ k < r$. Then G is r-elusive if and only if $r \leqslant a$ and one of the following holds:*
   (a) *$\ell = 0$;*
   (b) *$k = 0$ and $\ell = 1$;*
   (c) *$0 < k\ell < r$ and either $b < r$ or $(k+r)\ell \leqslant ka + r$.*
(iii) *Let Ω be the set of k-element subsets of $\{1,\ldots,n\}$ with $1 \leqslant k < n/2$. Write $n \equiv i \pmod r$ and $k \equiv j \pmod r$ with $0 \leqslant i, j < r$.*
   (a) *If r is odd, then G is r-elusive if and only if $r \leqslant k$ and $i \geqslant j$.*
   (b) *G is 2-elusive if and only if k is even, or n is odd, or $G = A_n$ and $n/2$ is odd.*

https://doi.org/10.1017/CBO9781139059060.002 Published online by Cambridge University Press

Table 1.4.1 *The finite simple classical groups*

Type	Notation	Conditions
Linear	$\mathrm{PSL}_n(q)$	$n \geqslant 2$, $(n,q) \neq (2,2),(2,3)$
Unitary	$\mathrm{PSU}_n(q)$	$n \geqslant 3$, $(n,q) \neq (3,2)$
Symplectic	$\mathrm{PSp}_n(q)'$	$n \geqslant 4$ even
Orthogonal	$\Omega_n(q)$	nq odd, $n \geqslant 7$
	$\mathrm{P}\Omega_n^{\pm}(q)$	$n \geqslant 8$ even

Further results are established in [23]. For example, the conjugacy classes of derangements of prime order are determined for almost all primitive actions of almost simple sporadic groups (including the *Baby Monster* sporadic group for example, and almost all primitive actions of the *Monster*). In addition, the strongly r-elusive primitive actions of the almost simple groups with socle an alternating or sporadic group are determined in [23]. We also show that if r is the largest prime divisor of $|\Omega|$, then such a group G contains a derangement of order r, unless $G = \mathrm{M}_{11}$, $|\Omega| = 12$ and $r = 3$ (see [23, Corollary 1.2]).

In view of Theorem 1.3.7, and the work in [23], the challenge now is to extend the study of r-elusivity to almost simple groups of Lie type. Here we will focus on classical groups; derangements of prime order in almost simple groups of exceptional Lie type will be investigated in future work.

1.4 Derangements in classical groups

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive almost simple classical group over $\mathbb{F}_q$ with socle T and natural (projective) module V of dimension n. Let $H = G_\alpha$ be a point stabiliser. The possibilities for T (up to isomorphism) are listed in Table 1.4.1. These groups will be formally introduced in Chapter 2, where the notation and given conditions will be explained. In Chapter 2 we will also describe the associated geometries and automorphisms of the classical groups.

We are interested in the following problem:

Problem 1.4.1 *For each prime divisor r of $|\Omega|$, determine whether T is r-elusive, that is, determine whether or not T contains a derangement of order r.*

Let x be an element of T. Recall that

(i) H is a maximal subgroup of G such that $G = HT$, and
(ii) x is a derangement if and only if $x^G \cap H$ is empty.

https://doi.org/10.1017/CBO9781139059060.002 Published online by Cambridge University Press

Therefore, in order to attack Problem 1.4.1 we require detailed information on the subgroup structure of G (in order to determine the possibilities for H). We also need a description of the G-classes of elements of prime order in T, and we need to study the fusion of the H-classes of such elements in G (to determine whether $x^G \cap H$ is non-empty for all $x \in T$ of a given prime order).

In view of (ii) above, our aim in Chapter 3 is to bring together a range of results on conjugacy classes of elements of prime order in the finite classical groups. Most of these results can be found in the literature, in one form or another, but it is desirable to have a single reference for this important information. Indeed, a detailed description of conjugacy classes is essential for our application to derangements, and more generally we expect that the content of Chapter 3 will be useful in many other problems involving finite classical groups.

Let V be the natural T-module, let $x \in T$ be an element of prime order r, and write $q = p^f$ where p is a prime. (Here V is an n-dimensional vector space over $\mathbb{F}_{q^u}$, where $u = 2$ if T is a unitary group, otherwise $u = 1$.) Let $\mathbb{F}$ be the algebraic closure of $\mathbb{F}_q$ and set $\overline{V} = V \otimes \mathbb{F}$. Since $x \in \mathrm{PGL}(V)$, we may define $\hat{x} \in \mathrm{GL}(\overline{V})$ to be a preimage of x.

In order to describe the conjugacy class of x in G, we distinguish the cases $r = p$ and $r \neq p$. In the former case, x is a *unipotent* element; 1 is the only eigenvalue of $\hat{x}$ on $\overline{V}$, and the G-class of x is essentially determined by the Jordan block structure of $\hat{x}$ on $\overline{V}$. If $r \neq p$ then x is *semisimple*; here $\hat{x} \in \mathrm{GL}(\overline{V})$ is diagonalisable and the G-class of x can typically be described in terms of the multiset of eigenvalues of $\hat{x}$ on $\overline{V}$. In both cases we will discuss class representatives, and we will provide information on the centraliser $C_G(x)$ and the type of subspace decompositions of V fixed by x. Some of these results are conveniently summarised in the tables in Appendix B. We will also discuss the conjugacy classes of outer automorphisms of T of prime order.

The case $r = 2$ requires special attention. Indeed, our treatment of semisimple involutions is one of the main features of Chapter 3. This detailed analysis is needed for the application to derangements, and more generally it is designed to complement the extensive information in [67, Table 4.5.1] by Gorenstein, Lyons and Solomon.

The main theorem on the subgroup structure of finite classical groups is due to Aschbacher. In [3], Aschbacher introduces eight *geometric* families of subgroups of G, denoted by $\mathscr{C}_i$ ($1 \leqslant i \leqslant 8$), which are defined in terms of the underlying geometry of the natural T-module V. For example, these collections include the stabilisers of suitable subspaces of V, and the stabilisers of appropriate direct sum and tensor product decompositions of V. Essentially, Aschbacher's main theorem states that if H is a maximal subgroup of G with

Table 1.4.2 *Aschbacher's subgroup collections*

Collection	Description
$\mathscr{C}_1$	Stabilisers of subspaces, or pairs of subspaces, of V
$\mathscr{C}_2$	Stabilisers of decompositions $V = \bigoplus_{i=1}^{t} V_i$, where $\dim V_i = a$
$\mathscr{C}_3$	Stabilisers of prime degree extension fields of $\mathbb{F}_q$
$\mathscr{C}_4$	Stabilisers of decompositions $V = V_1 \otimes V_2$
$\mathscr{C}_5$	Stabilisers of prime index subfields of $\mathbb{F}_q$
$\mathscr{C}_6$	Normalisers of symplectic-type r-groups, $r \neq p$
$\mathscr{C}_7$	Stabilisers of decompositions $V = \bigotimes_{i=1}^{t} V_i$, where $\dim V_i = a$
$\mathscr{C}_8$	Stabilisers of nondegenerate forms on V
$\mathscr{S}$	Almost simple absolutely irreducible subgroups
$\mathscr{N}$	Novelty subgroups ($T = \mathrm{P}\Omega_8^+(q)$ or $\mathrm{Sp}_4(q)'$ $(p = 2)$, only)

$HT = G$, then either H is contained in one of the $\mathscr{C}_i$ collections, or H is almost simple and the socle of H acts absolutely irreducibly on V. Following [86], we use $\mathscr{S}$ to denote the latter collection of *non-geometric* subgroups. It turns out that a small additional subgroup collection (denoted by $\mathscr{N}$) arises when $T = \mathrm{Sp}_4(q)'$ (with $p = 2$) or $\mathrm{P}\Omega_8^+(q)$, due to the existence of certain exceptional automorphisms. A brief description of these subgroup collections is presented in Table 1.4.2, and we refer the reader to Section 2.6 for further details.

Our study of derangements in finite classical groups is organised in terms of the subgroup collections in Table 1.4.2. The *subspace actions* corresponding to subgroups in $\mathscr{C}_1$ require special attention, and they are handled first in Chapter 4. Here we need to determine whether a given prime order element in T fixes an appropriate subspace (or pair of subspaces) of V. In order to answer this question, we need the detailed information on conjugacy class representatives recorded in Chapter 3 (in particular, we need to understand the subspace decompositions of V fixed by such elements). The remaining geometric subgroup collections $\mathscr{C}_i$, with $2 \leqslant i \leqslant 8$, are handled in Chapter 5, together with the small collection of *novelty* subgroups denoted by $\mathscr{N}$. In Chapter 6, we present detailed results on the r-elusivity of the low-dimensional almost simple classical groups.

Rather different techniques are required to deal with the non-geometric actions corresponding to the subgroups in the collection $\mathscr{S}$. If H is such a subgroup of G, with (simple) socle S, then there exists an absolutely irreducible representation $\rho : \hat{S} \to \mathrm{GL}(V)$, where $\hat{S}$ is a covering group of S. However, it is not easy to use this representation-theoretic description of the embedding of H in G to study the fusion of H-classes in G (of course, even the dimensions of the irreducible $\mathbb{F}_q\hat{S}$-modules are not known, in general). Therefore, a somewhat different approach is required, and we will study the r-elusivity of $\mathscr{S}$-actions of finite classical groups in a separate paper.

https://doi.org/10.1017/CBO9781139059060.002 Published online by Cambridge University Press

1.5 Main results

We are now in a position to discuss some of our main results on derangements of prime order in almost simple classical groups. More detailed results will be presented in Chapters 4, 5 and 6; some of these statements are necessarily somewhat involved, with reference to a number of tables, so in this section we will state simplified versions. We also give precise references for the more detailed statements that can be found later in the text.

As before, let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive almost simple classical group over $\mathbb{F}_q$ with socle T and natural (projective) module V of dimension n. Let $H = G_\alpha$ be a point stabiliser, and define the subgroup collections as in Table 1.4.2. Write $q = p^f$, where p is a prime, and assume that $H \notin \mathscr{S}$.

Theorem 1.5.1 *Let r be a prime divisor of $|\Omega|$.*

(i) *If $H \in \mathscr{C}_1 \cup \mathscr{C}_2$, $r = p > 2$ and T is r-elusive, then (G,H) belongs to a known list of cases.*
(ii) *In all other cases, T is r-elusive if and only if (G,H,r) belongs to a known list of cases.*

Remark 1.5.2 Some comments on the statement of Theorem 1.5.1.

(a) For $H \in \mathscr{C}_1 \cup \mathscr{C}_2$, we refer the reader to the theorems referenced in Table 1.5.1, which provide detailed results. For example, if $H \in \mathscr{C}_1$ and $r \neq p$ is odd, then T is r-elusive if and only if (G,H,r) is one of the cases recorded in Theorem 4.1.6. As indicated in Theorems 4.1.4 and 5.2.1, in some (but not all) cases we are able to present necessary and sufficient conditions for r-elusivity when $r = p > 2$, which typically depend on number-theoretic properties of partitions of n.
(b) If $H \in \mathscr{C}_i$ (with $3 \leqslant i \leqslant 8$), then the precise conditions for r-elusivity are stated in Theorem 5.i.1 and the specific cases that arise are listed in Table 5.i.2 (for $i \neq 7$). We find that the collection of primes r for which T is r-elusive is rather restricted:
- If $H \in \mathscr{C}_4 \cup \mathscr{C}_7$ then T is r-elusive only if $r = 2$.
- If $H \in \mathscr{C}_3$ and T is r-elusive then either $r = 2$, or $T = \mathrm{PSL}^\varepsilon_n(q)$, H is of type $\mathrm{GL}^\varepsilon_{n/k}(q^k)$ and $r = k$.
- If $H \in \mathscr{C}_5$ is a subfield subgroup over $\mathbb{F}_{q_0}$, where $q = q_0^k$, then T is r-elusive only if $r \in \{2,3,5,k,p\}$.
- If $H \in \mathscr{C}_6$ then T is r-elusive only if $r \leqslant 3$, or if r is a Mersenne or Fermat prime.
- If $H \in \mathscr{C}_8$ then T is r-elusive only if $r \in \{2,3,5,p\}$.

https://doi.org/10.1017/CBO9781139059060.002 Published online by Cambridge University Press

Table 1.5.1 *References for $\mathscr{C}_i$-actions, $i = 1,2$*

	$r = p > 2$	$r \neq p, r > 2$	$r = 2$
$\mathscr{C}_1$	4.1.4	4.1.6	4.1.7
$\mathscr{C}_2$	5.2.1	5.2.3	5.2.5

(c) By definition, if T is not r-elusive then T contains a derangement of order r. In this situation, specific derangements are usually identified in the proofs of the main theorems.

In the next theorem, we highlight the special case $r = 2$.

Theorem 1.5.3 *T is 2-elusive if and only if $|\Omega|$ is even and (G,H) is one of the cases in Table 4.1.3 (for $H \in \mathscr{C}_1$) or Table 5.1.2 (in all other cases).*

We say that T is $2'$*-elusive* if $|\Omega|$ is divisible by an odd prime, but T does not contain a derangement of odd prime order.

Theorem 1.5.4 *Let G be a primitive almost simple classical group with socle T. Then T is not $2'$-elusive.*

This is a special case of the main theorem of [22], which describes the structure of quasiprimitive and biquasiprimitive groups that are $2'$-elusive. In particular, if G is a primitive almost simple group with socle T and point stabiliser H, then T is $2'$-elusive if and only if (G,H) is one of the following (in terms of the Atlas [41] notation):

$$(\mathrm{M}_{11}, \mathrm{PSL}_2(11)),\ ({}^2F_4(2)', \mathrm{PSL}_2(25)),\ ({}^2F_4(2), \mathrm{PSL}_2(25).2_3)$$

Our final theorem concerns the r-elusivity of the low-dimensional classical groups with $n \leqslant 5$.

Theorem 1.5.5 *Let G be a primitive almost simple classical group with socle T and point stabiliser H, where*

$$T \in \{\mathrm{PSL}_2(q), \mathrm{PSL}_3^{\varepsilon}(q), \mathrm{PSL}_4^{\varepsilon}(q), \mathrm{PSp}_4(q)', \mathrm{PSL}_5^{\varepsilon}(q)\} \tag{1.5.1}$$

Let r be a prime. Then T is r-elusive if and only if (G,H,r) is one of the cases recorded in Tables 6.4.1–6.4.8.

The proof of Theorem 1.5.5 is given in Chapter 6. For $H \notin \mathscr{S}$, this is a corollary of Theorem 1.5.1, noting that it is straightforward to determine

https://doi.org/10.1017/CBO9781139059060.002 Published online by Cambridge University Press

necessary and sufficient conditions in part (i) when n is small. A complete list of the subgroups in $\mathscr{S}$ is given in [13, Chapter 8] (also see Table 6.3.1), and we study each possibility in turn, working with the corresponding irreducible representation (and its character) to investigate the fusion of H-classes in G.

Corollary 1.5.6 *Let G be a primitive almost simple classical group over $\mathbb{F}_q$ with point stabiliser H and socle T as in* (1.5.1)*. Let $r > 5$ be a prime. Then T is r-elusive only if one of the following holds:*

(i) $H \in \mathscr{C}_5$ *is a subfield subgroup over* $\mathbb{F}_{q_0}$*, where* $q = q_0^k$ *and* $r \in \{k, p\}$.
(ii) $T = \mathrm{PSL}_n(q)$*,* $n \in \{3,5\}$ *and H is a* $\mathscr{C}_8$*-subgroup of type* $\mathrm{GU}_n(q_0)$*, where* $q = q_0^2$ *and* $r = p$.
(iii) $H \in \mathscr{S}$ *has socle S and* (T,S,r) *is one of the following:*
  (a) $T = \mathrm{PSL}_5^{\varepsilon}(q)$*,* $S = \mathrm{PSL}_2(11)$ *and* $r = 11$*;*
  (b) $T = \mathrm{PSL}_5(3)$*,* $S = \mathrm{M}_{11}$ *and* $r = 11$*;*
  (c) $T = \mathrm{PSL}_4^{\varepsilon}(q)$*,* $S = A_7$ *or* $\mathrm{PSL}_2(7)$*, and* $r = 7$*;*
  (d) $T = \mathrm{PSL}_3^{\varepsilon}(q)$*,* $S = \mathrm{PSL}_2(7)$ *and* $r = 7$.

https://doi.org/10.1017/CBO9781139059060.002 Published online by Cambridge University Press