Young Algebraists' Conference
(Lausanne, June 2014)

Topics in Permutation Group Theory

Lectures by

Tim Burness
(University of Bristol, UK)

Contents

1 Introduction

The study of permutation groups is an old subject with a rich history, stretching all the way back to the origins of group theory in the early 19th century. Galois introduced the notion of a group in his study of the permutations of roots of polynomial equations (the familiar *Galois group* of the polynomial), and *groups of substitutions* (what we now call *permutation groups*) were a focus of interest for much of the 19th century. Of course, the modern notion of a permutation group is extremely flexible, and they arise naturally throughout mathematics, with important applications across the sciences.

For instance, given any mathematical object or structure Σ (e.g. vector space, group, graph, topological space, etc.) based on a set of points Ω (e.g. vectors, group elements, vertices, points, etc.) then the set $\mathrm{Aut}(\Sigma)$ of *automorphisms* (or *symmetries*) of Σ (i.e. the bijective maps $f : \Omega \to \Omega$ such that f and f^{-1} preserve the structure of Σ) is a permutation group on Ω. That is, $\mathrm{Aut}(\Sigma)$ is a group of bijections from Ω to itself. By Cayley's Theorem, *every* group can be viewed as a permutation group on some set!

1.1 Main themes

There is a vast literature on permutation groups and so we have had to be very selective in choosing the topics for these lectures. In particular, we will focus on *finite* permutation groups, which continues to be a very active area of current research. The topics have been chosen to illustrate the development of the subject, from classical results proved in the 19th century, through to cutting-edge advances in much more recent times. The topics also highlight some of the applications of permutation group theory in other areas of mathematics, and they provide an opportunity to discuss a number of interesting open problems. Let me highlight three main themes:

1. *Primitivity.* The notion of primitivity is fundamental in permutation group theory. It is best viewed as a natural *irreducibility* condition, and in some sense the primitive groups are the "basic building blocks" of all permutation groups.
2. *Impact of CFSG.* In the last 30 years, the Classification of Finite Simple Groups (CFSG) has revolutionised the study of finite permutation groups. We will explain why, and discuss some of the far-reaching consequences.
3. *Applications.* Some of the topics we will discuss have interesting connections to other areas of mathematics, such as combinatorics, representation theory, number theory, graph theory, etc., and we will highlight these applications.

A rough overview of the five lectures is presented in Table 1.1.

Lectures	Overview
I, II	**Primitivity:** Basic properties; O'Nan-Scott Theorem and applications
	Variations on the theme of primitivity
III, IV	**Derangements:** Counting; order; elusivity; applications
IV, V	**Bases:** Applications; bounds; probabilistic methods
	Bases for algebraic groups (time permitting...)

Table 1.1: Organisation of lectures

1.2 Further reading

There are several standard references for permutation groups:

- P.J. Cameron, *Permutation groups*, London Math. Soc. Student Texts, vol. 45, CUP, 1999.

- J.D. Dixon and B. Mortimer, *Permutation groups*, Springer Graduate Texts in Math., vol. 163, Springer, 1996.
- D.S. Passman, *Permutation groups*, Dover Publications, 2012 (reprint of 1968 original).
- H. Wielandt, *Finite permutation groups*, Academic Press, 1964.

Many more specific references are provided in the bibiliography (see Section 7). There are also some good notes available online (easily found by Googling). For example:

- J. Bamberg, *Permutation Group Theory*, RMIT Summer Course notes, 2006.
- J.B. Fawcett, *The O'Nan-Scott theorem for finite primitive permutation groups, and finite representability*, Masters thesis, University of Waterloo, 2009.

There are also some excellent mathematical blogs that frequently discuss permutation groups (and many other interesting topics!). Here are two good examples:

- *Peter Cameron's Blog:* `http://cameroncounts.wordpress.com`
- *SymOmega:* `http://symomega.wordpress.com`

2 Basic notions

In this section we briefly recall some basic concepts and constructions that we will need later. We also fix some of the notation we will use throughout these notes.

2.1 Permutation groups

Let G be a group, let Ω be a set and let $\mathrm{Sym}(\Omega)$ be the group of all permutations of Ω. An *action* of G on Ω is a homomorphism $\varphi : G \to \mathrm{Sym}(\Omega)$, and we say that Ω is a *G-set*. For $x \in G$, $\alpha \in \Omega$ we write α^x to denote the element $\alpha(x\varphi) \in \Omega$. The image of φ, denoted G^Ω, is a subgroup of $\mathrm{Sym}(\Omega)$. In other words, G^Ω is a *permutation group* on Ω. The *degree* of G^Ω is the cardinality of Ω. We say that G is *faithful* (or equivalently, Ω is a faithful G-set) if $\ker(\varphi) = 1$, in which case $G \cong G^\Omega$.

For $x \in G$ and $\alpha \in \Omega$ we define

$$\begin{aligned} \alpha^G &= \{\alpha^x \mid x \in G\} \\ G_\alpha &= \{x \in G \mid \alpha^x = \alpha\} \\ C_\Omega(x) &= \{\alpha \in \Omega \mid \alpha^x = \alpha\} \\ \mathrm{supp}(x) &= \{\alpha \in \Omega \mid \alpha^x \neq \alpha\} \end{aligned}$$

the *orbit* of α, *stabiliser* of α, *fixed point set* of x, and *support* of x, respectively. Recall that G_α is a subgroup of G and we have $G_{\alpha^x} = (G_\alpha)^x = x^{-1}G_\alpha x$. By the Orbit-Stabiliser theorem, there is a bijection between α^G and the set of cosets of G_α in G. The orbits are the equivalence classes with respect to the relation $\sim$ on Ω, where $\alpha \sim \beta$ if and only if $\alpha^x = \beta$ for some $x \in G$, so the set of orbits form a partition of Ω. Then G is *transitive* (or equivalently, Ω is a transitive G-set) if there is only one orbit, namely Ω. Note that if G is transitive, then $\ker(\varphi) = \bigcap_{x\in G}(G_\alpha)^x$, so G is faithful if and only if G_α is core-free.

We say that G is *semiregular* if $G_\alpha = 1$ for all $\alpha \in \Omega$, and *regular* if it is both semiregular and transitive. In a transitive action, the orbits of G_α on Ω are called *suborbits*, and the number of such orbits is called the *rank* of G. Given a positive integer k, we say that G is *k-transitive* on Ω if it acts transitively on the set of all k-tuples of distinct elements of Ω, in terms of the componentwise action

$$(\alpha_1, \ldots, \alpha_k)^x = (\alpha_1^x, \ldots, \alpha_k^x).$$

Note that if $k \geqslant 2$ then G is k-transitive on Ω if and only if G is transitive on Ω and G_α is $(k-1)$-transitive on $\Omega \setminus \{\alpha\}$. In particular, G is 2-transitive if and only if the rank of G is two.

Two G-sets Ω and Γ are *isomorphic*, denoted $\Omega \cong \Gamma$, if there exists a bijection $\varphi : \Omega \to \Gamma$ such that $(\alpha^x)\varphi = (\alpha\varphi)^x$ for all $\alpha \in \Omega$ and $x \in G$. For example, $\alpha^G \cong G/G_\alpha$ (in terms of the natural action of G on the set of cosets G/G_α). In particular, if G is transitive then $\Omega \cong G/G_\alpha$, hence $\Omega \cong G$ if G is regular, where G acts on itself by right multiplication.

The permutation groups $H \leqslant \mathrm{Sym}(\Gamma)$ and $K \leqslant \mathrm{Sym}(\Delta)$ are *permutation isomorphic* if there exists a bijection $\varphi : \Gamma \to \Delta$ and an isomorphism $\psi : H \to K$ such that

$$(\gamma^x)\varphi = (\gamma\varphi)^{x\psi}$$

for all $\gamma \in \Gamma$ and $x \in H$. In other words, H and K are 'the same', up to a relabelling of elements.

Examples 2.1.

(i) The standard action of the symmetric group $G = S_n$ on $\{1, \ldots, n\}$ is faithful, n-transitive and $G_\alpha = S_{n-1}$. Similarly, the standard action of the alternating group A_n is $(n-2)$-transitive (but not $(n-1)$-transitive).

(ii) The standard action of the dihedral group D_{2n} (with $n \geqslant 3$) on the set of n vertices of a regular n-gon is faithful and transitive, but it is only 2-transitive if $n = 3$.

(iii) Fix an integer $1 < k < m$. Then $G = S_m$ acts faithfully and transitively on the set of k-element subsets of $\{1, \ldots, m\}$, where the action is defined by $\Gamma^x = \{\gamma^x \mid \gamma \in \Gamma\}$. Here $G_\Gamma = S_k \times S_{m-k}$ and the degree of G is $\binom{m}{k}$. The actions of G on k-sets and $(m-k)$-sets are isomorphic. If $k \leqslant m/2$ and Γ is a fixed k-set, then the suborbits of G_Γ are

$$\Phi_i = \{\Lambda : |\Lambda \cap \Gamma| = i\},\ i = 0, \ldots, k.$$

Therefore, G has rank $k+1$.

(iv) The general linear group $\mathrm{GL}_d(q)$ acts faithfully and intransitively on $V = (\mathbb{F}_q)^d$; the orbits are $\{0\}$ and $\{v \in V \mid v \neq 0\}$. The natural action on vectors induces an action on the set of 1-dimensional subspaces of V, which is 2-transitive, but only faithful if $q = 2$; the kernel is the centre Z of $\mathrm{GL}_d(q)$ (that is, the scalar matrices). The corresponding (faithful) action of $\mathrm{PGL}_d(q) = \mathrm{GL}_d(q)/Z$ is 2-transitive; this is called the *standard action* of $\mathrm{PGL}_d(q)$.

(v) Let G be a group and consider the natural action of G on the coset spaces G/H and G/K, where H, K are subgroups of G. These two G-sets are isomorphic if and only if H and K are conjugate.

2.2 Wreath products

Wreath products are fundamental constructions in permutation group theory. Let $H \leqslant \mathrm{Sym}(\Gamma)$ and $K \leqslant \mathrm{Sym}(\Delta)$ be permutation groups, where $|\Gamma|, |\Delta| \geqslant 2$ and $\Delta = \{1, \ldots, n\}$. Let H^n denote the direct product of n copies of H. Then K acts naturally on H^n by permuting the n factors; more precisely, $k \in K$ acts on $(h_1, \ldots, h_n)$ by moving h_i to the i^k-th coordinate, so

$$(h_1, \ldots, h_n)^k = (h_{1^{k^{-1}}}, \ldots, h_{n^{k^{-1}}}).$$

The *wreath product* of H and K, denoted by $H \wr K$, is the corresponding semidirect product $H^n K$, so the group operation is defined as follows:

$$\begin{aligned}(a_1, \ldots, a_n)k \cdot (b_1, \ldots, b_n)\ell &= (a_1, \ldots, a_n)(b_1, \ldots, b_n)^{k^{-1}} k\ell \\ &= (a_1 b_{1^k}, \ldots, a_n b_{n^k})k\ell\end{aligned}$$

The direct product H^n is called the *base group* of $H \wr K$, and K is the *top group*.

Set $G = H \wr K$. There is a faithful action of G on $\Omega = \Gamma \times \Delta$ defined by

$$(\gamma, i)^{(h_1, \ldots, h_n)k} = (\gamma^{h_i}, i^k). \tag{2.1}$$

We call this the *standard action* of G. Note that G is transitive if and only if H and K are both transitive. Also note that the partition $\{\Gamma \times \{i\} \mid 1 \leqslant i \leqslant n\}$ of Ω is G-invariant.

There is also a natural faithful action of G on the Cartesian product $\Omega = \Gamma^n$ defined by

$$(\gamma_1, \ldots, \gamma_n)^{(h_1, \ldots, h_n)k} = \left(\left(\gamma_{1^{k^{-1}}}\right)^{h_{1^{k^{-1}}}}, \ldots, \left(\gamma_{n^{k^{-1}}}\right)^{h_{n^{k^{-1}}}} \right). \tag{2.2}$$

This is called the *product action* of G. Note that this is simply a combination of the coordinatewise action of H^n on Ω, together with the natural permuting action of K on coordinates. To check that this is indeed an action, let

$$x = (a_1, \ldots, a_n)k^{-1},\ y = (b_1, \ldots, b_n)\ell^{-1},\ \alpha = (\gamma_1, \ldots, \gamma_n) \in \Omega.$$

Now $xy = (a_1 b_{1^{k^{-1}}}, \ldots, a_n b_{n^{k^{-1}}})(\ell k)^{-1}$ and thus

$$\alpha^{xy} = \left((\gamma_{1\ell k})^{a_1 \ell k b_{1^{(\ell k)k^{-1}}}}, \ldots, (\gamma_{n\ell k})^{a_{n\ell k} b_{n^{(\ell k)k^{-1}}}} \right) = \left((\gamma_{1\ell k})^{a_1 \ell k b_{1^\ell}}, \ldots, (\gamma_{n\ell k})^{a_{n\ell k} b_{n^\ell}} \right)$$

and

$$(\alpha^x)^y = ((\gamma_{1^k})^{a_{1^k}}, \ldots, (\gamma_{n^k})^{a_{n^k}})^y = \left((\gamma_{1\ell k})^{a_1 \ell k b_{1^\ell}}, \ldots, (\gamma_{n\ell k})^{a_{n\ell k} b_{n^\ell}} \right)$$

as required.

For example, consider the wreath product $G = S_3 \wr S_2$, which is a group of order $(3!)^2(2!) = 72$. The standard action embeds G in S_6; up to conjugacy, we may view G as the stabiliser in S_6 of the partition $\{1,2,3\} \cup \{4,5,6\}$, where the base group, $S_3 \times S_3$, fixes both parts of the partition, and the top group S_2 swaps the two parts. Similarly, the product action embeds G in S_9.

2.3 Simple groups

Let's start by recalling the Classification theorem.

Theorem 2.2 (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) *Z_p for a prime p;*

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

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

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

Let T be a nonabelian finite simple group with automorphism group $\mathrm{Aut}(T)$. Let $\varphi : T \to \mathrm{Aut}(T)$ be the map sending $t \in T$ to the inner automorphism φ_t induced by conjugation by t. Since $Z(T) = 1$, φ is a monomorphism, so we may identify T with $\mathrm{im}(\varphi) = \mathrm{Inn}(T)$.

A finite group G is *almost simple* if there exists a nonabelian finite simple group T such that

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

We say that T is the *socle* of G. For example, S_n is almost simple if $n \geqslant 5$, and $\mathrm{PGL}_n(q)$ is almost simple for all $n \geqslant 2$ and prime-powers q (unless $(n,q) = (2,2)$ or $(2,3)$).

We define $\mathrm{Out}(T) = \mathrm{Aut}(T)/T$. The structure of $\mathrm{Out}(T)$ is well understood; indeed, the following result is an important corollary of Theorem 2.2 (no direct proof is known):

Theorem 2.3 (Schreier Conjecture)**.** *Let T be a nonabelian finite simple group. Then* $\mathrm{Out}(T)$ *is soluble.*

For example, if $T = A_n$ then $\mathrm{Out}(T) \cong Z_2 \times Z_2$ if $n = 6$, otherwise $\mathrm{Out}(T) \cong Z_2$. Similarly, if $T = \mathrm{PSL}_n(q)$ and $q = p^f$ (with p prime), then $\mathrm{Out}(T) \cong Z_{(n,q-1)} \rtimes (Z_f \times Z_a)$, where $a = 2$ if $n \geqslant 3$, otherwise $a = 1$.

The next result records two more additional facts that will be useful later:

Proposition 2.4. *Let G be an almost simple group with socle T. The following hold:*

(i) *$C_G(T) = 1$;*

(ii) *If $k \in \mathbb{N}$, then $\mathrm{Aut}(T^k) \cong \mathrm{Aut}(T) \wr S_k$.*

Proof. First consider (i). It suffices to show that $C_{\mathrm{Aut}(T)}(\mathrm{Inn}(T)) = 1$. Since $Z(T) = 1$, the map $\varphi : T \to \mathrm{Inn}(T)$, $t \mapsto \varphi_t$, is an isomorphism, where $x\varphi_t = t^{-1}xt$ for all $x \in T$. Let $\psi \in C_{\mathrm{Aut}(T)}(\mathrm{Inn}(T))$ and fix $s,t \in T$. Then

$$t^{-1}st = s\varphi_t = s(\psi^{-1}\varphi_t\psi) = s\varphi_{t\psi} = (t\psi)^{-1}s(t\psi)$$

and thus $(t\psi)t^{-1} \in Z(T) = 1$, so $t\psi = t$ for all t and thus $\psi = 1$.

For part (ii), see [38, Exercise 4.3.9] (or [39, Proposition 1.6.1]). □

It is difficult to overestimate the impact of CFSG on the study of finite permutation groups – this will be a common theme throughout these notes. In order to fully exploit the classification, one often needs detailed information on the structure of the simple groups themselves, in terms of subgroups, representations and conjugacy classes of elements, for example.

The problem of determining the maximal subgroups of simple groups dates back to Galois' letter to Chevalier on the eve of his fatal duel in 1832, and it continues to be a major area of research. Many important advances have been made post-CFSG, and there is a vast literature in this area (see [12, 35, 63], for example). For example, for simple groups of Lie type there are very powerful reduction theorems due to Aschbacher, Liebeck, Seitz and others that play a major role in the study of permutation groups. The connection is transparent: the transitive actions of a simple group G correspond to the conjugacy classes of subgroups of G, and we will see that the *primitive* actions correspond to conjugacy classes of *maximal* subgroups. Moreover, many general questions concerning finite permutation groups can be reduced to the simple (or almost simple) case, using powerful tools such as the *O'Nan-Scott Theorem*, as we shall see in Sections 3 – 5.

2.4 The socle

Let G be a finite group. The subgroup of G generated by the minimal normal subgroups of G is called the *socle* of G, denoted $\mathrm{Soc}(G)$ (recall that a nontrivial normal subgroup N of G is *minimal* if it does not properly contain a nontrivial normal subgroup of G).

Lemma 2.5. *Let G be a finite group.*

(i) *Any two distinct minimal normal subgroups of G commute. In particular, $\mathrm{Soc}(G)$ is a direct product of distinct minimal normal subgroups of G.*

(ii) *Every minimal normal subgroup of G is a direct product of isomorphic simple groups.*

Proof.

(i) If N_1, N_2 are distinct minimal normal subgroups of G, then $[N_1,N_2] \leqslant N_1 \cap N_2 \trianglelefteq G$, so $[N_1,N_2] = N_1 \cap N_2 = 1$ by minimality.

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

2.5 Regular normal subgroups

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group with a regular normal subgroup N and point stabiliser $H = G_\alpha$. Then $G = HN$ is a semidirect product and the action of G on Ω is isomorphic to the action of G on N given by

$$a^{hn} = (h^{-1}ah)n$$

for all $a,n \in N$, $h \in H$. (If we write $G = NH$ instead, then the action is given by $a^{nh} = h^{-1}(an)h$.) Indeed, the map $\psi : N \to \Omega$ given by $n\psi = \alpha^n$ is a bijection, and for $x = hn \in G$ we have

$$(a^x)\psi = (h^{-1}ah)n\psi = \alpha^{h^{-1}ahn} = \alpha^{ahn} = (\alpha^a)^{hn} = (a\psi)^x$$

as required. With respect to this action of G on N, note that $H = G_1$ (where 1 is the identity element in N). Also note that $C_H(N) = 1$ since the action of G on Ω (and thus the action of G on N) is faithful.

Conversely, suppose H and N are groups, and H acts on N by automorphisms, i.e. there is a homomorphism $\varphi : H \to \mathrm{Aut}(N)$. Let $G = H \ltimes_\varphi N$ be the corresponding semidirect product and consider the action of G on N defined by

$$a^{hn} = a^{h\varphi}n$$

where $a^{h\varphi}$ denotes the image of $a \in N$ under the automorphism $h\varphi \in \mathrm{Aut}(N)$. Note that this really is an action:

$$a^{h_1n_1 \cdot h_2n_2} = a^{h_1h_2 \cdot n_1^{h_2\varphi}n_2} = a^{(h_1h_2)\varphi}n_1^{h_2\varphi}n_2$$

and

$$(a^{h_1n_1})^{h_2n_2} = (a^{h_1\varphi}n_1)^{h_2n_2} = (a^{h_1\varphi}n_1)^{h_2\varphi}n_2 = a^{(h_1h_2)\varphi}n_1^{h_2\varphi}n_2.$$

This action of G on N is faithful, $H = G_1$ and N is a regular normal subgroup.

Example 2.6. As an important special case of this construction, let V be a finite dimensional vector space over $\mathbb{F}_q$, and let H be a subgroup of $\mathrm{GL}(V)$. Then the corresponding semidirect product $G = HV$ acts faithfully on V by affine transformations

$$u^{hv} = uh + v$$

for all $u,v \in V$ and $h \in H$. Moreover, V is a regular normal subgroup and $H = G_0$ is the stabiliser of the zero vector. We say that G is an *affine* permutation group.

3 Primitivity

3.1 Introduction

Let G be a permutation group on a set Ω, with orbits Ω_i, $i \in I$. Then G induces a transitive permutation group G^{Ω_i} on Ω_i; these are called the *transitive constituents* of G. In some sense, G is built from its transitive constituents; indeed, G is a subdirect product of the G^{Ω_i} (that is, the corresponding projection maps $G \to G^{\Omega_i}$ are surjective). For example, if $G = \{1, (1,2)(3,4)\}$ and $\Omega = \{1,2,3,4\}$ then the orbits are $\Omega_1 = \{1,2\}$, $\Omega_2 = \{3,4\}$, and G is a proper subdirect product of the transitive constituents $G^{\Omega_1} = \{1, (1,2)\}$, $G^{\Omega_2} = \{1, (3,4)\}$.

In turn, the transitive constituents themselves may be built (in some sense) from smaller permutation groups. Here we need the notion of *primitivity*, which is a natural "irreducibility" condition that leads us to the basic building blocks of all permutation groups; the *primitive groups*. Moreover, we will see that the abstract structure of a primitive group is rather restricted (note that transitivity alone imposes no restrictions whatsoever on the abstract structure of G).

Definition 3.1. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group. A nonempty subset Γ of Ω is a *block* if, for all $x \in G$, either $\Gamma^x = \Gamma$ or $\Gamma \cap \Gamma^x = \emptyset$. Each translate Γ^x is also a block, and we say that $\{\Gamma^x \mid x \in G\}$ is a *block system* (this is a partition of Ω). The block systems $\{\Omega\}$ and $\{\{\alpha\} \mid \alpha \in \Omega\}$ are *trivial*, and any other block system is *nontrivial*.

Note that all blocks in a block system have the same cardinality. In particular, if the degree of G is a prime number, then the only block systems are trivial. Two closely related notions:

- A partition $\Omega = \Gamma_1 \cup \cdots \cup \Gamma_k$ is *G-invariant* if, for all i and all $x \in G$, $(\Gamma_i)^x \in \{\Gamma_1, \ldots, \Gamma_k\}$. The *trivial* partitions are Ω and $\bigcup_{\alpha \in \Omega} \alpha$.
- A *G-congruence* on Ω is a G-invariant equivalence relation, i.e. $\alpha \sim \beta$ if and only if $\alpha^x \sim \beta^x$ for all $x \in G$. The universal relation and equality are the *trivial* congruences.

It is easy to see that

$$\begin{aligned} G \text{ has a nontrivial block system} &\iff \Omega \text{ admits a nontrivial } G\text{-invariant partition} \\ &\iff \Omega \text{ admits a nontrivial } G\text{-congruence} \end{aligned}$$

Definition 3.2. A transitive group $G \leqslant \mathrm{Sym}(\Omega)$ is *imprimitive* if it has a nontrivial block system, otherwise G is *primitive*.

Equivalent definitions can be given in terms of G-invariant partitions and G-congruences, and it turns out that there are several other equivalent definitions for primitivity (see Lemma 3.4, for example).

Examples 3.3.

(i) The standard actions of S_n ($n \geqslant 2$) and A_n ($n \geqslant 3$) are primitive.

(ii) Consider the standard action of $G = D_{12}$ on the set of vertices $\Omega = \{1,2,3,4,5,6\}$ of a hexagon (numbered consecutively). Then G has two nontrivial block systems:

$$\{\{1,4\},\{2,5\},\{3,6\}\}, \quad \{\{1,3,5\},\{2,4,6\}\}.$$

In fact, it is easy to see that the standard action of D_{2n} is imprimitive if n is composite.

(iii) The symmetry group of a cube acts imprimitively on the set of vertices of the cube; the four pairs of diagonally opposite vertices form a block system.

(iv) Any transitive group of prime degree is primitive, e.g. $\langle (1,2,3,4,5) \rangle \cong Z_5$ is a primitive subgroup of S_5.

(v) The action of S_m on the set of k-element subsets of $\{1, \ldots, m\}$ is primitive for all $1 < k < m$, $k \neq m/2$ (if $k = m/2$ then $\{\{1, \ldots, m/2\}, \{m/2+1, \ldots, m\}\}$ is a block).

(vi) Wreath products are an important source of examples. As in Section 2.2, let $H \leqslant \mathrm{Sym}(\Gamma)$ and $K \leqslant \mathrm{Sym}(\Delta)$ be transitive permutation groups, where $|\Gamma|, |\Delta| \geqslant 2$ and $\Delta = \{1, \ldots, n\}$, and set $G = H \wr K$. The *standard action* of G on $\Omega = \Gamma \times \Delta$ (see (2.1)) is imprimitive since

$$\{\Gamma \times \{i\} \mid 1 \leqslant i \leqslant n\}$$

is a block system. However, one can show that the *product action* of G on $\Omega = \Gamma^n$ (see (2.2)) is primitive if and only if H is primitive and non-regular on Γ (see [38, Lemma 2.7A]). For example, both conditions are necessary:

- If $\Sigma \subset \Gamma$ is a nontrivial block for H, then $\Sigma^n \subset \Omega$ is a nontrivial block for G.
- If H is regular then $\{(\gamma, \ldots, \gamma) \mid \gamma \in \Gamma\} \subset \Omega$ is a block for G.

Note that if $G \leqslant \mathrm{Sym}(\Omega)$ is imprimitive and $\{\Gamma_1, \ldots, \Gamma_k\}$ is a nontrivial block system, then G is isomorphic to a subgroup of $\mathrm{Sym}(\Gamma_1) \wr S_k$.

Suppose $G \leqslant \mathrm{Sym}(\Omega)$ is imprimitive. A nontrivial block system $\Delta = \{\Gamma^x \mid x \in G\}$ is *maximal* if the induced group $G^\Delta \leqslant \mathrm{Sym}(\Delta)$ is primitive. For example, the two block systems in Examples 3.3(ii) are maximal. For a non-example, if we take a natural copy of $G = D_{12} \wr S_4$ in S_{24} then $\Delta = \{\{1,4\}^x \mid x \in G\}$ is a non-maximal block system (here $G^\Delta = S_3 \wr S_4 < S_{12}$ is imprimitive).

Let $\Delta_1 = \{\Gamma^x \mid x \in G\}$ be a maximal block system and set $H = (G_\Gamma)^\Gamma$ (the group induced on Γ by the setwise stabiliser G_Γ of Γ in G) and $K_1 = G^{\Delta_1}$. Note that $H \leqslant \mathrm{Sym}(\Gamma)$ is transitive and $K_1 \leqslant \mathrm{Sym}(\Delta_1)$ is primitive. There is a bijection between Ω and $\Gamma \times \Delta_1$ that embeds G into $H \wr K_1$ (see [38, Theorem 2.6A]). If H is imprimitive then we can repeat the process, taking a maximal block system $\Delta_2 = \{(\Gamma_1)^x \mid x \in H\}$ with respect to the action of H on Γ. Then H is isomorphic to a subgroup of $L \wr K_2$, where $L = (H_{\Gamma_1})^{\Gamma_1} \leqslant \mathrm{Sym}(\Gamma_1)$ is transitive and $K_2 = H^{\Delta_2} \leqslant \mathrm{Sym}(\Delta_2)$ is primitive, so we can embed G in $(L \wr K_2) \wr K_1$. If Ω is finite then this process eventually terminates, at which point G is isomorphic to a subgroup of an iterated wreath product

$$((\ldots(K_r \wr K_{r-1}) \wr \ldots) \wr K_2) \wr K_1 \leqslant \mathrm{Sym}(((\ldots(\Delta_r \times \Delta_{r-1}) \times \ldots) \times \Delta_2) \times \Delta_1)$$

of primitive groups $K_i \leqslant \mathrm{Sym}(\Delta_i)$, $1 \leqslant i \leqslant r$. Here the K_i are the corresponding *primitive components* of G (unlike transitive constituents, these are *not* uniquely determined by G).

3.2 Basic properties

Lemma 3.4. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group. Then G is primitive if and only if G_α is a maximal subgroup of G.*

Proof. This is Exercise 12. □

Lemma 3.5. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive permutation group and let N be a nontrivial normal subgroup of G. Then N is transitive.*

Proof. The N-orbits on Ω form a block system for G, since

$$(\alpha^N)^x = \alpha^{Nx} = \alpha^{xN} = (\alpha^x)^N$$

for all $\alpha \in \Omega$ and $x \in G$. □

Lemma 3.6. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a 2-transitive permutation group. Then G is primitive.*

Proof. Suppose G is imprimitive, with a nontrivial block system $\{\Gamma_1, \Gamma_2, \ldots\}$. Choose distinct points $\alpha, \beta \in \Gamma_1$ and $\gamma \in \Gamma_2$. By 2-transitivity, there exists an element $x \in G$ such that $(\alpha, \beta)^x = (\alpha, \gamma)$. But this implies that $\emptyset \neq \Gamma_1 \cap \Gamma_1^x \neq \Gamma_1$, a contradiction. □

Note that the converse to Lemma 3.6 is false. For example, take the above example $Z_5 < S_5$, which is primitive but not 2-transitive (it is easy to construct other examples; for instance, Remark 3.11 describes when a primitive *affine* group is 2-transitive). Therefore,

$$\text{2-transitive} \implies \text{primitive} \implies \text{transitive}$$

but none of the reverse implications hold. In Section 3.5 we will consider several variations on primitivity (2-transitivity is one of many).

Let G be a finite group. Recall that the *socle* of G, denoted $\mathrm{Soc}(G)$, is the subgroup of G generated by its minimal normal subgroups (see Section 2.4). It turns out that the socle of a finite primitive permutation group is rather restricted.

Lemma 3.7. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group and let N be a nontrivial normal subgroup of G. If $C_G(N)$ is nontrivial, then $C_G(N)$ is regular.*

Proof. By Lemma 3.5, both N and $C_G(N)$ are transitive (note that $C_G(N)$ is a normal subgroup of G). Suppose $x \in C_G(N)_\alpha$, so $\alpha \in C_\Omega(x)$. Then N preserves $C_\Omega(x)$ (if $\alpha \in C_\Omega(x)$ and $n \in N$, then $(\alpha^n)^x = (\alpha^x)^n = \alpha^n$), so the transitivity of N implies that $C_\Omega(x) = \Omega$ and thus $x = 1$. Therefore $C_G(N)_\alpha = 1$ and $C_G(N)$ is regular. □

Theorem 3.8. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group. Then one of the following holds:*

(i) *G has a unique minimal normal subgroup N, where N is regular and elementary abelian.*

(ii) *G has a unique minimal normal subgroup N, and $C_G(N) = 1$.*

(iii) *G has exactly two minimal normal subgroups N and $C_G(N)$, which are isomorphic, nonabelian and regular.*

Proof. First we claim that G has at most two minimal normal subgroups. If N_1 and N_2 are distinct minimal normal subgroups of G, then Lemmas 2.5 and 3.7 imply that N_1 is transitive, $N_1 \leqslant C_G(N_2)$ and $C_G(N_2)$ is regular. Therefore, N_1 is also regular, so $|N_1| = |C_G(N_2)|$ and thus $N_1 = C_G(N_2)$. Similarly, $N_2 = C_G(N_1)$. This justifies the claim.

Let N_1 and N_2 be minimal normal subgroups of G. If $C_G(N_1) = 1$ then (ii) holds (by Lemma 2.5(i), if $N_1 \neq N_2$ then $N_2 \leqslant C_G(N_1)$, a contradiction). Now assume $C_G(N_1) \neq 1$.

Suppose $N_1 \neq N_2$. Then $N_1 = C_G(N_2)$ and $N_2 = C_G(N_1)$ as above, so N_1 and N_2 are regular and nonabelian. Fix $\alpha \in \Omega$ and set $L = (N_1N_2)_\alpha$. Then $L \cap N_1 = L \cap N_2 = 1$ since N_1 and N_2 are regular, so $LN_1 = LN_2 = N_1N_2$ and thus

$$L \cong L/(L \cap N_1) \cong LN_1/N_1 = N_1N_2/N_1 \cong N_2.$$

Similarly, $L \cong N_1$. Therefore (iii) holds.

Finally, suppose $C_G(N_1) \neq 1$ and N_1 is the unique minimal normal subgroup of G. Then $C_G(N_1)$ is a regular normal subgroup of G (by Lemma 3.7) and thus $C_G(N_1)$ is a minimal normal subgroup (if $C_G(N_1)$ contains a nontrivial subgroup K normal in G, then K is also regular, so $K = C_G(N_1)$). Therefore, $N_1 = C_G(N_1)$ so N_1 is regular and abelian. By Lemma 2.5(ii), it follows that N_1 is elementary abelian. □

Corollary 3.9. *If G is a finite primitive group, then $\mathrm{Soc}(G) \cong T^k$ for some simple group T.*

3.3 The O'Nan-Scott Theorem

We now turn to one of the most important theorems in permutation group theory. The *O'Nan-Scott Theorem* is a very powerful tool for studying finite primitive permutation groups, describing their structure and action in terms of the socle of the group. In many situations, this theorem can be used to reduce a general problem to a much more specific problem concerning almost simple groups, at which point one can appeal to CFSG and the vast literature on simple groups and their subgroups, conjugacy classes and representations. We will see several examples of this sort of reduction.

The theorem was stated independently by O'Nan and Scott in the preliminary proceedings of the Santa Cruz Conference on Finite Groups in 1979, though only Scott's version made it into the final Proceedings [81]. Shortly afterwards, an error in the statement was corrected by Aschbacher. In [66], Liebeck, Praeger and Saxl give a self-contained proof, and Fawcett's thesis [39] provides a very detailed and readable account of the proof. In order to state the theorem, we need to introduce five families of primitive permutation groups (see Table 3.1).

	Description
I	Almost simple
II	Affine-type
III	Diagonal-type
IV	Product-type
V	Twisted wreath products

Table 3.1: The five families of primitive groups

I. Almost simple. Recall that a permutation group $G \leqslant \mathrm{Sym}(\Omega)$ is *almost simple* if $\mathrm{Soc}(G) = T$ is a nonabelian simple group, in which case

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

Also recall that if G is transitive with point stabiliser H, then the action of G on Ω is isomorphic to the natural action of G on the set of cosets G/H. Moreover, G is primitive if and only if H is a maximal subgroup of G (by Lemma 3.4). Note that H is core-free, so it does not contain T. We also note the fact that T is non-regular. (The latter fact is not obvious – the proof requires the Schreier Conjecture; see [39, Proposition 2.4.2] for the details.)

II. Affine-type. Let p be a prime and let $V = (\mathbb{F}_p)^d$ be a d-dimensional vector space over $\mathbb{F}_p$ (which we will view as an additive group). Let $\mathrm{AGL}(V) = \mathrm{AGL}_d(p)$ be the group of *affine transformations* of V, which are of the form

$$u \mapsto ux + v$$

for $u, v \in V$ and $x \in \mathrm{GL}(V)$. This action is faithful, so $\mathrm{AGL}(V)$ is a permutation group on V. If we identify $\mathrm{GL}(V)$ with the stabiliser of the zero vector, and V with the subgroup of translations, then V is a regular normal subgroup and $\mathrm{AGL}(V) = \mathrm{GL}(V) \ltimes V$.

A permutation group $G \leqslant \mathrm{Sym}(V)$ is of *affine-type* if

$$V \leqslant G \leqslant \mathrm{AGL}(V).$$

Here V is a regular normal subgroup of G (so G is transitive), $G_0 \leqslant \mathrm{GL}(V)$ is linear (the stabiliser of the zero vector in G) and $G = G_0 \ltimes V$.

Proposition 3.10. *Let $G \leqslant \mathrm{Sym}(V)$ be an affine-type group.*

(i) *G is primitive if and only if $G_0 \leqslant \mathrm{GL}(V)$ is irreducible.*

(ii) *If G is primitive, then V is the unique minimal normal subgroup of G. In particular, $\mathrm{Soc}(G) = V$ is elementary abelian.*

Proof.

(i) Suppose G is imprimitive. Fix a nontrivial block system and let $U \subset V$ be the block containing the zero vector. If $v \in U$ then $v \in U \cap (U + v) = U \cap U^v$, so $U = U + v$ and thus U is a proper nonzero subspace of V (since the underlying field is $\mathbb{F}_p$, we just need to check closure under addition). Since G_0 fixes the zero vector, it follows that U is G_0-invariant and thus G_0 is reducible.

Conversely, suppose U is a proper nonzero G_0-invariant subspace of V. Let $g = xv \in G$, where $x \in G_0$ and $v \in V$. Then

$$U^g = Ux + v = U + v$$

and thus U^g is a coset of U in V. Therefore, either $U^g = U$ or $U^g \cap U = \emptyset$, so U is a nontrivial block and thus G is imprimitive.

(ii) Suppose G is primitive. By Lemma 3.7, $C_G(V)$ is regular and thus $C_G(V) = V$ (we have $V \leqslant C_G(V)$ since V is abelian). Let N be a minimal normal subgroup of G. If $N \cap V = 1$ then $[N,V] = 1$ and thus $N \leqslant C_G(V) = V$, which is a contradiction. Therefore, $N \cap V \neq 1$, so $N \cap V = N$ by the minimality of N, whence $N \leqslant V$. Now N is transitive and the regularity of V implies that N is also regular, so $|N| = |V|$ and thus $N = V$. □

Remark 3.11. Recall that a transitive group $G \leqslant \mathrm{Sym}(\Omega)$ is 2-*transitive* if and only if G_α acts transitively on $\Omega \setminus \{\alpha\}$. In particular, an affine group $G \leqslant \mathrm{AGL}(V)$ is 2-transitive if and only if $G_0 \leqslant \mathrm{GL}(V)$ acts transitively on the set of non-zero vectors of V (of course, this condition implies that G_0 is irreducible, but it is much stronger). There is a complete classification of the linear groups with this transitivity property; this is a theorem of Hering [56] (also see [65, Appendix 1]).

III. Diagonal-type. Let $k \geqslant 2$ be an integer, let T be a nonabelian finite simple group and consider the natural action of $G = T^k$ on the cosets of the diagonal subgroup $H = \{(t,\ldots,t) \mid t \in T\}$. Clearly, this action is faithful and transitive. Moreover, if $k = 2$ then H is a maximal subgroup of G (see Exercise 11), so in this case G is a primitive *diagonal-type* group. We can build larger diagonal-type groups by including additional automorphisms of T^k (recall that $\mathrm{Aut}(T^k) = \mathrm{Aut}(T) \wr S_k$, see Proposition 2.4(ii)).

The formal set-up is as follows. For $a \in \mathrm{Aut}(T)$, let $\overline{a}$ denote the coset $\mathrm{Inn}(T)a \in \mathrm{Out}(T)$. Define

$$\begin{aligned} W &= \{(a_1,\ldots,a_k)\pi \in \mathrm{Aut}(T) \wr S_k \mid \overline{a}_1 = \overline{a}_i \text{ for all } i\} \leqslant \mathrm{Aut}(T) \wr S_k \\ D &= \{(a,\ldots,a)\pi \in \mathrm{Aut}(T) \wr S_k\} \cong \mathrm{Aut}(T) \times S_k \\ \Omega &= W/D \\ A &= W \cap \mathrm{Aut}(T)^k \\ M &= \mathrm{Inn}(T)^k \cong T^k \end{aligned} \tag{3.1}$$

Note that $W = A \rtimes S_k \cong T^k.(\mathrm{Out}(T) \times S_k)$ (a possibly nonsplit extension) and $|\Omega| = |T|^{k-1}$. We can consider the natural transitive action of W on Ω:

$$(D(a_1,\ldots,a_k)\pi)^{(b_1,\ldots,b_k)\sigma} = D(a_1,\ldots,a_k)\pi \cdot (b_1,\ldots,b_k)\sigma = D(a_1 b_{1\pi},\ldots,a_k b_{k\pi})\pi\sigma \tag{3.2}$$

Lemma 3.12. *In terms of the above notation, the following hold:*

(i) *M is the unique minimal normal subgroup of W, so $\mathrm{Soc}(W) = M \cong T^k$.*

(ii) *The natural action of W on Ω is faithful.*

Sketch proof.

(i) Write $M = T_1 \times \cdots \times T_k$, where

$$T_i = \{(1,\ldots,1,a_i,1,\ldots,1) \mid a_i \in \mathrm{Inn}(T)\} < W.$$

If $g = (a_1,\ldots,a_k)\pi \in W$ then $T_i^g = T_{i\pi}$, so W acts transitively on $\{T_1,\ldots,T_k\}$ by conjugation. Let L be a proper nontrivial normal subgroup of W that is contained in M. Then $L = \prod_{i\in I} T_i$ for some nonempty subset I of $\{1,\ldots,k\}$, and thus the transitivity of W implies that $L = M$. Finally, to see that M is unique, suppose $g = (a_1,\ldots,a_k)\pi \in C_W(M)$. Then $g \in \bigcap_i C_W(T_i)$, so $T_{i\pi} = T_i^g = T_i$ for all i and thus $\pi = 1$. Therefore, $a^{a_i} = a$ for all $a \in \mathrm{Inn}(T)$, so $a_i \in C_{\mathrm{Aut}(T)}(\mathrm{Inn}(T)) = 1$ (see Proposition 2.4(i)) for all i. Hence $g = 1$, $C_W(M) = 1$ and thus M is unique (by Lemma 2.5(i)).

(ii) Let $\alpha = D \in \Omega$, so $W_\alpha = D$. We will show that W_α is core-free. Since $M \lhd W$ we have $MW_\alpha \leqslant W$. If $g = (a_1,\ldots,a_k)\pi \in W$ then $a_i a_1^{-1} \in \mathrm{Inn}(T)$ for all i, so

$$g = (a_1 a_1^{-1},\ldots,a_k a_1^{-1}) \cdot (a_1,\ldots,a_k)\pi \in MW_\alpha$$

and thus $W = MW_\alpha$. Therefore, M is transitive on Ω. Suppose U is a nontrivial normal subgroup of W contained in W_α. By (i), $M \leqslant U$ so $M \leqslant W_\alpha$ and thus $M = M_\alpha$, which contradicts the transitivity of M. Therefore W_α is core-free, whence the action of W on Ω is faithful. □

A permutation group $G \leqslant \mathrm{Sym}(\Omega)$ is of *diagonal-type* if $M \leqslant G \leqslant W$, i.e.

$$T^k \leqslant G \leqslant T^k.(\mathrm{Out}(T) \times S_k).$$

Note that G is transitive since it contains the transitive subgroup M. Let

$$P_G = \{\pi \in S_k \mid (a_1, \ldots, a_k)\pi \in G \text{ for some } (a_1, \ldots, a_k) \in A\} \leqslant S_k.$$

Note that P_G is the subgroup of S_k induced via the conjugation action of G on the k factors of $\mathrm{Soc}(G) = M = \mathrm{Inn}(T)^k$; we call it the *top group* of G. Many properties of G are controlled by P_G, including primitivity.

Proposition 3.13. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a diagonal-type group, so $M \leqslant G \leqslant W$. Let $P_G \leqslant S_k$ be the corresponding top group. Then G is primitive if and only if P_G is primitive, or $k = 2$ and $P_G = 1$.*

Proof. See [38, Theorem 4.5A]. □

For example, there are precisely 5 diagonal-type primitive groups of degree 60, corresponding to the 5 subgroups of $\mathrm{Out}(A_5) \times S_2 \cong Z_2 \times Z_2$, e.g. $A_5 \times A_5$ and $A_5 \wr S_2$.

IV. Product-type. These groups arise as "blow-ups" of almost simple or diagonal-type primitive groups. Let $H \leqslant \mathrm{Sym}(\Gamma)$ be a primitive group of type I (almost simple) or III (diagonal). Let $k \geqslant 2$ be an integer and consider the wreath product $W = H \wr S_k$. Recall from Section 2.2 that W has a natural *product action* on the Cartesian product $\Omega = \Gamma^k$, given by

$$(\gamma_1, \ldots, \gamma_k)^{(h_1,\ldots,h_k)p^{-1}} = (\gamma_{1^p}^{h_{1^p}}, \ldots, \gamma_{k^p}^{h_{k^p}}).$$

Let $T = \mathrm{Soc}(H)$ and $B = \mathrm{Soc}(W)$, so $B = T^k$. Note that W acts faithfully on Ω.

A permutation group $G \leqslant \mathrm{Sym}(\Omega)$ is of *product-type* if $B \leqslant G \leqslant W$. Let

$$P_G = \{\pi \in S_k \mid (h_1, \ldots, h_k)\pi \in G \text{ for some } (h_1, \ldots, h_k) \in H^k\} \leqslant S_k$$

be the corresponding *top group* of G (as before, P_G is the group of permutations induced via the conjugation action of G on the k factors of $\mathrm{Soc}(G) = T^k$). Note that $\mathrm{Soc}(G) = T^k \leqslant G \leqslant H \wr P_G$. The condition for primitivity is as follows:

Proposition 3.14. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a product-type group, so $B \leqslant G \leqslant W$. Let P_G be the corresponding top group. Then G is primitive if and only if P_G is transitive.*

Proof. Since H is non-regular, this follows immediately from [38, Lemma 2.7A]. □

V. Twisted wreath products. These groups are a bit more difficult to describe (see [38, pp.133–137] for more details). The basic ingredients are as follows. Let $k \geqslant 2$ be an integer and let $P \leqslant S_k$ be a transitive subgroup with point stabiliser Q. Let T be a nonabelian simple group and suppose $\varphi : Q \to \mathrm{Aut}(T)$ is a homomorphism with $\mathrm{Inn}(T) \leqslant \mathrm{im}(\varphi)$. Define

$$B = \{f : P \to T \mid f(pq) = f(p)^{\varphi(q)} \text{ for all } p \in P, q \in Q\}.$$

Then B is a group under pointwise multiplication, and $B \cong T^k$. Now P acts on B via $f^p(x) = f(px)$ $(p, x \in P)$ and we define $G = B \rtimes P$ to be the corresponding semidirect product; this is the *twisted wreath product* $T \wr_\varphi P$ (the original construction is due to B.H. Neumann). Here B is the unique minimal normal subgroup of G.

Let $\Omega = G/P$ and $\alpha = P \in \Omega$. Then G acts transitively on Ω and $G_\alpha = P$ is core-free (since B is the unique minimal normal subgroup of G, and $B \cap P = 1$), so G acts faithfully on Ω. Note that $|\Omega| = |B| = |T|^k$ and $\mathrm{Soc}(G) = B$ is regular. The primitivity of G depends on some quite complicated conditions on P. In terms of degree, the smallest primitive group of this type arises when $T = A_5$ and $k = 6$, in which case $|\Omega| = 60^6$.

These groups were erroneously excluded in the original version of the O'Nan-Scott Theorem; their existence was pointed out later by Aschbacher.

We are now ready to state the O'Nan-Scott Theorem.

Theorem 3.15 (O'Nan & Scott, 1979)**.** *Any finite primitive permutation group is permutation isomorphic to one of the types* I, II, III, IV *or* V *described above.*

Some comments on the proof. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group, with socle M and point stabiliser $H = G_\alpha$. Let $n = |\Omega|$.

Case 1. M is abelian.

By Theorem 3.8, M is an elementary abelian p-group for some prime p, say $|M| = p^d$, and M is regular. As noted in Section 2.5, $G = HM$ is a semidirect product, and the action of G on Ω is isomorphic to the action of G on M given by $a^{hm} = (h^{-1}ah)m$. Let $V = (\mathbb{F}_p)^d$ (viewed as an additive group), let $\theta : M \to V$ be an isomorphism, and define a map

$$\begin{array}{rcl} \psi : G & \to & \mathrm{GL}(V) \ltimes V = \mathrm{AGL}(V) \\ hm & \mapsto & (\theta^{-1}\phi_h\theta)m\theta \end{array}$$

Here $\phi_h : M \to M$ is the map $a\phi_h = h^{-1}ah$, and it is easy to check that $\theta^{-1}\phi_h\theta \in \mathrm{GL}(V)$. Moreover, ψ is a monomorphism and $V \leqslant G\psi \leqslant \mathrm{AGL}(V)$. Finally, one checks (using Exercise 9, for example) that the action of G on M is permutation isomorphic to the action of $G\psi$ on V, so G is an *affine-type* group.

Case 2. M is nonabelian.

By Corollary 3.9, $M = T_1 \times \cdots \times T_k \cong T^k$ for some integer $k \geqslant 2$ and nonabelian simple group T. If $k = 1$ then G is *almost simple*, so let us assume $k \geqslant 2$. Let $\mathscr{T} = \{T_1, \ldots, T_k\}$ and note that G acts on $\mathscr{T}$ by conjugation, inducing a permutation group $P \leqslant S_k$. Let $\pi_i : M \to T_i$ be the i-th projection map, $1 \leqslant i \leqslant k$. There are now two subcases to consider.

Case 2.1. $\pi_i(M_\alpha) = T_i$ for some i.

First one uses the primitivity of G to show that $\pi_j(M_\alpha) = T_j$ for all j, so M_α is a subdirect product of M. More precisely,

$$M_\alpha = D_1 \times \cdots \times D_\ell \cong T^\ell,$$

where $D_i \cong T$ is a diagonal subgroup of $\prod_{j \in I_i} T_j$, and $I_1 \cup \cdots \cup I_\ell$ is a partition of $\{1, \ldots, k\}$. Set $m = |I_1|$. Now G_α acts transitively on $\{D_1, \ldots, D_\ell\}$, so $k = \ell m$. If $\ell = 1$ then one shows that there is no nontrivial P-invariant partition of $\mathscr{T}$ and thus either $k \geqslant 3$ and P is primitive, or $k = 2$. With further work, one goes on to show that G is of *diagonal-type*. On the other hand, if $\ell > 1$ then one can show that G is a *product-type* group (the blow-up of a diagonal-type group).

Case 2.2. $\pi_i(M_\alpha) < T_i$ for all i.

Let $N = N_G(T_1)$. For any subgroup $L \leqslant N$, let L^* be the group of automorphisms of T_1 induced by L by conjugation. There are two possibilities to consider, which lead to the final two types of primitive groups in the O'Nan-Scott Theorem.

Suppose $T_1^* \leqslant (N_\alpha)^*$. We define a homomorphism

$$\begin{array}{rcl} \varphi : N_\alpha & \to & \mathrm{Aut}(T_1) \\ n & \mapsto & (t \mapsto n^{-1}tn) \end{array}$$

Then $M_\alpha = 1$ and $\mathrm{im}(\varphi) = (N_\alpha)^* \geqslant T_1^* = \mathrm{Inn}(T_1)$, and with some work one shows that G is a *twisted wreath product*. This part of the argument requires the Schreier Conjecture (see Theorem 2.3), which in turn relies on CFSG.

Finally, if $T_1^* \not\leqslant (N_\alpha)^*$ then one can show that G is a *product-type* group (the blow-up of an almost simple group). Again, this argument requires the Schreier Conjecture. □

Remark 3.16. A few additional comments on the O'Nan-Scott Theorem:

(i) The five families I – V are pairwise disjoint;

(ii) Every soluble primitive group is affine;

	Upper bound on $\lvert G\rvert$	Comments
Bochert, 1889	$n(n-1)\cdots(n-\lfloor n/2\rfloor+1)\leqslant n^{n/2}$	See [10] and Theorem 5.6
Wielandt, 1969	c^n	G not 2-transitive; c constant
Praeger & Saxl, 1980	4^n	See [79]
Babai, 1981	$\exp(4\sqrt{n}\log^2 n)$	See [3, 4]
		$n\gg 0$ if G is 2-transitive

Table 3.2: Upper bounds on the orders of primitive groups, pre-CFSG

(iii) In the product-type construction (type IV above), we assume that $H\leqslant \mathrm{Sym}(\Gamma)$ is either almost simple or diagonal-type. Of course, we could apply the same construction to any primitive group, but we do not get anything new. For example, the "blow-up" of an affine group has a regular abelian socle, so it is also an affine-type group.

3.4 Applications

Let us now consider some far-reaching applications of the O'Nan-Scott Theorem. One of our main aims is to show that primitive groups are both *rare* and *small*.

3.4.1 The order of a primitive group

Estimating the order of a finite primitive permutation group in terms of its degree was one of the central problems of 19th century group theory. This problem is closely related to the 1860 Grand Prix problem of the Paris Academy (the prize was not awarded, although Jordan was one of the contestants).

Let G be a primitive permutation group of degree n, and let us assume $G\neq A_n, S_n$. Roughly speaking, the aim is to show that G is "small" in some sense. In Table 3.4.1 we record some of the earlier CSFG-free results in this direction. The proof of Bochert's bound relies on bounding the *base size* of G (we will discuss bases in Section 5); indeed, the bound in Table 3.4.1 follows immediately from Theorem 5.6. Similarly, Babai used novel combinatorial arguments to bound the base size; a detailed account of his proof is given in [38, Section 5.3].

Armed with the O'Nan-Scott Theorem, together with CFSG, it is possible to establish essentially optimal bounds. The following result is best possible (see Theorem 5.8 and [64]):

Theorem 3.17 (Liebeck, 1984)**.** *Let G be a primitive permutation group of degree n, with $G\neq A_n, S_n$. Then there exists an absolute constant c such that $\lvert G\rvert < n^{c\sqrt{n}}$.*

Again, the proof is based on bounding the base size of G; a more detailed statement is given in Theorem 5.8, where we also give a sketch of the proof. To see that this bound is essentially optimal, consider the action of $G=S_m$ on the set of 2-element subsets of $\{1,\ldots,m\}$. Here $n=\binom{m}{2}$ and $n^{\sqrt{n}/2}<\lvert G\rvert<n^{\sqrt{n}}$ for all n. More recently, a sharper version of Liebeck's theorem has been obtained by Maróti [74] (in part (i), we allow $k=1$, in which case G is almost simple):

Theorem 3.18 (Maróti, 2002)**.** *Let G be a primitive permutation group of degree n. Then one of the following holds:*

(i) *$G\leqslant H\wr S_k$ is a product-type group, where $H\leqslant \mathrm{Sym}(\Gamma)$ is a primitive group with socle A_m, and Γ is the set of d-element subsets of $\{1,\ldots,m\}$.*

(ii) *$(G,n)=(\mathrm{M}_{11},11)$, $(\mathrm{M}_{12},12)$, $(\mathrm{M}_{23},23)$ or $(\mathrm{M}_{24},24)$;*

(iii) $\lvert G\rvert\leqslant\prod_{i=0}^{\lfloor\log n\rfloor-1}(n-2^i)<n^{1+\lfloor\log n\rfloor}$.

Note that the first bound in (iii) is equality if G is the affine group $\mathrm{AGL}_d(2)$ acting on 2^d points (which is 3-transitive, and thus primitive). As immediate corollaries, we deduce that $\lvert G\rvert<50n^{\sqrt{n}}$ and $\lvert G\rvert<3^n$ (in fact, $\lvert G\rvert<2^n$ if $n>24$; note that $\lvert \mathrm{M}_{24}\rvert>2^{24}$, so the condition $n>24$ is needed).

3.4.2 The degree of a primitive group

Now let us turn to the degree of a primitive group. We will consider two related problems:

1. *For which positive integers n is there a primitive group of degree n (other than A_n or S_n)?*
2. *Can we determine all the primitive groups of degree $n \leqslant N$ (up to permutation isomorphism), for some suitable integer N?*

In order to consider the first problem, let's introduce some notation:

$$E = \{n \in \mathbb{N} \mid \text{there exists a primitive group of degree } n, \text{ other than } S_n \text{ or } A_n\}$$
$$e(x) = |\{n \in E \mid n \leqslant x\}|$$

For trivial reasons, if $n \in E$ then $n \geqslant 5$. For larger values of n, one of the earliest results is a theorem of Mathieu from 1861, which states that $n \in E$ if $5 \leqslant n \leqslant 33$. More generally, it turns out that the only numbers $n \leqslant 100$ that are *not* in E are as follows:

$$1, 2, 3, 4, 34, 39, 46, 51, 58, 69, 70, 75, 76, 86, 87, 88, 92, 93, 94, 96, 96, 99$$

Of course, we already know the degrees of several primitive groups:

- $n = p$ is a prime: Z_p acting regularly;
- $n = p+1$, where p is a prime: natural action of $\mathrm{PGL}_2(p)$;
- $n = m^2$: $S_m \wr S_2$ in product action;
- $n = \frac{1}{2}m(m-1)$: S_m on 2-elements subsets of $\{1, \ldots, m\}$.

Let $\pi(x)$ be the number of prime numbers $p \leqslant x$. Just by considering the first two possibilities for n, we deduce that $e(x) \gtrsim 2\pi(x)$, and by including the square and triangular degrees we get

$$e(x) \geqslant 2\pi(x) + (1+\sqrt{2})x^{\frac{1}{2}} - O(\log(x)).$$

Here the $O(\log(x))$ term is needed because some square numbers are also triangular (there are $O(\log x)$ such numbers at most x).

The following theorem [34] implies that this simple estimate for $e(x)$ is rather good. Moreover, we deduce that primitive groups are *rare*:

Theorem 3.19 (Cameron, Neumann & Teague, 1982)**.** *We have*

$$e(x) = 2\pi(x) + (1+\sqrt{2})x^{\frac{1}{2}} + O(x^{\frac{1}{2}}/\log x) \sim 2x/\log x.$$

In particular, E has density 0 as a subset of $\mathbb{N}$, so for almost all integers n, the only primitive groups of degree n are S_n and A_n.

The most interesting (and most difficult) part of the proof is in estimating the possible degrees of almost simple primitive groups of Lie type (it is not too difficult to reduce to this situation, by applying the O'Nan-Scott Theorem). This is equivalent to estimating the possible indices of maximal subgroups in such groups, and the proof uses various results on subgroup structure. Of course, CFSG plays an important role in the analysis. More recently, an analogous result for *quasiprimitive* groups (see Section 3.5.4) has been established by Heath-Brown, Praeger and Shalev [55, Theorem 1.5].

Now let us turn to the second question above, which also has a long history. In 1872, Jordan [60] gave a slightly inaccurate description of all the primitive groups of degree $n \leqslant 17$, and by 1912 the list had been extended by various authors to $n \leqslant 20$. In the 1960s, Sims used computational methods to determine all the primitive groups up to degree 50, and this was essentially the best result pre-CFSG.

Not surprisingly, the powerful combination of CFSG and the O'Nan-Scott Theorem has had a major impact on this problem. In 1988, Dixon and Mortimer determined all the non-affine groups

of degree $n \leqslant 1000$, and this has since been extended in various ways. In 2005, Roney-Dougal completely classified all the primitive groups of degree $n < 2500$, and this has been pushed even further: the state-of-the-art is a complete classification for $n < 4096$, due to Coutts, Quick and Roney-Dougal [36] (the groups are presented in tables, organised according to the various O'Nan-Scott families). Moreover, these groups can be accessed via the Primitive Groups Database in both GAP and MAGMA. For example, the MAGMA command PrimitiveGroup(n,i) will return the i-th primitive group of degree n. A list of the primitive groups of degree $n \leqslant 1000$ is given in Appendix B of the textbook by Dixon and Mortimer [38]. According to MAGMA, there are 24558 primitive groups of degree $n < 4096$, and the number in each family is as follows:

Diagonal: 68, Product-type: 1132, Almost simple: 10686, Affine: 12672, Twisted wreath: 0

3.4.3 The elements of a primitive group

We have seen that there are restrictions on the abstract structure of primitive groups, as well as their order and degree, so it is not surprising to learn that there are also restrictions on the elements in such groups. The following is a classical theorem of Jordan [61] (see [38, Theorem 3.3E] for a textbook proof, and Exercises 17 and 18 for the cases $p = 2, 3$):

Theorem 3.20 (Jordan, 1873)**.** *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive permutation group of degree n, containing a cycle of prime length p fixing at least three points. Then $G = A_n$ or S_n.*

The condition on the number of fixed points is essential:

- $n = p$: $\langle (1, \ldots, p) \rangle < S_p$.
- $n = p + 1$: In the standard action of $\mathrm{PGL}_2(p)$, elements of order p have a unique fixed point.
- $n = p + 2$: Let $p = 2^m - 1$ be a Mersenne prime and set $q = 2^m$. In the standard action of $\mathrm{PGL}_2(q)$, elements of order p have precisely two fixed points.

In more recent years, this result has been extended in several different ways. For instance, a very recent theorem of Jones [58] (building on earlier work by many authors) provides a complete classification of the finite primitive permutation groups containing a cycle of *any* length (the proof relies on the classification of 2-transitive groups, so CFSG plays an important role). In particular, if G contains any cycle with at least three fixed points, then $G = A_n$ or S_n.

Of course, one can consider other restrictions on the cycle-structure of elements in a primitive group. For example, Müller [77] has recently determined the primitive groups containing an element with precisely two cycles, and this has been extended in [51] to elements with at most four cycles. The results in the latter paper are used to study *normal coverings* of symmetric groups (see Section 4.6) and there are interesting number-theoretic applications (see [51] and the references therein). Clearly, if $x \in G$ has at most four cycles then at least one of the cycles must have length at least $n/4$, where n denotes the degree of G, so $|x| \geqslant \lceil n/4 \rceil$. One of the key ingredients in the proof of the main theorem of [51] is a recent classification of the primitive groups that contain an element of order at least $n/4$; this uses the O'Nan-Scott Theorem and CFSG (see [50, Theorem 1.3]).

Jordan's theorem is also related to the classical notion of *minimal degree*. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive permutation group of degree n. The minimal degree of G, denoted by $\mu(G)$, is the smallest number of points moved by any non-identity element of G. For example, $\mu(S_n) = 2$ and $\mu(A_n) = 3$. An old problem in permutation group theory is to classify the primitive groups $G \neq S_n, A_n$ such that $\mu(G)$ is "small". By Theorem 3.20, $\mu(G) \geqslant 4$ for such a group G. In [4], Babai proves that $\mu(G) \geqslant \frac{1}{2}(\sqrt{n} - 1)$ (without using CFSG), which is essentially best possible (using CFSG, one can show that $\mu(G) \geqslant 2(\sqrt{n} - 1)$; see [68]). If one allows some exceptions, then these results can be pushed further. For example, the primitive groups G with $\mu(G) \geqslant n/3$ are classified in [68], and this has been extended by Guralnick and Magaard [49], who determine the groups with $\mu(G) \geqslant n/2$. Both of these results require CFSG.

3.5 Variations on primitivity

In this final section we briefly consider some variations on the notion of primitivity, both stronger and weaker, which have been investigated in recent years. This list is by no means exhaustive!

3.5.1 2-transitivity

Recall that 2-transitivity is stronger than primitivity (see Lemma 3.6). Determining the 2-transitive groups is an old problem:

Theorem 3.21 (Burnside, 1897)**.** *Any finite 2-transitive permutation group is either affine or almost simple.*

In other words, a 2-transitive group has a unique minimal normal subgroup, which is either elementary abelian and regular, or nonabelian and simple. As previously mentioned, the 2-transitive affine groups were classified by Huppert (in the soluble case) and Hering (insoluble groups). Using CFSG, the 2-transitive almost simple groups have also been classified (see [28, Section 5] and [38, Section 7.7], for example). It turns out that there are eight infinite families; these include the standard action of $\mathrm{PGL}_d(q)$, and natural actions of the Suzuki groups ${}^2B_2(q)$ and Ree groups ${}^2G_2(q)$ of degree q^2+1 and q^3+1, respectively. There are also some "sporadic" examples, such as a 2-transitive action of A_7 on 15 points (this arises from the fact that $A_7 < A_8 \cong \mathrm{PSL}_4(2)$), and a 2-transitive action of the Conway group Co_3 of degree 276. See [30, Tables 7.3 and 7.4] for tables that describe all the 2-transitive groups.

Remark 3.22. The finite permutation groups with higher degrees of transitivity have also been classified using CFSG (see [30, Sections 7.3 and 7.4]). Firstly, if G is a k-transitive group of degree n, and $G \neq A_n, S_n$, then $k \leqslant 5$. More precisely:

- There are three infinite families of 3-transitive groups, including the standard actions of $\mathrm{PGL}_2(q)$ and $\mathrm{AGL}_d(2)$ (with $d > 2$). There are also five sporadic examples that are 3-transitive but not 4-transitive:

$$(G,n) = (\mathrm{M}_{11},12),\ (\mathrm{M}_{12},12),\ (\mathrm{M}_{22},22),\ (\mathrm{M}_{22}.2,22),\ (A_7 \ltimes 2^4,16)$$

- If $k = 4$ and G is not 5-transitive, then $(G,n) = (\mathrm{M}_{11},11)$ or $(\mathrm{M}_{23},23)$.
- If $k = 5$ then $(G,n) = (\mathrm{M}_{12},12)$ or $(\mathrm{M}_{24},24)$.

It is not surprising that the Mathieu sporadic simple groups feature prominently here; Mathieu discovered these groups in the 1860s and 1870s in his search for highly transitive permutation groups.

3.5.2 $\frac{3}{2}$-transitivity

A transitive permutation group $G \leqslant \mathrm{Sym}(\Omega)$ is *$\frac{3}{2}$-transitive* if all the orbits of G_α on $\Omega \setminus \{\alpha\}$ have the same size, and this size is greater than 1 (i.e. G_α acts nontrivially on $\Omega \setminus \{\alpha\}$). This notion was introduced by Wielandt [86]; it is stronger than transitivity, but weaker than 2-transitivity, so the terminology is appropriate.

Examples 3.23.

(i) Any 2-transitive group (other than S_2 on 2 points) is $\frac{3}{2}$-transitive.

(ii) More generally, any non-regular normal subgroup of a 2-transitive group is $\frac{3}{2}$-transitive.

(iii) The action of $G = S_7$ (or A_7) on the set Ω of 2-element subsets of $\{1,\ldots,7\}$ is $\frac{3}{2}$-transitive. Here $|\Omega| = 21$ and G_α has two orbits, both of length 10 (see Exercise 19).

(iv) Every *Frobenius group* is $\frac{3}{2}$-transitive. Here a transitive permutation group $G \leqslant \mathrm{Sym}(\Omega)$ is Frobenius if it is non-regular and only the identity element has more than one fixed point. Equivalently, if $H = G_\alpha$ then $H \cap H^x = 1$ for all $x \in G \setminus H$. In particular, G_α acts semiregularly on $\Omega \setminus \{\alpha\}$, so G is $\frac{3}{2}$-transitive.

The following theorem of Wielandt [86, Theorem 10.4] is a first step towards a classification of these groups:

Theorem 3.24 (Wielandt, 1964)**.** *Any $\frac{3}{2}$-transitive group is either primitive or Frobenius.*

Later in the 1960s, Passman classified all soluble $\frac{3}{2}$-transitive groups. Much more recently, an analogue of Theorem 3.21 for $\frac{3}{2}$-transitive groups has been established (see [6, Theorem 1.1]):

Theorem 3.25 (Bamberg, Giudici, Liebeck, Praeger & Saxl, 2013)**.** *Any finite primitive $\frac{3}{2}$-transitive permutation group is either affine or almost simple. Moreover, all the almost simple groups with this property have been determined.*

It turns out that all the almost simple examples are 2-transitive, with the exception of one infinite family with socle $\mathrm{PSL}_2(q)$ (with q even and degree $\frac{1}{2}q(q-1)$), and the above example of A_7 (or S_7) acting on 21 points. The proof uses all the usual machinery: the O'Nan-Scott Theorem, combined with CFSG and detailed information on the structure of simple groups. It also uses an elementary (but very useful) observation: if $G \leqslant \mathrm{Sym}(\Omega)$ is transitive and r is a prime that divides $|\Omega|$ and a subdegree of G, then G is not $\frac{3}{2}$-transitive. Some recent work on *bases* for permutation groups is another important ingredient in the proof (we will discuss bases in Section 5).

Even more recently, the $\frac{3}{2}$-transitive affine groups of the form $HV \leqslant \mathrm{AGL}(V)$, where $V = (\mathbb{F}_p)^d$ and p divides $|H|$, have been determined (see [48]).

3.5.3 Extreme primitivity

A non-regular primitive permutation group $G \leqslant \mathrm{Sym}(\Omega)$ is *extremely primitive* if G_α acts primitively on each of its nontrivial orbits. Of course, this notion is stronger than primitivity.

Examples 3.26.

(i) Every 2-*primitive* group is extremely primitive (such a group G is primitive, and G_α acts primitively on $\Omega \setminus \{\alpha\}$). For example, every 3-transitive group is 2-primitive, so the standard actions of $\mathrm{PGL}_2(q)$ and $\mathrm{AGL}_d(2)$ (with $d \geqslant 3$) are 2-primitive.

(ii) Two sporadic examples:

$$\begin{array}{llll} G = \mathrm{J}_2, & G_\alpha = \mathrm{PSU}_3(3): & |\Omega| = 100 = 1+36+63 \\ G = \mathrm{Co}_2, & G_\alpha = \mathrm{McL}: & |\Omega| = 47104 = 1+275+2025+7128+15400+22275 \end{array}$$

The study of extremely primitive groups can be traced back to work of Manning in the 1920s. Indeed, a theorem of Manning from 1927 shows that if G is such a group then G_α acts faithfully on each of its nontrivial orbits, so G_α is a primitive permutation group in its own right. This is a very important observation because it implies that the abstract structure of G_α is rather restricted (indeed, we can apply the O'Nan-Scott Theorem to G_α). This is exploited in the proof of the following theorem (see [73, Theorem 1.1]):

Theorem 3.27 (Mann, Praeger & Seress, 2007)**.** *Any finite extremely primitive permutation group is either affine or almost simple.*

In the same paper, Mann, Praeger and Seress determine almost all the affine examples – as usual, there are a small number of infinite families, plus a handful of sporadic examples. They prove that their list is complete, up to finitely many additional groups. The reason they are unable to obtain a complete classification is related to an old conjecture of G.E. Wall from 1961 on the number of maximal subgroups of a finite group. The conjecture asserts that any finite group G has at most $|G|$ maximal subgroups (Wall proved this for soluble groups). In [73], this is needed in the case where G is simple, but it is only known to be true asymptotically, that is, if $|G| \geqslant c$ for some undetermined constant c. This is the reason why there may be finitely many additional examples.

Therefore, the main challenge is to determine the extremely primitive almost simple groups. With this aim in mind, Burness, Praeger and Seress have handled the case where the socle is an alternating, classical or sporadic group (see [24, 25]), and work on determining the groups with socle an exceptional group of Lie type is in progress. Again, it turns out that recent results on *bases* for almost simple groups plays a key role.

Remark 3.28. Wall's conjecture is false. The breakthrough occurred during an AIM workshop on group cohomology in June 2012; see

`http://aimath.org/news/wallsconjecture/wall.conjecture.pdf`

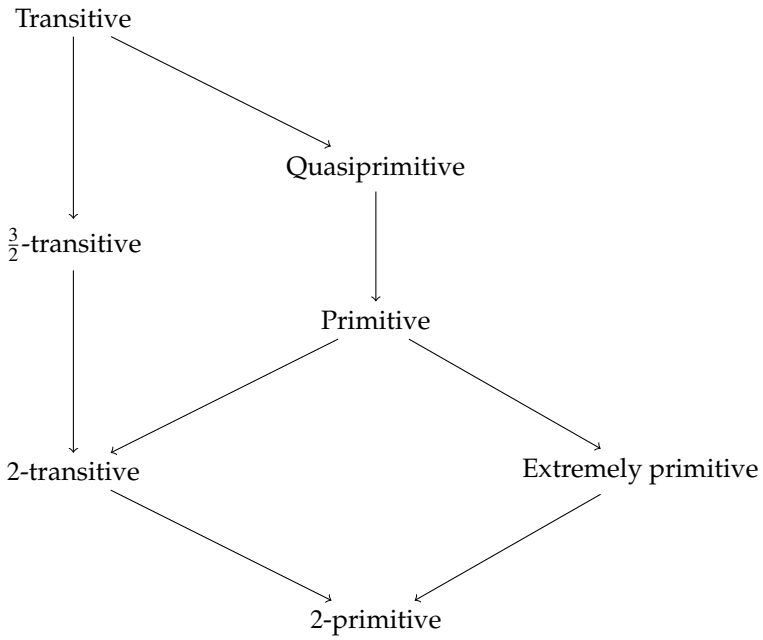

Figure 3.1: Some families of transitive permutation groups

for an exciting account of this discovery by Guralnick et al., which is based on extensive computer calculations with Kazhdan-Lusztig polynomials and 1-cohomology. The first counterexamples are primitive affine groups of the form $\mathrm{SL}_8(p) \ltimes V$ for some (large) irreducible module V for $\mathrm{SL}_8(p)$ and large prime p (large enough so that Lusztig's conjecture holds).

3.5.4 Quasiprimitivity

Recall that any nontrivial normal subgroup of a primitive group is transitive (see Lemma 3.5); this observation motivates the following definition. A permutation group $G \leqslant \mathrm{Sym}(\Omega)$ is *quasiprimitive* if every nontrivial normal subgroup of G is transitive. Clearly, every primitive group is quasiprimitive, but this is a weaker notion. For example, any transitive action of a finite simple group G is quasiprimitive, but it is only primitive if G_α is a maximal subgroup.

Praeger has established an analogue of the O'Nan-Scott Theorem for quasiprimitive groups (see [78]); similar families arise, with some tweaking of the conditions. For example, a diagonal-type group G with socle T^k (and $k \geqslant 3$) is quasiprimitive if and only if $G \leqslant T^k.(\mathrm{Out}(T) \times S_k)$ and the group induced by G on the k factors of T^k is transitive (rather than primitive). Quasiprimitive groups have applications in graph theory; for example, every (non-bipartite) 2-arc transitive graph is a cover of a 2-arc transitive graph with a quasiprimitive automorphism group, so properties of quasiprimitive groups are important in the study of such graphs.

In Figure 3.1 we present a diagrammatic representation of the relations between the various transitive permutation groups we have considered in this section.

4 Derangements

4.1 Introduction

The study of derangements is a classical topic with a rich history that can be traced all the way back to the early 18th century. It is an active area of current research, with numerous applications in diverse areas such as number theory, representation theory and topology. There are also many interesting open problems. In this section, we will introduce the basic notions and we will focus on the following themes:

- Existence
- Proportion
- Order
- Elusivity and related problems

Let G be a permutation group on a set Ω.

Definition 4.1. An element $x \in G$ is a *derangement* if it has no fixed points on Ω. Let $\Delta(G)$ be the set of derangements in G (which may be the empty set!).

Note that $\Delta(G)$ is a normal subset of G. For example, the derangements in S_5 (with respect to the natural action on $\{1,\ldots,5\}$) are $(1,2,3,4,5)$, $(1,2,3)(4,5)$ and their conjugates.

Clearly, if G is transitive with point stabiliser H then

$$\Delta(G) = G \setminus \bigcup_{g \in G} H^g \tag{4.1}$$

so $x \in G$ is a derangement if and only if $x^G \cap H$ is empty.

4.2 Existence

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group of degree $n \geqslant 2$. Recall that the *Orbit-Counting Lemma* states that

$$\frac{1}{|G|} \sum_{x \in G} |C_\Omega(x)| = k$$

where k is the number of orbits of G on Ω (see Exercise 4). Now, if G is transitive then $k = 1$ and $|C_\Omega(1)| = n \geqslant 2$, so there exists an element $x \in G$ with $|C_\Omega(x)| = 0$. In other words, G contains a derangement. This is a theorem of Jordan (see [59]):

Theorem 4.2 (Jordan, 1872)**.** *Let G be a transitive permutation group of degree $n \geqslant 2$. Then G contains a derangement.*

In view of (4.1), Jordan's theorem is equivalent to the well known fact that

$$G \neq \bigcup_{g \in G} H^g \tag{4.2}$$

for any proper subgroup H of a finite group G.

Remark 4.3. It is easy to see that Jordan's theorem does *not* extend to infinite permutation 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 $G = \mathrm{GL}(V)$. Let Ω be the set of complete flags of V, that is, the set of subspace chains

$$0 = U_0 \subset U_1 \subset U_2 \subset \cdots \subset U_{n-1} \subset U_n = V$$

where each U_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 (e.g. the Jordan canonical form), so x fixes a complete flag and thus G has no derangements.

(iii) More generally, let G be a connected algebraic group 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 action on the flag variety G/B. In fact, by a theorem of Fulman and Guralnick [45, Theorem 2.4], if G is a simple algebraic group acting on a coset variety G/H, then G is derangement-free if and only if one of the following holds:

(a) H contains a Borel subgroup (so H is a parabolic 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 $p = 2$.

As described by Serre [84], Theorem 4.2 has some interesting applications in number theory and topology:

(i) *A number-theoretic application.* Let $f \in \mathbb{Z}[x]$ be an irreducible polynomial of 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. 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:

- *How abundant are derangements in transitive permutation groups?*
- *Can we find derangements with additional properties, such as a prescribed order?*

4.3 Counting

Let G be a transitive permutation group on a set Ω of size $n \geqslant 2$. Let

$$\delta(G) = \frac{|\Delta(G)|}{|G|} \in (0,1)$$

denote the proportion of derangements in G (equivalently, $\delta(G)$ is the probability that a randomly chosen element of G is a derangement).

Examples 4.4.

(i) If $G = S_5$ and $\Omega = \{1,2,3,4,5\}$, then

$$\delta(G) = \frac{|(1,2,3,4,5)^G| + |(1,2,3)(4,5)^G|}{|G|} = \frac{24+20}{120} = \frac{11}{30}.$$

(ii) If G is regular then $\delta(G) = 1 - \frac{1}{n}$. In particular, $\delta(G)$ can be arbitrarily close to 1.

(iii) A 2-transitive group $G \leqslant \mathrm{Sym}(\Omega)$ is *sharply 2-transitive* if for any two pairs (α_1, α_2) and (β_1, β_2) of distinct elements in Ω there exists a *unique* $x \in G$ such that $(\alpha_1, \alpha_2)^x = (\beta_1, \beta_2)$. If G is such a group then $\delta(G) = \frac{1}{n}$ (see Exercise 21). This shows that $\delta(G)$ can be arbitrarily close to 0.

(iv) Consider the standard action of $G = D_{2n}$ on the set of vertices of a regular n-gon. It is an easy exercise to show that

$$\delta(G) = \begin{cases} 3/4 - 1/2n & n \text{ even} \\ 1/2 - 1/2n & n \text{ odd} \end{cases}$$

The study of derangements in transitive permutation groups has a long history. 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* [76], in which he presents a systematic combinatorial analysis of games of chance (e.g. card games, etc.) that were popular in the gambling dens of early 18th century Paris.

The card game *treize* features prominently in Montmort's book. Here is Montmort's description of the game (taken from the second edition of his book, published in 1713):

> "The players draw to see who will be the dealer. Let's call the dealer 'Pierre', and let's suppose that there are as many other players as you like. Pierre takes a full deck of 52 cards, shuffles them, and deals them out one after the other, calling out 'un' as he turns over the first card, 'deux' as he turns over the second, 'trois' as he turns over the third, and so on up to the thirteenth. Now if, in this whole series of cards, he never once turns over the card he is naming, he pays out what each other player has put up for the game, and the deal passes to the player sitting to his right."

Montmort studied several variations of this game. For example, suppose we start with 13 distinct cards from a single suit. In the language of permutation groups, Pierre's initial hand corresponds to an element of the symmetric group S_{13}, and he "loses" the game if this element is a derangement. Montmort calculated the following probability:

$$\mathbb{P}(\text{Pierre loses}) = \delta(S_{13}) = \frac{63633137}{172972800} = 0.36788...$$

More generally, Montmort introduced the familiar "inclusion-exclusion principle" to obtain the following formula for $\delta(S_n)$, for *any* n. (In the statement, $[x]$ denotes the integer nearest to x.)

Theorem 4.5 (Montmort, 1708)**.** *Consider the standard action of S_n on $\Omega = \{1,\dots,n\}$, where $n \geqslant 2$. Then*

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

In particular, $\delta(S_n)$ tends to $1/e$ as n tends to infinity.

Proof. Let $G = S_n$ and let $\delta'(G)$ be the probability that a randomly chosen element of G is *not* a derangement, so $\delta(G) = 1 - \delta'(G)$. In addition, for each $i \in \Omega$, let E_i be the event that a randomly chosen element of G fixes i. Then

$$\begin{aligned}
\delta'(G) &= \mathbb{P}(E_1 \cup \cdots \cup E_n) \\
&= \sum_i \mathbb{P}(E_i) - \sum_{i<j} \mathbb{P}(E_i \cap E_j) + \sum_{i<j<k} \mathbb{P}(E_i \cap E_j \cap E_k) - \cdots + (-1)^{n+1}\mathbb{P}(E_1 \cap \cdots \cap E_n) \\
&= \sum_i \frac{(n-1)!}{n!} - \sum_{i<j} \frac{(n-2)!}{n!} + \sum_{i<j<k} \frac{(n-3)!}{n!} - \cdots + (-1)^{n+1}\frac{1}{n!} \\
&= \binom{n}{1} \cdot \frac{(n-1)!}{n!} - \binom{n}{2} \cdot \frac{(n-2)!}{n!} + \binom{n}{3} \cdot \frac{(n-3)!}{n!} - \cdots + (-1)^{n+1}\frac{1}{n!} \\
&= 1 - \frac{1}{2!} + \frac{1}{3!} - \cdots + (-1)^{n+1}\frac{1}{n!}
\end{aligned}$$

□

Remark 4.6. More generally, the distribution of fixed points in a random permutation in S_n tends to a Poisson(1) distribution as n tends to infinity (see Diaconis et al. [37] for generalisations). Therefore, if X denotes the number of fixed points of a randomly chosen permutation in S_n, then for each fixed integer $k \geqslant 0$ we have

$$\mathbb{P}(X = k) \to \frac{1}{k!e} \text{ as } n \to \infty$$

In general, it is very difficult to compute $\delta(G)$ precisely and we must make do with bounds. Of course, Jordan's theorem implies that $\delta(G) > 0$, but can we do better?

Rather surprisingly, the first general result in this direction only appeared in 1992 [31]; the proof of Theorem 4.7 below is another nice application of the Orbit-Counting Lemma. Further motivation stems from a problem posed by the number theorist H. Lenstra:

Is there a lower bound on $\delta(G)$ in terms of n?

This problem arose naturally in Lenstra's analysis of the number field sieve in integer factorisation (see [15]). The connection is as follows. Let $f \in \mathbb{Z}[x]$ be an irreducible polynomial of degree n, and let $\pi(m)$ be the number of prime numbers $p \leqslant m$. Define

$$Z(f,m) = \frac{|\{p \in \pi(m) \mid f \text{ has no roots modulo } p\}|}{\pi(m)}.$$

By Chebotarev's density theorem, $Z(f,m)$ tends to $\delta(G)$ as m tends to infinity, where G is the Galois group of f viewed as a permutation group on its roots. (In particular, since Jordan's theorem implies that $\delta(G) > 0$, one can show that there are infinitely many primes p such that f has no roots modulo p; see [84, Section 4].)

Theorem 4.7 (Cameron & Cohen, 1992)**.** *Let G be a transitive permutation group of degree $n \geqslant 2$. Then $\delta(G) \geqslant 1/n$, with equality if and only if G is sharply 2-transitive.*

Proof. Fix $\alpha \in \Omega$ and set $H = G_\alpha$, so $|G| = n|H|$. By the Orbit-Counting Lemma,

$$\sum_{x \in G} |C_\Omega(x)| = |G|$$

and

$$\sum_{x \in H} |C_{\Omega\setminus\{\alpha\}}(x)| = k|H| = \frac{k|G|}{n}$$

where k denotes the number of orbits of H on $\Omega \setminus \{\alpha\}$. Therefore,

$$\begin{aligned} |G| - \frac{k|G|}{n} = \sum_{x \in G} |C_\Omega(x)| - \sum_{x \in H} |C_{\Omega\setminus\{\alpha\}}(x)| &= \sum_{x \in G} |C_\Omega(x)| - \sum_{x \in H} |C_\Omega(x)| + |H| \\ &= \sum_{x \in G\setminus(\Delta(G)\cup H)} |C_\Omega(x)| + |H| \\ &\geqslant (|G| - |\Delta(G)| - |H|) + |H| = |G| - |\Delta(G)| \end{aligned}$$

Rearranging, we get

$$\delta(G) = \frac{|\Delta(G)|}{|G|} \geqslant \frac{k}{n} \geqslant \frac{1}{n}.$$

Moreover, if equality holds, then $k = 1$ and thus G is 2-transitive. Further, if $|C_\Omega(x)| \geqslant 2$ for some $x \in G$ then $x \in H$, so x fixes α. But this holds for *any* choice of α, so $x = 1$ and thus G is sharply 2-transitive. See Exercise 21 for the converse. □

This result is clearly best possible, but stronger bounds hold if we allow some specified exceptions. Here the best result to date is due to Guralnick and Wan [52]:

Theorem 4.8 (Guralnick & Wan, 1997)**.** *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 sharply 2-transitive;*

(iii) $(G,n) = (S_4,4)$, $(S_5,5)$, $(A_5,5)$ *or* $(Z_3,3)$.

The cases in (iii) are genuine exceptions (e.g. recall that if $(G,n) = (S_5,5)$ then $\delta(G) = 11/30 < 2/5$). It is interesting to note that this extension of the lower bound on $\delta(G)$ from $1/n$ to $2/n$ requires the classification of 2-transitive groups, which in turn relies on CFSG. As explained in [52], this result has applications to algebraic curves over finite fields.

Inspired by Montmort's theorem on the proportion of derangements in S_n, it is natural to consider the asymptotic behaviour of $\delta(G)$ when G belongs to other interesting infinite families of groups, such as simple groups. For example, it is not too difficult to show that $\delta(A_n) \geqslant 1/3$ and $\delta(\mathrm{PSL}_2(q)) \geqslant 1/3$ for all $n,q \geqslant 5$ (in terms of the standard actions of degree n and $q+1$, respectively; see Exercise 24). In both cases, we observe that $\delta(G)$ is bounded away from zero by an absolute constant. Indeed, a deep theorem of Fulman and Guralnick [42, 43, 44, 45] shows that this property holds for *any* simple transitive group.

Theorem 4.9 (Fulman & Guralnick, 2014)**.** *There exists an absolute constant $\varepsilon > 0$ such that $\delta(G) > \varepsilon$ for any simple transitive group G.*

This theorem confirms a conjecture of Boston et al. [11] and Shalev. The proof uses CFSG, and a detailed analysis of the conjugacy classes and maximal subgroups of simple groups. Note that for the purposes of deriving a lower bound on $\delta(G)$, we may assume that G is primitive.

The asymptotic nature of the proof does not yield an explicit constant, although it is claimed in [45] that we can take ε to be approximately $1/25$ with at most finitely many exceptions (it is expected that there are no exceptions, and it is speculated in [11, p.3274] that the optimal constant is $\varepsilon = 2/7$, which is realised by the standard action of $\mathrm{PSL}_3(2)$). 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 k-sets with k bounded, for example).

Remark 4.10. Let's make a few additional comments on Theorem 4.9:

(i) The result 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 $G = \mathrm{PGL}_2(p^r) \rtimes \langle \phi \rangle$ and $\Omega = \phi^G$, where ϕ is a field automorphism of $\mathrm{PGL}_2(p^r)$ of order r (so G acts transitively on Ω, and $G_\alpha = \mathrm{PGL}_2(p) \times \langle \phi \rangle$). Then every element in $G \setminus \mathrm{PGL}_2(p^r)$ has a fixed point, whence

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

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

(ii) Using Theorem 4.9 and the O'Nan-Scott Theorem, Fulman and Guralnick have established a weaker bound that applies more generally: There exists an absolute constant $\varepsilon > 0$ such that $\delta(G) > \varepsilon/\log n$ for any non-affine primitive group of degree $n \geqslant 2$ (see [45, Theorem 1.5]). In view of (i), taking $p = 2$, this is essentially best possible.

(iii) For a general finite primitive group G, the parameter $\delta(G)$ behaves rather differently. Indeed, by a theorem of Boston et al. [11, Theorem 5.11], the set

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

is dense in the open interval $(0,1)$. However, it is *not* known if this set is equal to $(0,1) \cap \mathbb{Q}$.

(iv) Let G be a simple algebraic group acting on a coset variety G/H, as in part (iii) of Remark 4.3. Here [45, Lemma 2.2] implies that $G \setminus \Delta(G)$ is dense in G (with respect to the Zariski topology) if and only if H contains a maximal torus of G. In particular, if H does not contain a maximal torus then 'almost all' elements in G are derangements (in the sense that $\Delta(G)$ contains a non-empty open subvariety of G).

4.4 Order and elusivity

In this section we will consider derangements with additional properties, such as a specified order. The most general result in this direction is the following theorem of Fein, Kantor and Schacher [41] concerning derangements of prime power order:

Theorem 4.11 (Fein, Kantor & Schacher, 1981)**.** *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group of degree $n \geqslant 2$. Then G contains a derangement of prime power order.*

Sketch proof. The basic strategy is as follows. Assume the theorem is false and let G be a minimal counterexample (with respect to $|G|$), so each $x \in G$ of prime power order has fixed points. Suppose G is imprimitive and let $\Delta = \{\Gamma_1, \ldots, \Gamma_k\}$ be a maximal block system. The primitive group $G^\Delta \leqslant \mathrm{Sym}(\Delta)$ induced by G on Δ also has no derangements of prime power order (indeed, if $y \in G$ induces a derangement of p-power order on Δ, then some power y^m (with $(m,p) = 1$) is a derangement of p-power order on Ω). Therefore, we may assume G is primitive. Let N be a nontrivial normal subgroup of G. Then N is transitive on Ω (see Lemma 3.5) and N does not contain a derangement of prime power order, so the minimality of $|G|$ implies that $N = G$, whence G is simple.

The proof now proceeds case-by-case through the various families of simple groups arising in the Classification. It would be very interesting to find a Classification-free proof!

Let's give some details in the case $G = A_d$, $d \geqslant 5$. Set $H = G_\alpha$, which is a maximal subgroup since G is primitive. Suppose H acts intransitively on $\{1,\ldots,d\}$, so $H = (S_e \times S_{d-e}) \cap G$ for some $1 \leqslant e < d$. Let p be a prime divisor of d and write $d = d_p t$, where d_p is the largest p-power dividing d. If p is odd, let $x \in G$ be the product of t disjoint cycles of length d_p and note that H contains a conjugate of x (because we are assuming that H meets every G-class of elements of prime order), so d_p divides e. Similarly, if $p = 2$ and $d_2 \geqslant 4$ then H contains an element that is the product of $2t$ disjoint cycles of length $d_2/2$, so $d_2/2$ divides e. Therefore, $e = d/2$ is the only possibility, so $H = (S_{d/2} \times S_{d/2}) \cap G$ and $|H|$ divides $((d/2)!)^2$. By *Bertrand's Postulate*, there is a prime p such that $d/2 < p < d$. Let $x \in G$ be an element of order p. Since p does not divide $|H|$, it follows that $x^G \cap H$ is empty, so x is a derangement. This is a contradiction, whence H is transitive.

Since G does not contain a derangement of order 3, it follows that H contains a 3-cycle, and thus H acts imprimitively on $\{1,\ldots,d\}$ (since A_d is the only primitive subgroup of A_d containing a 3-cycle, by Theorem 3.20). Therefore, $H = (S_a \wr S_b) \cap G$ for integers $a, b > 1$ with $d = ab$, so $|H|$ divides $(a!)^b(b!)$. Now choose a prime p such that $d/2 < p < d$, and repeat the above argument. □

One of the original motivations for Theorem 4.11 stems from an application in number theory. 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 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, m, and the set of equivalence classes forms a group under tensor product. This is called the *Brauer group* of K, denoted $\mathscr{B}(K)$. Now, if L/K is a field extension then 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 homomorphism. The connection to derangements arises from the key observation that Theorem 4.11 is equivalent to the fact that $\mathscr{B}(L/K)$ is infinite for any nontrivial extension of global fields. See [41] for further details.

In view of Theorem 4.11, it is natural to ask whether or not every transitive group contains a derangement of *prime* order. First observe that $G \leqslant \mathrm{Sym}(\Omega)$ contains a derangement of prime order p only if $|\Omega|$ is divisible by p (since every cycle in the decomposition of a derangement of order p must have length p). Also note that if G contains a nontrivial semiregular subgroup H, then any element $x \in H$ of prime order is a derangement. More precisely, G contains a derangement of prime order if and only if G has a nontrivial semiregular subgroup. However, not all transitive permutation groups contain such elements:

Examples 4.12.

(i) Consider the 3-transitive action of the smallest Mathieu group $G = \mathrm{M}_{11}$ on $12 = 2^2.3$ points, so $G_\alpha = \mathrm{PSL}_2(11)$. Here G has unique conjugacy classes of elements of order 2 or 3, and $|G_\alpha|$ is divisible by 2 and 3, so G does not contain a derangement of prime order. (Note that G contains a derangement of order 4.)

(ii) The following example is due to Fein, Kantor and Schacher [41]. Let $p = 2^n - 1$ be a Mersenne prime and let G be the group

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

of affine transformations of $\mathbb{F}_{p^2}$. Let $H = \mathrm{AGL}_1(p)$ be the subgroup of transformations with $a, b \in \mathbb{F}_p$. Then G acts transitively on G/H, so we may view G as a permutation group of degree $p(p+1)$. Since G contains a unique conjugacy class of elements of order 2 or p, we deduce that G does not contain a derangement of prime order. Generalisations of this construction are given in [32], producing elusive groups of degree $p^m(p+1)$ for all Mersenne primes p and all positive integers m.

The terminology in the next definition suggests that transitive groups with no derangements of prime order are somewhat rare.

Definition 4.13. Let G be a transitive group of degree $n \geqslant 2$. Following [32], we say that G is *elusive* if it does not contain a derangement of prime order. Furthermore, following [18], if p is a prime divisor of n then G is *p-elusive* if G does not contain a derangement of order p, and *strongly p-elusive* if G does not contain a derangement of p-power order.

Elusive permutation groups have been much studied in recent years. For example, various constructions are given in [32, 47], and the following theorem of Giudici [46] classifies the (quasi)primitive elusive groups. (Note that this result indicates that every quasiprimitive elusive group arises naturally from the specific example in part (i) of Examples 4.12.)

Theorem 4.14 (Giudici, 2003)**.** *Let G be an elusive permutation group on Ω with a transitive minimal normal subgroup N. Then $G = \mathrm{M}_{11} \wr K$ acting with its product action on $\Omega = \Gamma^k$ for some $k \geqslant 1$, where K is a transitive subgroup of S_k and $|\Gamma| = 12$.*

Sketch proof. By Lemma 2.5(ii), $N = T^k$ for some simple group T. Note that N is also elusive. If T is abelian, then the transitivity of N implies that $N_\alpha = N_\beta$ for all $\alpha, \beta \in \Omega$, so N is regular, but this contradicts the fact that N is elusive (all elements of prime order have fixed points). Therefore, T is a nonabelian simple group.

Set $L = N_\alpha$ and write $N = T^k = T_1 \times \cdots \times T_k$ and $L_i = L \cap T_i$. Let C_i be a conjugacy class of T_i containing elements of prime order. Then C_i is a conjugacy class of N, and thus the elusivity of N implies that $C_i \cap L$ is non-empty and so $L_i \neq 1$. Moreover, the action of T_i on the set of cosets T_i/L_i is elusive.

This essentially reduces the problem to determining the simple elusive groups. At this point, Giudici appeals to a theorem of Liebeck, Praeger and Saxl [67, Corollary 5], which lists all the finite simple groups which have a proper subgroup with the same set of prime divisors. One then has to study the cases on this list to determine whether or not there is a derangement of prime order. It turns out that the only simple elusive group is M_{11} acting on a set of size 12 with point stabiliser $\mathrm{PSL}_2(11)$. Therefore, $T_i = \mathrm{M}_{11}$, $L_i = \mathrm{PSL}_2(11)$ and the given structure of G quickly follows (note that K is transitive since $N = (\mathrm{M}_{11})^k$ is a minimal normal subgroup). □

Corollary 4.15. *The 3-transitive action of M_{11} on 12 points is the only almost simple primitive elusive group.*

In other words, with a single exception, every almost simple primitive group contains a derangement of prime order. This observation has motivated recent work of Burness, Giudici and Wilson that aims to provide a systematic, quantitative study of derangements of prime order in almost simple primitive groups. A basic question is the following:

> *Let G be an almost simple primitive group of degree n, and let p be a prime divisor of n. Does G contain a derangement of order p?*

Further impetus for focussing on the almost simple case comes from the following reduction theorem (see [18, Theorem 2.1]; the proof uses the O'Nan-Scott Theorem):

Theorem 4.16. *Let G be a primitive permutation group on a finite set Ω, with socle N. Let p be a prime dividing $|\Omega|$. Then one of the following holds:*

(i) *G is almost simple;*

(ii) *N contains a derangement of order p;*

(iii) *$G \leqslant H \wr S_k$ acting with its product action on $\Omega = \Gamma^k$ for some $k \geqslant 2$, where $H \leqslant \mathrm{Sym}(\Gamma)$ is primitive, almost simple and the socle of H is p-elusive.*

A detailed analysis of derangements of prime order in almost simple primitive groups with socle an alternating or sporadic group is given in [18]; in particular, all the p-elusive and strongly p-elusive examples are determined. An analogous study of derangements in almost simple classical groups will appear in the forthcoming book [17], as an application of a more general investigation of the subgroup structure and conjugacy classes of classical groups.

Finally, let's record an intriguing open problem on the degrees of elusive groups (in some sense, a positive solution would formally justify the terminology):

Does the set of degrees of elusive groups have density zero as a subset of $\mathbb{N}$?

4.5 The polycirculant conjecture

In a different direction, derangements of prime order arise naturally in graph theory. Recall that a *digraph* Γ consists of a set $\mathscr{V}$ of vertices and a set $\mathscr{A}$ of ordered pairs of distinct elements of $\mathscr{V}$, called *arcs*. An *automorphism* of Γ is a permutation g of $\mathscr{V}$ such that $(u,v) \in \mathscr{A}$ if and only if $(u^g, v^g) \in \mathscr{A}$, and $\mathrm{Aut}(\Gamma)$ denotes the automorphism group of Γ. We say that Γ is *vertex-transitive* if $\mathrm{Aut}(\Gamma)$ acts transitively on $\mathscr{V}$. We will also say that Γ admits a derangement of prime order if $\mathrm{Aut}(\Gamma)$ contains such an element (with respect to the action of $\mathrm{Aut}(\Gamma)$ on $\mathscr{V}$).

In 1981, Marušič [75] asked the following question:

Does every finite vertex-transitive digraph admit a derangement of prime order?

For example, if G is a nontrivial finite group and $S \subset G$ is a subset with $1 \notin S$, then the corresponding *Cayley digraph* $\mathrm{Cay}(G,S)$ has the desired property (here $\mathscr{V} = G$, and $(g,h) \in \mathscr{A}$ if and only if $hg^{-1} \in S$). Indeed, observe that G acts regularly by right multiplication on the vertices of $\mathrm{Cay}(G,S)$.

Marušič's question can be generalised as follows. 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 example, 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 $\mathscr{A}$ setwise, and so must be 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 $Z_2 \times Z_2$ on four points is 2-closed, but it is not the full automorphism group of any digraph.

In 1997, Klin [29] extended Marušič's question to 2-closed groups. This led to what is now referred to as the *Polycirculant Conjecture*.

Conjecture 4.17 (The Polycirculant Conjecture)**.** *Let G be a finite transitive 2-closed permutation group. Then G has 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; of course, none of the known elusive groups are 2-closed! Giudici's theorem implies that all minimal normal subgroups of a counterexample to the Polycirculant Conjecture must be intransitive, which is a strong restriction. Various special cases have been handled in recent years, but the full conjecture (and indeed Marušič's original question) is still very much open.

4.6 Related problems and applications

To close this discussion on derangements, we briefly mention some related problems.

1. *Normal coverings.* Let G be a finite group and recall that if H is a proper subgroup of G then the union of the G-conjugates of H is a proper subset of G (see (4.2)). 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 [13, 14], 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.

2. *Character theory.* Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group of degree $n \geqslant 2$ with point stabiliser H, and let $\chi = 1_H^G$ be the corresponding permutation character (so $\chi(x) =$

$|C_\Omega(x)|$ for all $x \in G$). In this context, Theorem 4.2 implies that $\chi(x) = 0$ for some $x \in G$ (in which case, we say that χ *vanishes* at x), and there is an element of prime power order with this property by Theorem 4.11. In fact, a classical theorem of Burnside implies that if χ is *any* nonlinear irreducible complex character of G then $\chi(x) = 0$ for some $x \in G$, and a much more recent result of Malle, Navarro and Olsson [72] tells us that we can choose x with prime power order. The proof of the latter result uses Theorem 4.11.

In recent work, Burness and Tong-Viet [27] have determined the finite primitive permutation groups with a unique conjugacy class of derangements (for example, any sharply 2-transitive group has this property), and this is used to obtain detailed information on the structure of finite groups with a nonlinear irreducible character that vanishes on a unique conjugacy class.

3. *Isbell's conjecture.* Recall that if G is a transitive permutation group of degree $n \geqslant 2$, then Theorem 4.11 guarantees the existence of a derangement of p-power order for some prime p, but the proof does not provide any information about the primes involved. This is related to the following conjecture of Isbell from the early 1960s, which asserts that if a particular prime power dominates n, then G contains a derangement that has order a power of that prime.

   Conjecture (Isbell, c.1960). *Let p be a prime. There is a function $f(p,k)$ such that, if G is a transitive permutation group of degree $n = p^a k$ with $(p,k) = 1$ and $a \geqslant f(p,k)$ then G contains a derangement of p-power order.*

   Very little progress has been made on this conjecture (even for the prime $p = 2$, for example).

4. *Algorithms.* Given a set of generators for a permutation group G of degree $n \geqslant 2$, there are efficient (polynomial time) algorithms to determine whether or not G is transitive. If G is transitive, then Jordan's theorem implies that G contains a derangement, and there are efficient randomised algorithms to find a derangement in G. For instance, if we randomly choose m elements in G, then Theorem 4.7 implies that the probability that none of these elements is a derangement is at most

$$(1 - 1/n)^m < e^{-m/n}.$$

   Therefore, if we choose n^2 elements then the probability that one of them is a derangement is at least $1 - e^{-n}$. Very recently, a theoretical computer scientist, Vikraman Arvind, has *derandomised* this process and obtained a *deterministic* polynomial-time algorithm for finding a derangement that does not rely on CFSG (see [1]).

5. *Thompson's question.* J.G. Thompson has posed the following question (see Problem 8.75 in the Kourovka Notebook [62]):

   Let G be a finite primitive permutation group. Is $\Delta(G)$ a transitive subset of G?

   In other words, if $\alpha, \beta \in \Omega$ with $\alpha \neq \beta$ then is there a derangement $g \in G$ such that $\alpha^g = \beta$? It is not difficult to show that primitivity is essential here.

5 Bases

5.1 Introduction

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group. Since G acts faithfully on Ω, the identity is the only element of G that fixes every point in Ω. However, there may be smaller subsets of Ω with a trivial pointwise stabiliser. For example, if $G = \mathrm{GL}(V)$ and $\Omega = V$, then any subset of V containing a basis (in the usual sense of linear algebra) has this property. This leads us naturally to the notion of a *base* for G, which is another classical concept in permutation group theory. We will see that bases have many applications (both old and new), and there have been major advances in our understanding in recent years, using a wide range of tools and techniques. In particular, probabilistic methods have been used very effectively. We will focus on the following themes:

- Bounds for primitive groups
- Bases for almost simple groups: probabilistic methods
- Bases for algebraic groups

Definition 5.1. A subset B of Ω is a *base* for G if the pointwise stabiliser of B in G is trivial, i.e.

$$\bigcap_{\alpha \in B} G_\alpha = 1.$$

The *base size* of G, denoted by $b(G)$, is the minimal size of a base for G.

Note that Ω is always a base for G, so every permutation group has at least one base. Also note that if B is a base for G then so is $B^x = \{\alpha^x \mid \alpha \in B\}$ for all $x \in G$.

Examples 5.2.

(i) If $G = S_n$ and $\Omega = \{1, \ldots, n\}$, then $b(G) = n-1$. Similarly, $b(G) = n-2$ for the standard action of $G = A_n$.

(ii) At the other extreme, $b(G) = 1$ if and only if G has a regular orbit.

(iii) If $G = D_{2n}$ and Ω is the set of vertices of a regular n-gon, then $b(G) = 2$.

(iv) If G is a Frobenius group then $b(G) = 2$.

(v) Let V be a finite-dimensional vector space and set $G = \mathrm{GL}(V)$ and $\Omega = V$. Then $B \subseteq \Omega$ is a base if and only if B contains a basis of V. In particular, $b(G) = \dim V$.

(vi) Similarly, $b(G) = \dim V + 1$ if $G = \mathrm{PGL}(V)$ and Ω is the set of 1-dimensional subspaces of V.

(vii) If $G = HV \leqslant \mathrm{AGL}(V)$ is affine, then $b(G) = b(H) + 1$.

Remark 5.3. A base $B \subseteq \Omega$ is *minimal* if no proper subset of B is a base, i.e. $\bigcap_{\alpha \in B \setminus \{\beta\}} G_\alpha \neq 1$ for all $\beta \in B$. Of course, B is minimal if $|B| = b(G)$, but there may be larger minimal bases. For example, consider the natural action of $G = S_m$ on the set of 2-element subsets of $\{1, \ldots, m\}$, where $m \equiv 1 \pmod{12}$. Then

$$B_1 = \{\ \{1,2\},\{2,3\},\quad \{4,5\},\{5,6\},\quad \ldots\ \}$$

$$B_2 = \left\{ \begin{array}{ccc} \{1,2\},\{3,4\}, & \{5,6\},\{7,8\}, & \ldots \\ \{1,3\} & \{5,7\} & \end{array} \right\}$$

are both minimal bases for G (for example, if we remove $\{1,2\}$ from B_2, then the transposition $(2,m)$ fixes all the remaining sets), and $|B_1| = \frac{2}{3}(m-1)$, $|B_2| = \frac{3}{4}(m-1)$. In fact, $b(G) = \frac{2}{3}(m-1)$.

Bases arise naturally in several different contexts:

1. *Abstract group theory.* Let G be a finite group and let H be a core-free subgroup of G, so

$$\bigcap_{x \in G} H^x = 1$$

and G acts faithfully on the set of cosets $\Omega = G/H$, so we may view G as a permutation group on Ω. In this context, $b(G)$ is the size of the smallest subset $S \subseteq G$ such that

$$\bigcap_{x \in S} H^x = 1.$$

In particular, $b(G) = 2$ if and only if $H \cap H^x = 1$ for some $x \in G$.

2. *Permutation group theory.* Let G be a permutation group on a set Ω, and let B be a base for G. Observe that if $x, y \in G$ then

$$\alpha^x = \alpha^y \text{ for all } \alpha \in B \iff xy^{-1} \in \bigcap_{\alpha \in B} G_\alpha \iff x = y, \tag{5.1}$$

in other words, two elements of G are equal if and only if they have the same effect on a base. Therefore, if $|\Omega|$ is finite then $|G| \leqslant |\Omega|^{|B|}$, so

$$|G| \leqslant |\Omega|^{b(G)} \tag{5.2}$$

and we can use an upper bound on $b(G)$ to bound the order of G. This method was used to obtain many of the bounds on the order of a primitive group that we highlighted in Section 3.4.1. We will say more about this in Section 5.2.

3. *Computational group theory.* The concept of a *base and strong generating set* (BSGS) was introduced by Sims [85] in the early 1970s, and it plays a major role in the computational study of permutation groups. Given a base $B = \{\alpha_1, \ldots, \alpha_b\}$ for G, we obtain a subgroup chain

$$G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \ldots \geqslant G_{b-1} \geqslant G_b = 1 \tag{5.3}$$

where $G_i = \bigcap_{j=1}^{i} G_{\alpha_j}$. A subset S of G is a *strong generating set* for G (with respect to B) if $G_i = \langle S \cap G_i \rangle$ for all i. A BSGS for G provides an efficient way to encode the elements of G; by (5.1), each element of G is uniquely determined by its action on B, so it can be encoded as a $|B|$-tuple, rather than a $|\Omega|$-tuple. In addition, a BSGS can be used to compute the order of G, and to test membership in G; basic routines that form the basis of more sophisticated algorithms. The underlying philosophy here is the following:

$$\text{small bases} \rightsquigarrow \text{faster, more efficient algorithms.}$$

As a consequence, bases are essential in the familiar computer packages GAP and MAGMA. See [83, Section 4] for more details.

4. *Graph theory.* Let Γ be a graph with vertices V and automorphism group $G = \mathrm{Aut}(\Gamma) \leqslant \mathrm{Sym}(V)$. Then

$$\begin{aligned} b(G) &= \text{the } \textit{fixing number} \text{ of } \Gamma \\ &= \text{the } \textit{determining number} \text{ of } \Gamma \\ &= \text{the } \textit{rigidity index} \text{ of } \Gamma \end{aligned}$$

is a well-studied graph invariant. See the excellent survey article by Bailey and Cameron [5] for further details and much more.

Remark 5.4. As remarked in Section 3.5, results on bases have played an important role in recent efforts to classify certain families of transitive permutation groups. More precisely, if $G \leqslant \mathrm{Sym}(\Omega)$ is non-Frobenius and $\frac{3}{2}$-*transitive*, then $b(G) > 2$. Indeed, if $b(G) = 2$ then G_α has a regular suborbit, so G is $\frac{3}{2}$-transitive if and only if $G_{\alpha,\beta} = 1$ for all $\beta \in \Omega \setminus \{\alpha\}$, in which case G is Frobenius. Similarly, if G is almost simple and *extremely primitive* then $b(G) > 2$ (this is using the fact that no maximal subgroup of an almost simple group has prime order). Consequently, the proofs of the main theorems in [6, 24, 25] use recent work towards a classification of the almost simple groups G with the extremal $b(G) = 2$ property.

For the groups in Examples 5.2, it is easy to compute the exact base size. However, in general this is very difficult (indeed, algorithmically, this is known to be an *NP-hard* problem; see [9]) and we are often interested in obtaining bounds, with a particular focus on upper bounds.

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group on a finite set Ω and let $B = \{\alpha_1, \ldots, \alpha_{b(G)}\} \subseteq \Omega$ be a base. As in (5.3), B determines a stabiliser chain (with $b = b(G)$), and the minimality of B implies that all the inclusions in this chain are proper. Therefore, $|G| \geqslant 2^{b(G)}$, and combining this with (5.2) above, we deduce that

$$\frac{\log |G|}{\log |\Omega|} \leqslant b(G) \leqslant \log |G| \tag{5.4}$$

Notation. In (5.4) and throughout this section, all logarithms are with respect to the base 2.

Examples 5.5. It is easy to give examples of transitive groups G such that $b(G)$ is at either end of the range given in (5.4):

(i) Let $G = S_n$ and $\Omega = \{1, \ldots, n\}$. Then

$$b(G) = n - 1 < 2\frac{\log |G|}{\log |\Omega|}$$

(ii) Let $G = Z_2 \wr Z_k = Z_2^k \rtimes Z_k$ and $\Omega = \{1, \ldots, 2k\}$ (the standard action of the wreath product); $G < S_{2k}$ is a subgroup of permutations that preserve the partition

$$\Omega = \{1,2\} \cup \{3,4\} \cup \cdots \cup \{2k-1, 2k\}.$$

Then

$$b(G) = k = \log |G| - \log k > \frac{1}{2} \log |G|$$

Note that G is primitive in (i) and imprimitive in (ii). Therefore, it is natural to ask whether or not we can improve the upper bound on $b(G)$ in (5.4) if we restrict our attention to primitive groups. As we shall see in the next section, this is a very active area of current research.

5.2 Bounds for primitive groups

Let G be a primitive permutation group of degree n. A classical problem in permutation group theory is to find an upper bound on $b(G)$ in terms of n (as noted above, this yields an upper bound on $|G|$ in terms of n, which is the problem we discussed earlier in Section 3.4.1). We know that $b(G) = n - 1$ if $G = S_n$, and similarly $b(G) = n - 2$ if $G = A_n$, so let us assume $G \neq A_n, S_n$. In this situation, one of the earliest results is the following theorem:

Theorem 5.6 (Bochert, 1889)**.** *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive permutation group of degree n not containing A_n. Then $b(G) \leqslant n/2$.*

Proof. Seeking a contradiction, suppose B is a base of minimal size and $|B| > n/2$. Let $C = \Omega \setminus B$, so $|C| < |B|$ and thus C is not a base. In particular, there exists $1 \neq x \in \bigcap_{\alpha \in C} G_\alpha$, so $\mathrm{supp}(x) \subseteq B$, where we recall that

$$\mathrm{supp}(x) = \{\alpha \in \Omega \mid \alpha^x \neq \alpha\}$$

is the set of points in Ω moved by x. Fix $\alpha \in \mathrm{supp}(x)$. By minimality, $B \setminus \{\alpha\}$ is not a base, so there exists $1 \neq y \in \bigcap_{\beta \in B \setminus \{\alpha\}} G_\beta$, i.e. $\mathrm{supp}(y) \subseteq \Omega \setminus (B \setminus \{\alpha\}) = C \cup \{\alpha\}$. Since B is a base, $\mathrm{supp}(y) \cap B$ is non-empty, so $\alpha \in \mathrm{supp}(y)$ and thus $\mathrm{supp}(x) \cap \mathrm{supp}(y) = \{\alpha\}$. Therefore, G contains a 3-cycle (see Exercise 5), so Theorem 3.20 implies that G is A_n or S_n. We have reached a contradiction. □

The next major advance was established by Babai [3, 4], almost 100 years later:

Theorem 5.7 (Babai, 1981)**.** *Let G be a primitive permutation group of degree n not containing A_n.*

(i) *If G is not 2-transitive then $b(G) < 4\sqrt{n} \log n$.*

(ii) *If G is 2-transitive then $b(G) < c^{\sqrt{\log n}}$ for some absolute constant c.*

It is remarkable that Babai's proof is 'elementary' in the sense that it is CFSG-free. However, by appealing to the Classification, Liebeck [64] proved the following stronger result, which is essentially best possible (note that we allow $k = 1$ in part (ii), in which case G is almost simple). The final statement yields the bound $|G| < n^{c\sqrt{n}}$, as recorded in Theorem 3.17.

Theorem 5.8 (Liebeck, 1984). *Let G be a primitive permutation group of degree n not containing A_n. Then either*

(i) $b(G) < 9\log n$; *or*

(ii) $G \leqslant H \wr S_k$ *is a product-type group, where* $H \leqslant \mathrm{Sym}(\Gamma)$ *is a primitive group with socle* A_m, *and* Γ *is the set of* d*-element subsets of* $\{1,\ldots,m\}$.

In particular, $b(G) < c\sqrt{n}$ *for some absolute constant* c.

Sketch proof.

Main steps. The proof is accomplished in three steps, using the familiar combination of the O'Nan-Scott Theorem, CFSG and structural information on the simple groups themselves:

1. Use O'Nan-Scott to reduce the problem to almost simple groups.
2. Show that if G is almost simple, then either $|G| < n^9$, or G is *standard* in the following sense:
   - Either $\mathrm{Soc}(G) = A_m$ and Ω is an orbit of subsets or partitions of $\{1,\ldots,m\}$; or
   - $\mathrm{Soc}(G) = Cl(V)$ is a classical group and Ω is an orbit of subspaces of V.

   To establish the bound $|G| < n^9$, we need information on the maximal subgroups of G (recall that $n = |G : G_\alpha|$ and G_α is a maximal subgroup of G).
3. If $|G| < n^9$ then (5.4) implies that $b(G) \leqslant \log|G| < 9\log n$, as required. For the *standard* groups, it is not too difficult to write down a base of the required size.

O'Nan-Scott reduction. Let's look more closely at the first step. Set $H = G_\alpha$ and $N = \mathrm{Soc}(G) = T^k$ for some simple group T. First assume N is regular, so $G = HN$ is a semidirect product and the action of G on Ω is isomorphic to the action of G on N given by

$$a^{hn} = (h^{-1}ah)n$$

for all $h \in H$ and $a,n \in N$ (see Section 2.5). Note that $C_H(N) = 1$ since the action is faithful. Let $\{1,n_1,\ldots,n_t\}$ be a generating set for N (where 1 is the identity element of N); we claim that this is a base for G. Suppose $g \in G$ fixes each element in this set. Write $g = xy$ with $x \in H$ and $y \in N$. Since $1^{xy} = 1$, it follows that $y = 1$, so the relation $n_i^{xy} = n_i$ implies that $x \in C_H(n_i)$. Therefore, $x \in C_H(N) = 1$ and thus $x = 1$. This justifies the claim. Since every finite simple group is 2-generated, we can choose $t \leqslant 2k$, so

$$b(G) \leqslant 2k+1 \leqslant 2\log n + 1$$

(here $n = |N| = |T|^k$) and the result follows. This eliminates affine groups and twisted wreath products, so we may assume G is either product-type or diagonal-type.

Product-type groups. Suppose $G \leqslant H \wr P$ is a product-type group, where $H \leqslant \mathrm{Sym}(\Gamma)$ is almost simple with socle T, $P \leqslant S_k$ is transitive (with $k \geqslant 2$), and G acts on $\Omega = \Gamma^k$ with the product action (see (2.2)). Write $|\Gamma| = m$, so $n = m^k$. Assuming that the theorem holds for almost simple groups, we may assume that $b(H) < 9\log m$. Let $\{\gamma_1,\ldots,\gamma_b\} \subseteq \Gamma$ be a base for H with $b < 9\log m$. Set $\alpha_i = (\gamma_i,\ldots,\gamma_i) \in \Omega$, $1 \leqslant i \leqslant b$, and define $\beta_i \in \Omega$ by setting

$$\beta_1 = (\delta,\gamma,\ldots,\gamma),\ \beta_2 = (\gamma,\delta,\gamma,\ldots,\gamma),\ \ldots,\ \beta_{k-1} = (\gamma,\ldots,\gamma,\delta,\gamma)$$

where γ and δ are fixed distinct elements of Γ. Suppose $(h_1,\ldots,h_k)p^{-1}$ fixes each α_i. Then

$$(\gamma_i,\ldots,\gamma_i) = (\gamma_i,\ldots,\gamma_i)^{(h_1,\ldots,h_k)p^{-1}} = (\gamma_i^{h_{1p}},\ldots,\gamma_i^{h_{kp}})$$

and thus $\gamma_i^{h_j} = \gamma_i$ for each i, so $h_j = 1$ for each j. Finally, if $(1,\ldots,1)p^{-1}$ fixes β_i, then p fixes $i \in \{1,\ldots,k\}$, so we deduce that $\{\alpha_1,\ldots,\alpha_b,\beta_1,\ldots,\beta_{k-1}\}$ is a base for G. This gives

$$b(G) \leqslant b+k-1 < 9\log m + k - 1 < 9\log n.$$

Diagonal-type groups. Finally, let us eliminate diagonal-type groups. Define W and D as in (3.1), so

$$W = \{(a_1,\ldots,a_k)\pi \in \mathrm{Aut}(T) \wr S_k \mid \mathrm{Inn}(T)a_1 = \mathrm{Inn}(T)a_i \text{ for all } i\}$$
$$D = \{(a,\ldots,a)\pi \in \mathrm{Aut}(T) \wr S_k\} \cong \mathrm{Aut}(T) \times S_k$$

and let $G \leqslant W$ be a diagonal-type group. We will assume that $k \geqslant 3$ (the case $k = 2$ is similar). We may identify Ω with the set of right cosets W/D, in which case the action of G on Ω is given by

$$(D(a_1,\ldots,a_k)\pi)^{(b_1,\ldots,b_k)\sigma} = D(a_1b_{1\pi},\ldots,a_kb_{k\pi})\pi\sigma$$

(see (3.2)). Write $T = \langle x,y\rangle$ and define the following elements in Ω:

$$\alpha = D(1,\ldots,1),\ \beta_1 = D(x,1,\ldots,1),\ \ldots,\ \beta_k = D(1,\ldots,1,x)$$

and

$$\gamma_1 = D(y,1,\ldots,1),\ \ldots,\ \gamma_k = D(1,\ldots,1,y).$$

We claim that $\{\alpha,\beta_1,\ldots,\beta_k,\gamma_1,\ldots,\gamma_k\}$ is a base for G. Suppose $g = (b_1,\ldots,b_k)\sigma \in G$ fixes this set pointwise. Since g fixes α, we have

$$D(1,\ldots,1) = D(1,\ldots,1)^g = D(b_1,\ldots,b_k)\sigma$$

and thus $g = (b,\ldots,b)\sigma \in D$. If $\sigma = 1$ then

$$\beta_1 = \beta_1^g = D(xb,b,\ldots,b),\ \ \gamma_1 = \gamma_1^g = D(yb,b,\ldots,b),$$

so $(xbx^{-1},b,\ldots,b)$ and $(yby^{-1},b,\ldots,b)$ are in D and thus b centralises T, so $b = 1$ (by Proposition 2.4(i)) and $g = 1$. Finally, suppose $\sigma \neq 1$, say $1^\sigma \neq 1$ for example. Then $\beta_1 = \beta_1^g = D(xb,b,\ldots,b)\sigma$, so

$$(xb,b,\ldots,b)\sigma \cdot (x^{-1},1,\ldots,1) = (xb,b,\ldots,b,bx^{-1},b,\ldots,b)\sigma \in D$$

(here bx^{-1} is the j-th coordinate, where $j = 1^{\sigma^{-1}} \neq 1$) and thus $xb = b$, which is a contradiction. This justifies the claim, so

$$b(G) \leqslant 2k+1 < 9\log n$$

as required. □

Remark 5.9. The final statement in Liebeck's theorem is essentially best possible since there are primitive groups G with $b(G) = O(\sqrt{n})$. For example, if $G = S_m$ and Ω is the set of 2-subsets of $\{1,\ldots,m\}$ then $|\Omega| = \frac{1}{2}m(m-1) = n$ and we have already observed that $b(G) \approx \frac{2}{3}m = O(\sqrt{n})$. Also note that the estimate in (i) is also best possible (up to a small constant); for example, the standard action of $G = \mathrm{AGL}_d(2)$ has base size $b(G) = d+1 = \log n + 1$.

Of course, Liebeck's result holds for *any* primitive group, but it is possible to do better if we focus on specific families of primitive groups. For example, a striking theorem of Seress [82] states that $b(G) \leqslant 4$ for any soluble primitive group G (moreover, equality holds for infinitely many such G), and in the next section we will see that better bounds have been established for almost simple primitive groups.

To close this discussion, let us return to the bounds in (5.4). As noted in Examples 5.5, we can find transitive groups G such that $b(G)$ is close to either the upper or lower bound. However, one of the main open problems in this area asserts that if G is primitive, then $b(G)$ is 'small' in the following sense (see [80, p.207]):

Conjecture 5.10 (Pyber, 1993)**.** *There is an absolute constant c such that*

$$b(G) \leqslant c\frac{\log|G|}{\log n}$$

for any primitive group G of degree n.

Note that primitivity is essential. For instance, if we take $k = 2^m$ in Examples 5.5(ii) then $G = Z_2 \wr Z_k < S_{2k}$ is transitive and

$$b(G) = 2^m, \quad \frac{\log|G|}{\log n} = \frac{2^m + m}{m+1}.$$

The main approach to Pyber's conjecture has been via the O'Nan-Scott Theorem, and it has been verified for several families of primitive groups. We give a brief summary:

1. *Almost simple.* We will focus on bases for almost simple groups in the next section. The analysis of such groups can be partitioned into two cases; the so-called *standard* and *non-standard* groups (see Definition 5.14 below). Pyber's conjecture for non-standard groups was established by Liebeck and Shalev [69], using probabilistic methods (see Theorem 5.17); and the standard groups were handled by Benbenishty [7], who constructed explicit bases of an appropriate size.

2. *Diagonal-type.* Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive diagonal-type group of degree n, so

$$T^k \leqslant G \leqslant T^k.(\mathrm{Out}(T) \times P_G)$$

where $k \geqslant 2$, T is a nonabelian simple group, $n = |T|^{k-1}$ and $P_G \leqslant S_k$ is the group induced by the conjugation action of G on the k factors of T^k (recall that either P_G is primitive, or $k = 2$ and $P_G = 1$). Here the main result is a recent theorem of Fawcett [40]:

Theorem 5.11 (Fawcett, 2013)**.** *Pyber's conjecture holds for diagonal groups. More precisely,*

$$b(G) \leqslant \left\lceil \frac{\log|G|}{\log n} \right\rceil + 2$$

In fact, $b(G) = 2$ if $P_G \neq A_k, S_k$.

3. *Product-type and twisted wreath products.* It turns out that Pyber's conjecture for twisted wreath products quickly follows from the product-type case (basically, a twisted wreath product can be embedded in an appropriate product-type group).

   Let $G \leqslant H \wr P$ be a primitive product-type group on $\Omega = \Gamma^k$, where $H \leqslant \mathrm{Sym}(\Gamma)$ is primitive (almost simple or diagonal-type) with socle S, and $P \leqslant S_k$ is the transitive group induced by G on the k factors of $\mathrm{Soc}(G) = T^k$. Recall that the product action of G on Ω is given by

$$(\gamma_1, \ldots, \gamma_k)^{(h_1,\ldots,h_k)p^{-1}} = (\gamma_{1^p}^{h_{1^p}}, \ldots, \gamma_{k^p}^{h_{k^p}})$$

   Pyber's conjecture for product-type groups has recently been established in [26], and the following theorem is a key ingredient in the proof (see [26, Theorem 3.1], and recall that all logarithms are base-2):

   Theorem 5.12 (Burness & Seress, 2013)**.** *There exists an absolute constant c such that for any transitive group $P \leqslant \mathrm{Sym}(\Delta)$ of degree k, there exist η subsets of Δ such that*

$$\eta \leqslant c\left(1 + \frac{\log|P|}{k}\right)$$

   and the intersection of the setwise stabilisers of these subsets in P is trivial.

   This is essentially best possible, e.g. if $P = S_k$ then at least $\lceil \log k \rceil > \frac{1}{k}\log|P|$ subsets are required, e.g. if $k = 8$ take $\{1,2,3,4\}$, $\{1,2,5,6\}$ and $\{1,3,5,7\}$.

   The proof of Theorem 5.12 for primitive groups is relatively straightforward, using earlier work on so-called *distinguishing partitions* for permutation groups. The imprimitive case is more difficult and highly combinatorial, using colourings of an associated *structure tree* for P that encodes a chain of block systems for P.

   Let's briefly explain the relevance of Theorem 5.12, in the case where H is almost simple. Let $\{\gamma_1, \ldots, \gamma_b\} \subseteq \Gamma$ be a base for H with $b = b(H)$, and set $\alpha_i = (\gamma_i, \ldots, \gamma_i) \in \Omega = \Gamma^k$. If $g = (h_1, \ldots, h_k)p \in G$ fixes each α_i then each h_j fixes $\gamma_1, \ldots, \gamma_b$, so $g = (1, \ldots, 1)p$.

Since $P \leqslant S_k$ is transitive, let $X = \{X_1, \ldots, X_a\}$ be a set of subsets of $\Delta = \{1, \ldots, k\}$ provided by Theorem 5.12, where

$$a \leqslant c_1 \left(1 + \frac{\log |P|}{k}\right)$$

for some absolute constant c_1. Set $r = \lfloor \log |\Gamma| \rfloor$ and assume $a \geqslant r$ (for convenience). Let $Y_1 \cup \ldots \cup Y_s$ be the *common refinement* of the partitions $\{X_i \cup (\Delta \setminus X_i) \mid 1 \leqslant i \leqslant r\}$; this is an s-part partition of Δ, where $s \leqslant 2^r \leqslant |\Gamma|$. Choose distinct $\gamma_1, \ldots, \gamma_s \in \Gamma$ and define $\beta \in \Omega$ so that all the coordinates in β corresponding to points in Y_i are equal to γ_i. Now, if $g = (1, \ldots, 1)p \in G$ fixes β then p fixes each Y_j, so p fixes each X_i with $1 \leqslant i \leqslant r$. In this way, we can define a set of points $\{\beta_1, \ldots, \beta_{\lceil a/r \rceil}\}$ in Ω with the property that if $g = (1, \ldots, 1)p \in G$ fixes each β_i then p stabilises each subset in X, so $p = 1$.

We now have a base $\{\alpha_1, \ldots, \alpha_b, \beta_1, \ldots, \beta_{\lceil a/r \rceil}\}$ for G, where

$$a \leqslant c_1 \left(1 + \frac{\log |P|}{k}\right), \;\; r = \lfloor \log |\Gamma| \rfloor, \;\; b = b(H) \leqslant c_2 \frac{\log |H|}{\log |\Gamma|}$$

for absolute constants c_1, c_2 (since Pyber's conjecture holds for almost simple groups). Then

$$\begin{aligned} b(G) \leqslant \lceil a/r \rceil + b &\leqslant \left\lceil c_1 \frac{1}{\lfloor \log |\Gamma| \rfloor} + c_1 \frac{\log |P|}{k \lfloor \log |\Gamma| \rfloor} \right\rceil + c_2 \frac{\log |H|}{\log |\Gamma|} \\ &\leqslant c_3 \frac{\log |P|}{\log n} + c_4 \frac{\log |H|^k}{\log n} \\ &\leqslant c_5 \frac{\log |G|}{\log n} \end{aligned}$$

(Here we are using the fact that $|H| \leqslant |\mathrm{Aut}(S)| \leqslant |S|^2$ (H is almost simple with socle S), so $|G|^2 \geqslant |H|^k |P|$.)

4. *Affine-type.* Let $G = HV \leqslant \mathrm{AGL}(V)$ be a primitive affine-type group, where $V = (\mathbb{F}_p)^d$ and $H = G_0 \leqslant \mathrm{GL}(V)$ is irreducible. In this situation, Pyber's conjecture is still open, but several special cases have been settled:

	Conditions	Bound	Ref.
Seress, 1996	G soluble	$b(G) \leqslant 4$	[82]
Gluck & Magaard, 1998	$(p, \lvert H \rvert) = 1$	$b(G) \leqslant 95$	[49]
Halasi & Podoski, 2012	$(p, \lvert H \rvert) = 1$	$b(G) \leqslant 3$	[54]
Liebeck & Shalev, 2002	primitive	$b(G) \leqslant 18 \log \lvert H \rvert / n + c$	[70, 71]

Here the theorem of Liebeck and Shalev deals with all the affine-type primitive groups $G = HV$, where H acts primitively on V (as a linear group). In other words, H does not preserve a nontrivial direct sum decomposition of V.

Remark 5.13. To summarise, in order to complete the proof of Pyber's base size conjecture we may assume that $G = HV$ is an insoluble affine-type group, where p divides $|H|$, and H acts imprimitively as a linear group on V.

5.3 Almost simple groups & probabilistic methods

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive almost simple permutation group, with socle T and point stabiliser $H = G_\alpha$. As noted above, it is natural to partition the analysis of bases for such groups into two cases, according to the following definition:

Definition 5.14. We say that G is *standard* if one of the following holds:

(i) $T = A_m$ and Ω is an orbit of subsets or partitions of $\{1, \ldots, m\}$;

(ii) G is a classical group in a *subspace action*, i.e. Ω is an orbit of subspaces, or pairs of subspaces of complementary dimension, of the natural T-module.

Otherwise, G is *non-standard*.

In other words, G is standard if and only if $T = A_m$ and H is intransitive or imprimitive on $\{1,\dots,m\}$, or $T = Cl(V)$ is a classical group and H acts reducibly on V. In a meaningful sense, 'most' almost simple primitive groups are non-standard.

In general, if G is standard then H is a 'large' subgroup of G (a maximal parabolic subgroup, for example), which implies that $|G|$ is large compared to $|\Omega|$. Indeed, it is easy to see that the order of a standard group is not bounded above by a fixed polynomial function of its degree (in general). For example, if we take the standard action of $G = \mathrm{PGL}_n(q)$ then $|G| \sim q^{n^2-1}$ and $|\Omega| \sim q^{n-1}$. In view of (5.4), this implies that the base size of a standard group can be arbitrarily large (in the previous example, $b(G) = n+1$). Bases for standard groups have mainly been investigated using constructive methods; see [7, 8, 53, 57], for example.

For now on, let $G \leqslant \mathrm{Sym}(\Omega)$ be a non-standard group of degree n (with socle T and point stabiliser H as before). Our starting point is a theorem of Cameron, which states that there is an absolute constant c such that $|G| \leqslant n^c$ for any such group G. In particular, the order of a standard group *is* bounded above by a fixed polynomial of its degree. In [64], Liebeck shows that Cameron's theorem holds with $c = 9$, and this was later extended by Liebeck and Saxl, who showed that $c = 5$ (excluding $(G,n) = (\mathrm{M}_{23}, 23)$ and $(\mathrm{M}_{24}, 24)$). Given the existence of such a constant, Cameron made the following conjecture:

Conjecture 5.15 (Cameron, 1992)**.** *There is an absolute constant c such that $b(G) \leqslant c$ for any non-standard permutation group G.*

Shortly afterwards, an even stronger conjecture was formulated (see [33]):

Conjecture 5.16 (Cameron & Kantor, 1993)**.** *There is an absolute constant c such that if $G \leqslant \mathrm{Sym}(\Omega)$ is a non-standard permutation group then the probability that a randomly chosen c-tuple in Ω is a base for G tends to 1 as $|G|$ tends to infinity.*

This conjecture was proved by Liebeck and Shalev [69], using *probabilistic methods* (for alternating and symmetric groups, Cameron and Kantor showed that $c = 2$):

Theorem 5.17 (Liebeck & Shalev, 1999)**.** *The Cameron-Kantor Conjecture is true.*

In order to discuss the proof of this theorem, we need some additional notation. The *fixed point ratio* of $x \in G$, denoted by $\mathrm{fpr}(x)$, is the proportion of points in Ω that are fixed by x, i.e.

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

In other words, $\mathrm{fpr}(x)$ is the probability that a randomly chosen element of Ω is fixed by x.

The connection between fixed point ratios and base sizes arises as follows. For $c \in \mathbb{N}$, let $Q(G,c)$ be the probability that a randomly chosen c-tuple of points in Ω is *not* a base for G, so

$$b(G) \leqslant c \iff Q(G,c) < 1.$$

Of course, a c-tuple in Ω fails to be a base if and only if it is fixed by an element $x \in G$ of prime order, and we note that the probability that a random c-tuple is fixed by x is at most $\mathrm{fpr}(x)^c$. Let $\mathscr{P}$ be the set of elements of prime order in G, and let $x_1,\dots,x_k$ be a set of representatives for the distinct G-classes of elements in $\mathscr{P}$. Fixed point ratios are constant on conjugacy classes, so

$$Q(G,c) \leqslant \sum_{x \in \mathscr{P}} \mathrm{fpr}(x)^c = \sum_{i=1}^{k} |x_i^G| \cdot \mathrm{fpr}(x_i)^c =: \widehat{Q}(G,c). \tag{5.5}$$

In particular, we can use upper bounds on fixed point ratios to bound $\widehat{Q}(G,c)$ from above.

Example 5.18. We claim that $b(G) \leqslant 500$ if T is an exceptional group of Lie type over $\mathbb{F}_q$. To see this, we use a very general theorem of Liebeck and Saxl [68], which implies that $\mathrm{fpr}(x) \leqslant 4/3q$ for all non-identity elements $x \in G$. Now $|G| \leqslant |\mathrm{Aut}(E_8(q))| < q^{249}$ and thus

$$Q(G,500) \leqslant \widehat{Q}(G,500) \leqslant \left(\frac{4}{3q}\right)^{500} \sum_{i=1}^{k} |x_i^G| < \left(\frac{4}{3q}\right)^{500} |G| < \left(\frac{4}{3q}\right)^{500} q^{249} < q^{-1}.$$

The claim follows. (In fact, this very crude approximation shows that $b(G) \leqslant 426$.)

To deal with non-standard classical groups of arbitrarily large rank, we need a better upper bound on $\mathrm{fpr}(x)$. Indeed, the key ingredient is [69, Theorem $(\star)$], which states that there is an absolute constant $\varepsilon > 0$ such that

$$\mathrm{fpr}(x) < |x^G|^{-\varepsilon} \tag{5.6}$$

for any non-identity element $x \in G$ in any non-standard classical group G (the proof involves a detailed analysis of the maximal subgroups of the finite classical groups, following Aschbacher's subgroup structure theorem [2]). Note that the non-standard condition is essential. For example, in the standard action of $G = \mathrm{PGL}_n(q)$ we have $\mathrm{fpr}(x) \approx q^{-1}$ and $|x^G| \approx q^{2n-2}$ for $x = \mathrm{diag}(\lambda, 1, \ldots, 1) \in G$ (modulo scalars).

Write $T = Cl_n(q)$ (e.g. $\mathrm{PSL}_n(q)$, $\mathrm{PSp}_n(q)$ etc.). In order to apply the above bound (5.6), we need two basic facts:

1. G has at most q^{4n} conjugacy classes of elements of prime order.
2. $|x^G| \geqslant q^{n/2}$ for all $x \in G$ of prime order.

Set $c = \lceil 11/\varepsilon \rceil$. Then

$$\widehat{Q}(G,c) = \sum_{i=1}^{k} |x_i^G| \cdot \mathrm{fpr}(x_i)^c < \sum_{i=1}^{k} |x_i^G|^{-10} \leqslant k \cdot (q^{n/2})^{-10} \leqslant q^{-n}$$

and thus $Q(G,c) \to 0$ as $|G| \to \infty$, which completes the proof of the Cameron-Kantor Conjecture.

The proof of Theorem 5.17 yields an undetermined constant $c = \lceil 11/\varepsilon \rceil$. This led Cameron to make the following conjecture (see [30, p.122]), which suggests a remarkable dichotomy for almost simple primitive groups: either the base size can be arbitrarily large (standard groups), or there exists an extremely small base (non-standard groups).

Conjecture 5.19 (Cameron, 1999)**.** *Let G be a non-standard permutation group. Then $b(G) \leqslant 7$, with equality if and only if $G = \mathrm{M}_{24}$ in its natural action on 24 points.*

This conjecture is proved in a sequence of papers [16, 19, 22, 23], using similar probabilistic methods. In fact, we prove a slightly stronger result:

Theorem 5.20 (Burness et al., 2007–2011)**.** *Cameron's Conjecture is true. Moreover, if $G \leqslant \mathrm{Sym}(\Omega)$ is non-standard then the probability that a random 6-tuple in Ω forms a base for G tends to 1 as $|G|$ tends to infinity.*

One of the key ingredients in the proof for classical groups is an explicit version of (5.6), which roughly states that $\varepsilon \approx 1/2$ is optimal. In order to use this, write $T = Cl_n(q)$ and for $t \in \mathbb{R}$, set

$$\eta_G(t) = \sum_{i=1}^{k} |x_i^G|^{-t},$$

where the x_i represent the distinct G-classes of elements of prime order in G. If $n > 6$, then careful calculation reveals that $\eta_G(1/3) < 1$. Therefore, by combining this with the upper bound $\mathrm{fpr}(x) < |x^G|^{-1/2+1/n}$, we deduce that

$$\widehat{Q}(G,4) < \sum_{i=1}^{k} |x_i^G|^{1+4(-\frac{1}{2}+\frac{1}{n})} \leqslant \eta_G(1/3) < 1$$

if $n > 6$, and thus $b(G) \leqslant 4$. In this way, we obtain the following result for non-standard classical groups (see [16, Theorem 1]):

Theorem 5.21 (Burness, 2007)**.** *Let G be a non-standard classical group. Then either $b(G) \leqslant 4$, or $G = \mathrm{PSU}_6(2).2$, $H = \mathrm{PSU}_4(3).2^2$ and $b(G) = 5$.*

Remark 5.22. Some additional comments on bases for almost simple groups:

(i) If T is an alternating or sporadic group, then the exact value of $b(G)$ has been calculated in all cases. For example, if $T = A_n$ then [19, Theorem 1.1] implies that $b(G) = 2$ if $n > 12$ (if $G = A_{12}$ and $G_\alpha = \mathrm{M}_{12}$, then $b(G) = 3$). For symmetric and alternating groups, the proof uses Maróti's

upper bound on $|H|$ in Theorem 3.18, together with a theorem of Guralnick and Magaard [49] on the *minimal degree* of H (see Section 3.4.3), which translates into a lower bound on $|x^G|$ for non-identity elements $x \in H$. This is useful, because $\widehat{Q}(G,2) < |H|^2 \max_{1\neq x\in H} |x^G|^{-1}$. The proof for sporadic groups relies heavily on computational methods.

(ii) The proof of Theorem 5.20 reveals that there are infinitely many exceptional groups with $b(G) \geqslant 5$, and very recently it has been shown that there are also infinitely many with $b(G) = 6$ (see [21, Theorem 11]).

(iii) One of the ultimate aims is to compute the exact value of $b(G)$ for all non-standard groups. This is an ongoing project of Burness, Guralnick and Saxl (see [20], for example). There is particular interest in the special case $b(G) = 2$.

More generally, one might hope to classify all the primitive permutation groups with $b(G) = 2$. Here the affine groups are particularly interesting; if $G = HV$ is an affine group, then $b(G) = 2$ if and only if the irreducible group $H \leqslant \mathrm{GL}(V)$ has a regular orbit on V. Determining the linear groups H with this property is a basic problem in the representation theory of finite groups.

5.4 Bases for algebraic groups

Up to now, we have only considered bases in the context of finite permutation groups. In this final section, we briefly report on recent work of Burness, Guralnick and Saxl [21], which extends the study of bases to simple algebraic groups over algebraically closed fields. In some situations, by taking the fixed points of a suitable Frobenius morphism, we can use results on bases for algebraic groups to shed light on bases for the corresponding finite groups of Lie type.

Let G be a simple affine algebraic group over an algebraically closed field K of characteristic $p \geqslant 0$, e.g. $\mathrm{SL}_n(K)$, $\mathrm{Sp}_n(K)$, $E_8(K)$, etc. Consider the natural action of G on the primitive coset variety $\Omega = G/H$, where H is a closed maximal subgroup of G (here H is closed with respect to the *Zariski topology* on G). We define three base-related measures that arise naturally in this context:

(i) As before, the *exact base size*, denoted $b(G)$, is the smallest integer c such that Ω contains c points with trivial pointwise stabiliser.

(ii) The *connected base size*, denoted $b^0(G)$, is the smallest integer c such that Ω contains c points whose pointwise stabiliser is finite.

(iii) The *generic base size*, denoted $b^1(G)$, is the smallest integer c such that the product variety $\Omega^c = \Omega \times \cdots \times \Omega$ (c factors) contains a non-empty open subvariety Λ and every c-tuple in Λ is a base for G.

Evidently, we have

$$b^0(G) \leqslant b(G) \leqslant b^1(G).$$

In [21], these base-related measures are calculated for all primitive actions of any simple algebraic group G, with the precise values computed in almost all cases. For example, the next result can be viewed as a sharpened algebraic group analogue of Theorem 5.20 (here P_i denotes the maximal parabolic subgroup of G that corresponds to deleting the i-th node in the Dynkin diagram of G):

Theorem 5.23. *Let G be a simple algebraic group over an algebraically closed field and let Ω be a primitive G-variety with point stabiliser H. Assume G is not a classical group in a subspace action. Then $b^1(G) \leqslant 6$, with equality if and only if $(G,H) = (E_7,P_7)$, (E_6,P_1) or (E_6,P_6).*

As an example of the detailed results obtained in [19], we record the following theorem for non-subspace actions of classical algebraic groups:

Theorem 5.24. *Let G be a simple classical algebraic group in a primitive non-subspace action with point stabiliser H. Assume $p \neq 2$. Then either $b^0(G) = b(G) = b^1(G) = 2$, or one of the following holds:*

(i) $b^0(G) = b(G) = b^1(G) = b > 2$ *and (G,H,b) is recorded in Table 5.1;*

G	Type of H	Conditions	b
SL_n	$\mathrm{GL}_{n/2} \wr S_2$	$n \geqslant 4$	3
	Sp_n	$n = 6$	4
	Sp_n	$n \geqslant 8$	3
Sp_n	$\mathrm{Sp}_{n/2} \wr S_2$	$n \geqslant 8$	3
	$\mathrm{Sp}_{n/3} \wr S_3$	$n = 6$	3
SO_n	$\mathrm{GL}_{n/2}$	$n \geqslant 10$	3
	G_2	$n = 7$	4

Table 5.1: Values of b in Theorem 5.24(i)

(ii) $b^0(G) = b(G) = 2$, $b^1(G) = 3$ *and*

$$(G,H) = (\mathrm{SL}_2, \mathrm{GL}_1 \wr S_2),\ (\mathrm{SL}_n, \mathrm{SO}_n),\ (\mathrm{Sp}_n, \mathrm{GL}_{n/2}) \text{ or } (\mathrm{SO}_n, \mathrm{O}_{n/2} \wr S_2).$$

Let $c \geqslant 2$ be an integer. The expression

$$\mathscr{Q}(G,c) = \frac{c}{c-1} \cdot \sup_{x \in \mathscr{P}} \left\{ \frac{\dim(x^G \cap H)}{\dim x^G} \right\}$$

plays an important role in the proofs of the main results in [19], where $\mathscr{P}$ denotes the set of elements of prime order in H (including all nontrivial unipotent elements if $p = 0$). Indeed, a key theorem states that if H^0 is reductive, then

$$\mathscr{Q}(G,c) < 1 \implies b^1(G) \leqslant c.$$

This is an algebraic group analogue of the implication $\widehat{Q}(G,c) < 1 \implies b(G) \leqslant c$ for finite permutation groups. Similarly, the lower bound

$$b^0(G) \geqslant \frac{\dim G}{\dim \Omega} = \frac{\dim G}{\dim G - \dim H}$$

is the analogue of the lower bound in (5.4). We also show that $b^1(G) \leqslant b^0(G) + 1$.

Finally, let's comment on the connection between bases for algebraic groups and the corresponding finite groups. Let p be a prime, let G be a simple algebraic group over the algebraic closure $\overline{\mathbb{F}}_p$, and let σ be a Frobenius morphism of G such that the set of fixed points G_σ is a finite group of Lie type over $\mathbb{F}_q$, for some p-power q. If H is a closed positive-dimensional σ-stable subgroup of G then we can consider the action of G_σ on the set of cosets of H_σ in G_σ. We write $b(G_\sigma)$ for the base size of G_σ in this action. In addition, for a positive integer c, let $P(G_\sigma, c)$ be the probability that c randomly chosen points in G_σ/H_σ form a base for G_σ. We define the *asymptotic base size* of G_σ, denoted by $b^\infty(G_\sigma)$, to be the smallest value of c such that $P(G_\sigma, c)$ tends to 1 as q tends to infinity.

In [19], various relations between the base-related measures

$$b(G),\ b^0(G),\ b^1(G),\ b(G_\sigma),\ b^\infty(G_\sigma)$$

are investigated. For example, a straightforward application of the Lang-Weil estimates in algebraic geometry shows that $b^1(G) = b^\infty(G)$, and we also establish the bound $b^0(G) \leqslant b(G_\sigma)$ if $q > 2$. In future work, one of the main aims is to use the results in [19] to determine the precise base size of any almost simple primitive group of Lie type.

6 Exercises

Unless stated otherwise, $G \leqslant \mathrm{Sym}(\Omega)$ is a permutation group on a finite set Ω, and $\alpha \in \Omega$.

1. Let G be a transitive abelian permutation group. Prove that G is regular.
2. Let K be a subgroup of a transitive group G. Prove that $G = G_\alpha K$ if and only if K is transitive.
3. Prove that the rank of a transitive group G is well defined (i.e. it is independent of the choice of α).
4. Let G be a finite group acting on a set Ω, and let k be the number of orbits of G. Prove the *Orbit-Counting Lemma*, that is, show that
$$\frac{1}{|G|}\sum_{x\in G}|C_\Omega(x)| = k.$$
5. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group of degree $n \geqslant 3$ and suppose $x, y \in G$ are elements such that $\mathrm{supp}(x) \cap \mathrm{supp}(y) = \{\alpha\}$. Show that the commutator $[x, y]$ is a 3-cycle.
6. Here we consider the transitivity of the standard actions of $\mathrm{PSL}_2(q)$ and $\mathrm{PGL}_2(q)$.
   (i) Prove that the standard action of $\mathrm{PSL}_2(q)$ is 2-transitive, and 3-transitive if and only if q is even.
   (ii) Prove that the standard action of $\mathrm{PGL}_2(q)$ is 3-transitive, and 4-transitive if and only if $q = 3$.
7. Let $G = \mathrm{AGL}_d(p)$, where $d \geqslant 2$. Prove that the standard action of G is 3-transitive if and only if $p = 2$, and 4-transitive if and only if $(d, p) = (2, 2)$.
8. Let G and H be permutation groups on a set Ω. Prove that G and H are permutation isomorphic if and only if G and H are conjugate as subgroups of $\mathrm{Sym}(\Omega)$.
9. Let $H \leqslant \mathrm{Sym}(\Gamma)$ and $K \leqslant \mathrm{Sym}(\Delta)$ be transitive groups. Suppose there is an isomorphism $\psi : H \to K$ such that $H_\gamma \psi = K_\delta$ for some $\gamma \in \Gamma$, $\delta \in \Delta$. Prove that H and K are permutation isomorphic.
10. Let $H \leqslant \mathrm{Sym}(\Gamma)$ and $K \leqslant \mathrm{Sym}(\Delta)$ be permutation groups, where $|\Gamma|, |\Delta| \geqslant 2$ and $\Delta = \{1, \ldots, n\}$. Prove that the standard and product actions of $H \wr K$ are faithful.
11. Let G be a finite group. Prove that $\{(g, g) \mid g \in G\}$ is a maximal subgroup of $G \times G$ if and only if G is simple.
12. If $G \leqslant \mathrm{Sym}(\Omega)$ is transitive, prove that G is primitive if and only if G_α is a maximal subgroup of G. Deduce that if $m > 4$ then S_m acts primitively on the set of 2-element subsets of $\{1, \ldots, m\}$.
13. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a diagonal-type group. Prove that G is not 2-transitive.
14. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group and consider the natural coordinatewise action of G on $\Omega \times \Omega$. Let Δ be an orbit of G in this induced action; the *diagonal* orbit is $\{(\alpha, \alpha) \mid \alpha \in \Omega\}$. The *orbital graph* of Δ is the digraph with vertex set Ω and an edge from α to β for each $(\alpha, \beta) \in \Delta$. Prove that G is primitive on Ω if and only if all non-diagonal orbital graphs are connected.
15. Prove that if $G \leqslant \mathrm{Sym}(\Omega)$ is primitive and $\alpha, \beta \in \Omega$ are distinct points, then either $G = \langle G_\alpha, G_\beta \rangle$, or G is regular of prime degree.
16. Prove that there are precisely 68 diagonal-type primitive groups of degree less than 4096.
17. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive permutation group of degree n containing a 2-cycle. Prove that $G = S_n$.
18. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive permutation group of degree n containing a 3-cycle. Define a relation $\sim$ on Ω as follows:
$$\alpha \sim \beta \iff \alpha = \beta, \text{ or there exists a 3-cycle } (\alpha, \beta, \gamma) \in G$$
Prove that $\sim$ is a G-congruence, and deduce that $G = A_n$ or S_n.

19. Prove that the action of S_n on the set of k-element subsets of $\{1,\ldots,n\}$ (with $k \leqslant n/2$) is $\frac{3}{2}$-transitive if and only if $(n,k) = (7,2)$.

20. As in Section 3.4.2, let

$$E = \{n \in \mathbb{N} \mid \text{there exists a primitive group of degree } n, \text{ other than } S_n \text{ or } A_n\}.$$

Show that $E \cap \{1,\ldots,10\} = \{5,6,7,8,9,10\}$.

21. Let G be a sharply 2-transitive group of degree $n \geqslant 2$. Prove that $\delta(G) = \frac{1}{n}$. Also prove that any two derangements in G are conjugate.

22. Let $d_n = |\Delta(S_n)|$ be the number of derangements in S_n (with respect to the standard action of S_n on $\{1,\ldots,n\}$, $n \geqslant 2$). Without using Montmort's formula, prove that

$$d_n = (n-1)(d_{n-1} + d_{n-2})$$

and use this to derive the recurrence relation

$$d_n = nd_{n-1} + (-1)^n.$$

Use this to give an alternative proof of Montmort's formula for d_n.

23. Prove that $\delta(S_n) - \delta(A_n) = \frac{(-1)^n(n-1)}{n!}$ with respect to the standard actions on $\{1,\ldots,n\}$.

24. Compute $\delta(G)$ for the standard action of $G = \mathrm{PSL}_2(q)$. (*Hint.* By the Fundamental Theorem of Projective Geometry, no nontrivial element of G fixes three or more points.)

25. Let G be a transitive permutation group of degree $n \geqslant 2$ with a regular insoluble normal subgroup N. Prove that $\delta(G) \geqslant 1/2$. (*Hint.* If N is a finite insoluble group and $\varphi \in \mathrm{Aut}(N)$, then $C_N(\varphi) \neq 1$.) In particular, this implies that $\delta(G) \geqslant 1/2$ if G is a twisted wreath product.

26. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive group of degree mp, where p is a prime and $m < p$. Prove that G is non-elusive.

27. Give an example to show that the primitivity of G is essential in Thompson's problem on the transitivity of $\Delta(G)$.

28. Let G be an almost simple primitive group of degree n with socle $T = A_m$ and point stabiliser H. Suppose H acts primitively on $\{1,\ldots,m\}$. Use Bochert's theorem to prove that $|G| < n^4$ (cf. proof of Theorem 5.8).

29. Let $H \leqslant \mathrm{Sym}(\Gamma)$ and $K \leqslant \mathrm{Sym}(\Delta)$ be permutation groups, where Γ and Δ are disjoint finite sets.

    (i) For the natural action of $H \times K$ on $\Gamma \cup \Delta$, prove that $b(H \times K) = b(H) + b(K)$.

    (ii) For the natural action of $H \times K$ on $\Gamma \times \Delta$, prove that $b(H \times K) = \max\{b(H), b(K)\}$.

    (iii) For the standard action of $H \wr K$ on $\Gamma \times \Delta$, prove that $b(H \wr K) = |\Delta| \cdot b(H)$.

30. Find a base of size m for the product action of $S_m \wr S_k$ on $\{1,\ldots,m\}^k$, where $k \leqslant m$. Is this the minimal size of a base?

31. Consider the action of $G = S_m$ on the set of k-element subsets of $\{1,\ldots,m\}$. Prove that $\mu(G) = 2\binom{m-2}{k-1}$ (where $\mu(G)$ denotes the *minimal degree* of G; see Section 3.4.3). Similarly, show that $\mu(G) = 2m^{k-1}$ for the product action of $G = S_m \wr S_k$ on $\{1,\ldots,m\}^k$.

32. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group of degree n. Prove that $b(G)\mu(G) \geqslant n$.

7 References

[1] V. Arvind, *The parameterized complexity of fixpoint free elements and bases in permutation groups*, in Parameterized and Exact Computation (eds. G. Gutin and S. Szeider), Lecture Notes in Computer Science, vol. 8246, Springer, pp.4–5, 2013.

[2] M. Aschbacher, *On the maximal subgroups of the finite classical groups*, Invent. Math. **76** (1984), 469–514.

[3] L. Babai, *On the order of doubly transitive permutation groups*, Invent. Math. **65** (1982), 473–484.

[4] L. Babai, *On the order of uniprimitive permutation groups*, Annals of Math. **113** (1981), 553–568.

[5] R.F. Bailey and P.J. Cameron, *Base size, metric dimension and other invariants of groups and graphs*, Bull. London Math. Soc. **43** (2011), 209–242.

[6] J. Bamberg, M. Giudici, M.W. Liebeck, C.E. Praeger and J. Saxl, *The classification of almost simple $\frac{3}{2}$-transitive groups*, Trans. Amer. Math. Soc. **365** (2013), 4257–4311.

[7] C. Benbenishty, *On actions of primitive groups*, PhD thesis, The Hebrew University of Jerusalem, 2005.

[8] C. Benbenishty, J.A. Cohen and A.C. Niemeyer, *The minimum length of a base for the symmetric group acting on partitions*, European J. Comb. **28** (2007), 1575–1581.

[9] K.D. Blaha, *Minimum bases for permutation groups: the greedy approximation*, J. Algorithms **13** (1992), 297–306.

[10] A. Bochert, *Über die Zahl verschiedener Werte, die eine Funktion gegebener Buchstaben durch Vertauschung derselben erlangen kann*, Math. Ann. **33** (1889), 584–590.

[11] N. Boston, W. Dabrowski, T. Foguel, P.J. Gies, J. Leavitt and D.T. Ose, *The proportion of fixed-point-free elements of a transitive permutation group*, Comm. Algebra **21** (1993), 3259–3275.

[12] J.N. Bray, D.F. Holt and C.M. Roney-Dougal, *The Maximal Subgroups of the Low-dimensional Finite Classical Groups*, London Math. Soc. Lecture Note Series, vol. 407, Cambridge University Press, 2013.

[13] J.R. Britnell and A. Maróti, *Normal coverings of linear groups*, Algebra Number Theory **7** (2013), 2085–2102.

[14] D. Bubboloni, C.E. Praeger and P. Spiga, *Normal coverings and pairwise generation of finite alternating and symmetric groups*, J. Algebra **390** (2013), 199–215.

[15] J.P. Buhler, H.W. Lenstra Jr. and C. Pomerance, *Factoring integers with the number field sieve*, Lecture Notes in Math., vol. 1554, Springer-Berlin (1993), 50–94.

[16] T.C. Burness, *On base sizes for actions of finite classical groups*, J. London Math. Soc. **75** (2007), 545–562.

[17] T.C. Burness and M. Giudici, *Classical groups, derangements and primes*, to appear in the Lecture Notes Series of the Aust. Math. Soc., Cambridge University Press.

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

[19] T.C. Burness, R.M. Guralnick and J. Saxl, *On base sizes for symmetric groups*, Bull. London Math. Soc. **43** (2011), 386–391.

[20] T.C. Burness, R.M. Guralnick and J. Saxl, *Base sizes for $\mathscr{S}$-actions of finite classical groups*, Israel J. Math. **199** (2014), 711–756.

[21] T.C. Burness, R.M. Guralnick and J. Saxl, *On base sizes for algebraic groups*, preprint (arXiv:1310.1569)

[22] T.C. Burness, M.W. Liebeck and A. Shalev, *Base sizes for simple groups and a conjecture of Cameron*, Proc. London Math. Soc. **98** (2009), 116–162.

[23] T.C. Burness and E.A. O'Brien and R.A. Wilson, *Base sizes for sporadic simple groups*, Israel J. Math. **177** (2010), 307–334.

[24] T.C. Burness, C.E. Praeger and Á. Seress, *Extremely primitive classical groups*, J. Pure Appl. Algebra **216** (2012), 1580–1610.

[25] T.C. Burness, C.E. Praeger and Á. Seress, *Extremely primitive sporadic and alternating groups*, Bull. London Math. Soc. **44** (2012), 1147–1154.

[26] T.C. Burness and Á. Seress, *On Pyber's base size conjecture*, Trans. Amer. Math. Soc., to appear (arXiv:1309.5584)

[27] T.C. Burness and H.P. Tong-Viet, *Derangements in primitive permutation groups, with an application to character theory*, Q. J. Math., to appear (arXiv:1403.7666)

[28] P.J. Cameron, *Finite permutation groups and finite simple groups*, Bull. London Math. Soc. **13** (1981), 1–22.

[29] P.J. Cameron (ed.), *Problems from the Fifteenth British Combinatorial Conference*, Discrete Math. **167/168** (1997), 605–615.

[30] P.J. Cameron, *Permutation Groups*, London Math. Soc. Student Texts **45**, Cambridge University Press, 1999.

[31] P.J. Cameron and A.M. Cohen, *On the number of fixed point free elements in a permutation group*, Discrete Math. **106/107** (1992), 135–138.

[32] 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.

[33] P.J. Cameron and W.M. Kantor, *Random permutations: some group-theoretic aspects*, Combin. Probab. Comput. **2** (1993), 257–262.

[34] P.J. Cameron, P.M. Neumann and D.N. Teague, *On the degrees of primitive permutation groups*, Math. Z. **180** (1982), 141–149.

[35] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, and R.A. Wilson, *Atlas of finite groups*, Oxford University Press, 1985.

[36] H.J. Coutts, M. Quick and C.M. Roney-Dougal, *The primitive permutation groups of degree less than* 4096, Comm. Algebra **39** (2011), 3526–3546.

[37] P. Diaconis, J. Fulman and R.M. Guralnick, *On fixed points of permutations*, J. Alg. Combin. **28** (2008), 189–218.

[38] J.D. Dixon and B. Mortimer, *Permutation Groups*, Springer-Verlag, New York, 1996.

[39] J.M. Fawcett, *The O'Nan-Scott theorem for finite primitive permutation groups, and finite representability*, Masters thesis, University of Waterloo, 2009.

[40] J.M. Fawcett, *The base size of a primitive diagonal group*, J. Algebra **375** (2013), 302–321.

[41] B. Fein, W.M. Kantor and M. Schacher, *Relative Brauer groups II*, J. Reine Angew. Math. **328** (1981), 39–57.

[42] J. Fulman and R.M. Guralnick, *Derangements in finite classical groups for actions related to extension field and imprimitive subgroups*, in preparation.

[43] J. Fulman and R.M. Guralnick, *Derangements in subspace actions of finite classical groups*, preprint (arxiv:1303.5480).

[44] 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.

[45] J. Fulman and R.M. Guralnick, *Derangements in simple and primitive groups*, in Groups, Combinatorics & Geometry (Durham, 2001), World Sci. Publ., River Edge, NJ (2003), 99–121.

[46] M. Giudici, *Quasiprimitive groups with no fixed point free elements of prime order*, J. London Math. Soc. **67** (2003), 73–84.

[47] M. Giudici and S. Kelly, *Characterizing a family of elusive permutation groups*, J. Group Theory **12** (2009), 95–105.

[48] M. Giudici, M.W. Liebeck, C.E. Praeger, J. Saxl and P.H. Tiep, *Arithmetic results on orbits of linear groups*, Trans. Amer. Math. Soc., to appear (arXiv:1203.2457)

[49] D. Gluck and K. Magaard, *Base sizes and regular orbits for coprime affine permutation groups*, J. London Math. Soc. **58** (1998), 603–618.

[50] S. Guest, J. Morris, C.E. Praeger and P. Spiga, *On the maximum orders of elements of finite almost simple groups and primitive permutation groups*, Trans. Amer. Math. Soc., to appear (arXiv:1301.5166)

[51] S. Guest, J. Morris, C.E. Praeger and P. Spiga, *Finite primitive permutation groups containing a permutation having at most four cycles*, preprint (arXiv:1307.6881)

[52] R.M. Guralnick and D. Wan, *Bounds for fixed point free elements in a transitive group and applications to curves over finite fields*, Israel J. Math. **101** (1997), 255–287.

[53] Z. Halasi, *On the base size for the symmetric group acting on subsets*, Studia Sci. Math. Hungar. **49** (2012), 492–500.

[54] Z. Halasi and K. Podoski, *Every comprime linear group admits a base of size two*, preprint (arXiv:1212.0199)

[55] D.R. Heath-Brown, C.E. Praeger and A. Shalev, *Permutation groups, simple groups, and sieve methods*, Israel J. Math. **148** (2005), 347–375.

[56] C. Hering, *Transitive linear groups and linear groups which contain irreducible subgroups of prime order, II*, J. Algebra **93** (1985), 151–164.

[57] J.P. James, *Partition actions of symmetric groups and regular bipartite graphs*, Bull. London Math. Soc. **38** (2006), 224–232.

[58] G.A. Jones, *Primitive permutation groups containing a cycle*, Bull. Aust. Math. Soc. **89** (2014), 159–165.

[59] C. Jordan, *Recherches sur les substitutions*, J. Math. Pures Appl. (Liouville) **17** (1872), 351–367.

[60] C. Jordan, *Sur l'énumeration des groupes primitifs pour les dix-sept premiers degrés*, C.R. Acad. Sci. Paris **75** (1872), 1754–1757.

[61] C. Jordan, *Sur la limite de transitivité des groupes non-alternées*, Bull. Soc. Math. France **1** (1873), 40–71.

[62] E.I. Khukhro and V.D. Mazurov (eds.), *The Kourovka Notebook: Unsolved Problems in Group Theory (18th edition)*, Institute of Mathematics, Novosibirsk, 2014.

[63] P.B. Kleidman and M.W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Series, vol. 129, Cambridge University Press, 1990.

[64] M.W. Liebeck, *On minimal degrees and base sizes of primitive permutation groups*, Arch. Math. **43** (1984), 11–15.

[65] M.W. Liebeck, *The affine permutation groups of rank three*, Proc. London Math. Soc. **54** (1987), 477–516.

[66] 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.

[67] M.W. Liebeck, C.E. Praeger and J. Saxl, *Transitive subgroups of primitive permutation groups*, J. Algebra **234** (2000), 291–361.

[68] M.W. Liebeck and J. Saxl, *Minimal degrees of primitive permutation groups, with an application to monodromy groups of coverings of Riemann surfaces*, Proc. London Math. Soc. **63** (1991), 266–314.

[69] M.W. Liebeck and A. Shalev, *Simple groups, permutation groups, and probability*, J. Amer. Math. Soc. **12** (1999), 497–520.

[70] M.W. Liebeck and A. Shalev, *Bases of primitive linear groups*, J. Algebra **252** (2002), 95–113.

[71] M.W. Liebeck and A. Shalev, *Bases of primitive linear groups, II*, J. Algebra **403** (2014), 223–228.

[72] G. Malle, G. Navarro and J.B. Olsson, *Zeros of characters of finite groups*, J. Group Theory **3** (2000), 353–368.

[73] A. Mann, C.E. Praeger and Á. Seress, *Extremely primitive groups*, Groups Geom. Dyn. **1** (2007), 623–660.

[74] A. Maróti, *On the order of primitive groups*, J. Algebra **258** (2002), 631–640.

[75] D. Marušič, *On vertex symmetric digraphs*, Discrete Math. **36** (1981), 69–81.

[76] P.R. de Montmort, *Essay d'analyse sur les jeux de hazard*, Quillau, Paris, 1708.

[77] P. Müller, *Permutation groups with a cyclic two-orbits subgroup and monodromy groups of Laurent polynomials*, Ann. Scuola Norm. Sup. Pisa **12** (2013), 369–438.

[78] 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.

[79] C.E. Praeger and J. Saxl, *On the order of primitive permutation groups*, Bull. London Math. Soc. **12** (1980), 303–307.

[80] L. Pyber, *Asymptotic results for permutation groups*, in Groups and Computation (eds. L. Finkelstein and W. Kantor), DIMACS Series, vol. 11, pp.197–219, 1993.

[81] L.L. Scott, *Representations in characteristic p*, The Santa Cruz Conference on Finite Groups, Proceedings of Symposia in Pure Mathematics, vol. 37, pp.319–331, 1980.

[82] Á. Seress, *The minimal base size of primitive solvable permutation groups*, J. London Math. Soc. **53** (1996), 243–255.

[83] Á. Seress, *Permutation Group Algorithms*, Cambridge Tracts in Mathematics **152**, Cambridge University Press, 2003.

[84] J.-P. Serre, *On a theorem of Jordan*, Bull. Amer. Math. Soc. **40** (2003), 429–440.

[85] C.C. Sims, *Computation with permutation groups*, Proc. Second Sympos. on Symbolic and Algebraic Manipulation, (ACM, New York), pp.23–28, 1971.

[86] H. Wielandt, *Finite permutation groups*, Academic Press, New York, 1964.