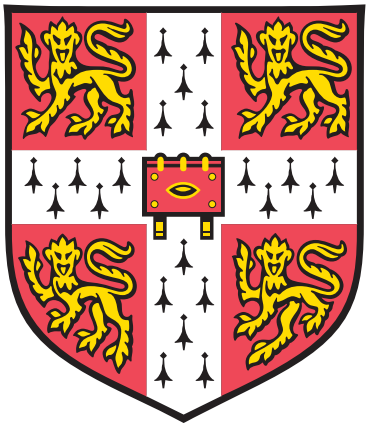
Bases of primitive permutation groups

by

Joanna B. Fawcett

St John's College
&
Department of Pure Mathematics
and Mathematical Statistics

University of Cambridge



A dissertation submitted
for the degree of
Doctor of Philosophy

To Mum and Dad

This dissertation is the result of my own work and includes nothing which is the outcome of work done in collaboration except where specifically indicated in the text.

All collaborative work was done with Eamonn O'Brien and Jan Saxl and is contained within Chapters 6 and 8. More specifically, the joint work consists of Theorem 8.0.1 and the original material in Sections 6.3, 8.2 and 8.4.

Abstract

A base B for a finite permutation group G acting on a set Ω is a subset of Ω with the property that only the identity of G can fix every element of B. In this dissertation, we investigate some properties of bases of several classes of primitive permutation groups including groups of diagonal type, twisted wreath type, and certain groups of affine type. In particular, we focus on determining when these groups possess a base of size 2.

To begin, we prove that a group G of diagonal type has a base of size 2 unless the top group of G is the symmetric or alternating group acting naturally, in which case the minimal base size of G is determined up to two possible values. In particular, we find that it can be unbounded. The minimal base size is also shown to satisfy a well-known conjecture of Pyber. Moreover, it is proved that if the top group of G does not contain the alternating group, then the proportion of pairs of points that are bases for G tends to 1 as $|G|$ tends to infinity. Some similar results are also proved.

Likewise, we prove that a group G of twisted wreath type has a base of size 2 when the top group of G is primitive, and for such groups G, we also prove that the proportion of pairs of points that are bases for G tends to 1 as $|G|$ tends to infinity. Otherwise, the top group of G is imprimitive, and it is shown that there are cases where the minimal base size is unbounded or quite small. Bounds on the minimal base size of G are also given.

Determining which groups of affine type have a base of size 2 is equivalent to determining which finite groups G and which faithful irreducible $\mathbb{F}_pG$-modules V, where p is any prime, are such that G has a regular orbit on V. We focus on the case where G is a symmetric group or an alternating group. With the exception of finitely many explicitly stated examples and one class of modules for which the existence of a regular orbit is proved to be impossible, it is shown that a regular orbit always exists.

Acknowledgements

First I would like to thank my supervisor Jan Saxl for making my dream to come to Cambridge and try my hand at group theory a reality, and for suggesting a problem which so quickly fascinated me. I am grateful for his kindness, his guidance and many valuable observations.

I would like to give my thanks to Peter Cameron for his fruitful suggestion to explore probabilistic avenues and for cheerfully taking the time to read through my work. I am grateful to Ross Lawther for giving my fourth term report a thorough read and making useful suggestions, to an anonymous referee for a careful reading of my preprint on the diagonal case, to my examiners for their insights and prompt reading of this dissertation, to Eamonn O'Brien for introducing me to Magma and swiftly responding to my many requests, and to Bob Guralnick for his mathematical help. I am also grateful to Sally Lowe for her patience and administrative advice, and to Martin Hyland for his tireless support. Lastly, I am grateful to Syd Bulman-Fleming, Kathie Cameron, Ed Wang and Ross Willard for helping me discover my love of group theory and mathematical research, and for getting me to Cambridge in the first place.

For the generous funding I have received, both for my degree and for travel to conferences worldwide, I gratefully acknowledge St John's College, the Cambridge Commonwealth Trust, the Lundgren Fund, the NSERC, and DPMMS.

My time in Cambridge at St John's College and DPMMS has been wonderful, far surpassing even my lofty expectations. I am very appreciative of my college, for their support, for many exciting adventures and for honouring traditions. In particular, I am grateful to Grant Bayliss for opening up doors and making me feel so welcome. I would also like to thank my friends and fellow PhD students, especially Frank DiTraglia and my officemate Jon Nelson, for their moral support, for listening to my complaints, for answering my questions and for making this experience so much fun.

Finally, this dissertation would not have been possible without the love, encouragement, patience and tolerance of my family. I am blessed to have such caring and supportive people in my life. I am immeasurably grateful to Francis, for happily fixing all of my computer problems, for carefully reading through papers, applications and this dissertation, for making me laugh at the darkest times, and for always being there. And I am indebted to my parents, whose belief in me has never wavered, and without whom I would have given up long ago.

Contents

Chapter 1

Introduction

Permutation groups are essential to mathematics and science, as they allow us to understand and model the different types of symmetry in the world around us. These symmetries may be captured in an economical way using tools called bases.

Let G be a finite permutation group acting on a set Ω. A base $\mathscr{B}$ for G is a non-empty subset of Ω with the property that only the identity can fix every element of $\mathscr{B}$. Bases have been very useful in permutation group theory in the past half century, both theoretically in bounding the order of a primitive permutation group in terms of its degree (e.g. [2]) and computationally (surveyed in [70]). Indeed, bases allow us to store the action of a group more efficiently, for if two elements g and h of G agree on every point of a base $\mathscr{B}$, then gh^{-1} fixes every point of $\mathscr{B}$ and so $g = h$. It is therefore desirable to understand bases of small cardinality and quantify how small this cardinality can be. Accordingly, we define the base size of G to be the minimal cardinality of a base for G, and we denote this quantity by $b(G)$.

We will focus on studying the bases of primitive permutation groups. A transitive permutation group G acting on a set Ω is primitive if there are no non-trivial G-invariant partitions of Ω, which essentially means that the action of G cannot be broken down into a smaller one. This makes primitive permutation groups the natural starting point for any problem in permutation group theory. Much research has been done on bounding the general base size of a primitive permutation group (e.g. [47]), and so we wish to look more closely at the base sizes of individual primitive permutation groups. With such an objective in mind, we appeal to the O'Nan-Scott Theorem [49, 67], which classifies the finite primitive permutation groups into five classes. These consist of groups of diagonal

type, twisted wreath type, product type, affine type and almost simple type.

Determining the base size of a group of almost simple type, which is a primitive almost simple group (see Section 2.4), has attracted much attention over the last decade. It was conjectured by Cameron [17] and then proved in [10, 13–15, 18, 33, 52] that if G is an almost simple primitive permutation group, then $b(G) \leqslant 7$ unless the action of G is standard, in which case the base size is unbounded in general. (G has a standard action if G is either S_n or A_n acting on the set of k-subsets or partitions of $\{1, \ldots, n\}$, or a classical group acting primitively on an orbit of subspaces of its natural module.) Moreover, it was proved in [13] that if G is S_n or A_n acting primitively on some set, then $b(G) = 2$ unless the action of G is standard or G is one of 12 listed exceptions. Together with the work of J. James [43], this classifies the primitive actions of S_n and A_n with base size 2. A similar result for primitive actions of almost simple classical groups is forthcoming in [11, 12].

In fact, even more can be said about the base sizes of almost simple primitive permutation groups with non-standard actions. Cameron and Kantor [18] conjectured that for such groups G there exists an absolute constant c with the property that the probability of a random c-tuple of points being a base for G tends to 1 as the order of G tends to infinity. In the same paper, Cameron and Kantor proved that their conjecture is true with $c = 2$ when G is S_n or A_n. Liebeck and Shalev [52] then proved the general conjecture for some undetermined constant c using [33]. The constant $c = 6$ was finally established through work in [14, 55].

Beyond groups of almost simple type, some work has been done on the base sizes of groups of affine type. For example, Seress [68] proved that a soluble primitive permutation group, which is necessarily of affine type, has a base of size at most 4. Furthermore, it turns out that classifying groups of affine type with base size 2 amounts to determining which finite non-trivial groups G and which faithful irreducible $\mathbb{F}_pG$-modules V, where p is any prime, are such that G has a regular orbit on V (see Section 6.2). Thus results on groups of affine type with base size 2 have been achieved indirectly through recent research on the regular orbits of finite groups, both in the case where the characteristic of the field does not divide the order of the group [34, 46, 48], and more generally [37].

Another research focus for bases of primitive permutation groups has been on proving Pyber's conjecture [64], which proposes that there exists an absolute constant c for which the base size of a primitive permutation group G of degree n is at most $c \log |G| / \log n$. Since the base size of G is bounded below by $\log |G| / \log n$ (see Lemma 2.3.2), this conjecture, if true, would imply that the base size of a primitive permutation group is well controlled even when unbounded. There is some evidence for the validity of Pyber's con-

jecture. Certainly almost simple groups with non-standard primitive actions satisfy the conjecture because their base sizes are bounded above by an absolute constant [18, 33, 52], and Benbenishty has verified the conjecture for standard actions of almost simple groups (see [53] for a reference). Similarly, soluble primitive permutation groups satisfy Pyber's conjecture [68], as do certain other groups of affine type [32, 54]. In fact, it has recently been proved that groups of twisted wreath type and product type also satisfy Pyber's conjecture [16].

Since much of the work done so far on bases of primitive permutation groups has dealt primarily with groups of almost simple type and some groups of affine type, we focus on studying bases of primitive permutation groups that are not of almost simple type, and in particular, bases of groups of diagonal type, groups of twisted wreath type, and certain groups of affine type. Precise definitions for these classes may be found in Sections 4.1, 5.1 and 6.1 respectively.

Groups of diagonal and twisted wreath type are not often studied on their own, as problems about primitive permutation groups typically reduce to groups of affine and almost simple type. However, we will see that the base sizes of groups of diagonal and twisted wreath type can be unbounded, and so there is work to be done. Groups of affine type, on the other hand, make up one of the largest and most diverse classes of primitive permutation groups. In fact, results about regular orbits are of independent interest to representation theorists. For example, results by Liebeck [48], Goodwin [34], and Köhler and Pahlings [46] provided an important contribution to the solution of the famous $k(GV)$-problem [66], which proved part of a well-known conjecture of Brauer concerning defect groups of blocks [9].

There is strong evidence that many primitive permutation groups have base size 2, as we have seen above. In fact, base size 2 is essentially the best possible result, for a primitive permutation group has base size 1 if and only if it has prime order and degree (see Lemma 2.3.3). Thus our primary objective will be to determine when groups of diagonal, twisted wreath and affine type have base size 2, though we will also prove some further results concerning bases for groups of diagonal and twisted wreath type.

The primitive action of groups of diagonal and twisted wreath type is largely controlled by a smaller permutation group called the top group. For groups of diagonal type, this top group must itself be primitive (or trivial of degree 2), and we prove that if it is not the symmetric or alternating group, then a base of size 2 always exists (Theorem 4.0.1). Moreover, when the top group is the symmetric or alternating group, we determine the minimal base size up to two possible values and see that it can be unbounded (Theorem

4.0.2). Using these results, we prove Pyber's conjecture for groups of diagonal type (Theorem 4.0.3). Lastly, we prove several probabilistic results that are similar to those described above for primitive almost simple groups (Theorems 4.0.4, 4.0.5 and 4.0.6).

Groups of twisted wreath type are somewhat more complicated than groups of diagonal type, as the top group can also be imprimitive, which means that it is transitive but not primitive. However, when it is primitive, including the case when it is the symmetric group or the alternating group, we prove that a base of size 2 always exists (Theorem 5.0.1) and that almost any pair of points forms a base (Theorem 5.0.2). Moreover, we give some bounds for the base size of a group of twisted wreath type with largest possible imprimitive top group, namely $S_m \wr_r S_r$, and we find that this base size is small in some cases and unbounded in others (Theorem 5.0.3). To do so, we classify the groups of twisted wreath type with top group $S_m \wr_r S_r$ (Proposition 5.5.1), which in turn requires us to determine the almost simple quotients of point stabilisers in $S_m \wr_r S_r$ (Lemma 5.4.10), and in particular, the normal subgroups of $S_m \wr_r S_r$ (Proposition 5.4.7). Lastly, we consider another class of groups of twisted wreath type with imprimitive top group and prove they have base size at most 3 (Theorem 5.0.4). Some general bounds on the base size are also given (Lemmas 5.2.5 and 5.2.6).

For groups of affine type, we focus on determining the regular orbits of the irreducible representations of the symmetric and alternating groups over fields of arbitrary characteristic. In particular, we prove that a regular orbit always exists with the exception of finitely many explicitly stated examples and one infinite class for which the existence of a regular orbit is proved to be impossible (Theorem 8.0.1).

Our focus on the symmetric and alternating groups is motivated by Hall, Liebeck and Seitz [37, Theorem 6], who proved that if G is a finite quasisimple group and V is a faithful FG-module where F is a field of characteristic p such that G has no regular orbits on V, then either $p > 0$ and G is of Lie type in characteristic p, or $G/Z(G) \simeq A_n$ where $0 < p \leqslant n$ and every non-trivial composition factor of V is the fully deleted permutation module (see the end of Section 8.3), or $(G, [V, G])$ is one of finitely many exceptional pairs. We wish to expand on this result and, in particular, determine the exceptions. Given the appearance of A_n in the theorem, it is natural to begin with this group, and since the representation theory of S_n is closely related and much simpler, we compute the regular orbits of S_n first.

This dissertation is organised as follows. In Chapter 2, we begin by gathering some basic notation as well as some concepts concerning permutation groups. Then the dissertation is divided into two parts. The first deals with the non-affine case, and the second

deals with the affine case. This is done because the methods used for groups of diagonal and twisted wreath type are not only similar but are more of a permutation group theory flavour, while the methods used for groups of affine type are more of a representation theory flavour.

In Part I, we focus on studying the bases of groups of diagonal type and groups of twisted wreath type. In Chapter 3, we begin by proving some properties of finite non-abelian simple groups; next we describe the general methodology for proving probabilistic results about bases; then we introduce some useful notation for counting conjugacy classes; and we finish with a technical result that will be used in both cases to prove most pairs of points form bases. In Chapters 4 and 5, we consider bases of groups of diagonal type and groups of twisted wreath type respectively. Lastly, Appendix A provides the source code of GAP functions used for proofs in the diagonal and twisted wreath cases.

In Part II, we focus on the base size 2 problem for groups of affine type, and in particular, on the regular orbit problem for the symmetric and alternating groups. In Chapter 6, we first define groups of affine type and see how the base size 2 problem for these groups is equivalent to the regular orbit problem, and then we determine some useful bounds on the dimensions of certain faithful irreducible representations. Chapter 7 consists entirely of background material about representation theory: we begin by introducing some properties of modules over fields of arbitrary characteristic, with a focus on finite fields; next we consider the representation theory of index 2 subgroups; and we finish by defining Brauer characters and summarising some of their main properties. Lastly, Chapter 8 is devoted to the regular orbit problem for the symmetric and alternating groups.

Note that most of the results for the diagonal and twisted wreath cases require the classification of the finite simple groups, while all of the results in the affine case are independent of the classification.

Chapter 2

Basic notation and permutation group theory

In this chapter, we outline the notation that will be used throughout this dissertation, and we then provide some important definitions and results about permutation groups, including some concerning bases. More specifically, in Section 2.1 we review some basic notation and facts, all of which are well known, and in Section 2.2 we collect some notation and facts that are specific to group actions including a definition of primitivity. In Section 2.3 we consider some useful properties of bases, and in Section 2.4 we delve deeper into the theory of primitive permutation groups and the O'Nan-Scott Theorem.

2.1 Some notation and useful facts

In this dissertation, all groups are finite and all group homomorphisms are performed on the right, unless otherwise specified. See [65] for more details on the notation and definitions given in this section.

Let G be a group with subgroups H and K. Let $g, h \in G$. The *commutator* of g and h is $[g,h] := g^{-1}h^{-1}gh$, the *centraliser* of g in G is denoted by $C_G(g)$, and the *conjugacy class* of g in G is denoted by g^G. The *centraliser* or *normaliser* of H in G is denoted by $C_G(H)$ or $N_G(H)$ respectively, and we say that K *centralises* or *normalises* H if $K \leqslant C_G(H)$ or $K \leqslant N_G(H)$. The subgroup of G generated by $\{[h,k] : h \in H, k \in K\}$ is denoted by $[H,K]$, and the *derived subgroup* $[G,G]$ of G is denoted by G'. The *centre* of G is denoted by $Z(G)$. A *right* (or *left*) *transversal* for H in G is a set of right (or left) representatives for the cosets of H, and we write $[G : H]$ for the *index* of H in G. The group G is an *extension of H by K* if $H \trianglelefteq G$ and $G/H \simeq K$, and the extension is *split* if G contains a subgroup L isomorphic to K for which $HL = G$ (or equivalently, $H \cap L = 1$).

The automorphisms of G form a group called the *automorphism group*, and this group is denoted by $\mathrm{Aut}(G)$. The inner automorphisms of G, that is, those that are induced by conjugation of elements of G, form a group called the *inner automorphism group* of G, and this group is denoted by $\mathrm{Inn}(G)$. $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$, and so we define the *outer automorphism group*, denoted by $\mathrm{Out}(G)$, to be the quotient of $\mathrm{Aut}(G)$ by $\mathrm{Inn}(G)$. Note that $G/Z(G) \simeq \mathrm{Inn}(G)$, so if T is a non-abelian simple group, then $T \simeq \mathrm{Inn}(T)$. Consequently, we often identify $\mathrm{Inn}(T)$ with T.

The following is a useful technical result.

Lemma 2.1.1. *Let G be a group with subgroups H, K and L, where L normalises K. Then $H \cap (KL) = (H \cap K)L$ if and only if $L \leqslant H$.*

Proof. If $H \cap (KL) = (H \cap K)L$, then $L \leqslant H$. Conversely, if $L \leqslant H$, then certainly $(H \cap K)L \leqslant H \cap (KL)$, and if $h = kl \in H \cap (KL)$, then $h = (hl^{-1})l \in (H \cap K)L$. □

We write $\log x$ for the natural logarithm, $\mathrm{Im}(\varphi)$ for the image of a function φ, $\mathbb{F}_q$ for the finite field of size q, C_n for the cyclic group of order n, and $[n]$ for the set $\{1, \ldots, n\}$ where n is any positive integer. An *involution* is an element of G of order 2.

2.2 Group actions

The definitions and results in this section are well known, but [17, 23] act as general references. Let G be a group, and suppose that G acts on a set Ω. We will always assume that Ω is finite, and we say that the *degree* of G is $|\Omega|$. Note that all actions will be performed on the right, unless otherwise specified, and so we normally write ω^g or ωg for the image of $\omega \in \Omega$ under $g \in G$.

The *stabiliser* of $\omega \in \Omega$, or *ω-stabiliser*, is the subgroup of G consisting of those elements that fix ω and is denoted by G_ω. The *orbit* of $\omega \in \Omega$ is $\omega^G := \{\omega g : g \in G\}$. Then the orbit-stabiliser theorem states that $|G| = |G_\omega||\omega^G|$ for all $\omega \in \Omega$.

The action of G is *transitive* if for every $\omega_1, \omega_2 \in \Omega$ there exists $g \in G$ for which $\omega_1 g = \omega_2$. In other words, $\omega^G = \Omega$ for any $\omega \in \Omega$. If there exists $\omega \in \Omega$ for which $\omega g \neq \omega$ for all $1 \neq g \in G$, or equivalently, if there exists $\omega \in \Omega$ for which $G_\omega = 1$, then ω is a *regular orbit* of G. When this occurs, $|G| = |\omega^G|$ by the orbit-stabiliser theorem. If G is transitive and has a regular orbit, then G acts *regularly* on Ω, and $|G| = |\Omega|$. The action is *faithful* if the identity of G is the only element of G fixing every element of Ω.

If G acts transitively on $\{(\omega_1, \omega_2) \in \Omega \times \Omega : \omega_1 \neq \omega_2\}$ where $(\omega_1, \omega_2)g := (\omega_1 g, \omega_2 g)$, then G is *2-transitive*. The *setwise stabiliser* of $\Delta \subseteq \Omega$ is the subgroup of G consisting of

those $g \in G$ for which $\Delta g = \Delta$, where $\Delta g := \{\delta g : \delta \in \Delta\}$. The set of fixed points in Ω of $g \in G$ is denoted by $\mathrm{fix}_\Omega(g)$. A permutation with no fixed points is *fixed-point-free*.

The group G is a *permutation group* on Ω if G acts faithfully on Ω. If G is a permutation group on Ω and H is a permutation group on Δ, then G and H are *permutation isomorphic* if there exists an isomorphism $\varphi : G \to H$ and a bijection $\psi : \Omega \to \Delta$ for which $(\omega g)\psi = \omega\psi(g\varphi)$ for all $\omega \in \Omega$ and $g \in G$. If H is a subgroup of G, then we denote the right (or left) coset space by $(G : H)$. Then a transitive action of G on Ω is permutation isomorphic to the action of G by right (or left) multiplication on $(G : G_\omega)$ for any $\omega \in \Omega$.

A *block* of G is a non-empty subset Γ of Ω such that for every $g \in G$, either $\Gamma = \Gamma g$ or $\Gamma \cap \Gamma g = \emptyset$. The blocks Ω and $\{\omega\}$ for all $\omega \in \Omega$ are *trivial*, while any other block of Ω is *non-trivial*. The action of G on Ω is *primitive* if it is transitive and there are no non-trivial blocks, and *imprimitive* if it is transitive but not primitive. Note that this definition for primitivity is equivalent to the more intuitive one given in the Introduction. Furthermore, we have the following equivalency. See [23, Corollary 1.5A] for a proof.

Proposition 2.2.1. *Let G be a group acting on Ω where $|\Omega| \geqslant 2$. Then G is primitive on Ω if and only if G is transitive on Ω and G_ω is maximal in G for all $\omega \in \Omega$.*

In fact, if G is transitive, then the stabilisers G_ω are conjugate for all $\omega \in \Omega$, so G is primitive if G_ω is maximal for some $\omega \in \Omega$.

We denote the symmetric and alternating groups on n points by S_n and A_n respectively. Note that S_n and A_n act primitively on $[n]$ by Proposition 2.2.1 for $n \geqslant 3$, and S_2 acts primitively on $[2]$. In addition, S_n and A_n are the only primitive permutation groups of degree n when $n = 3$ or $n = 4$, and the only permutation groups when $n = 2$.

Now we investigate the automorphism group of A_n.

Proposition 2.2.2. *If $n \geqslant 5$, then $S_n \leqslant \mathrm{Aut}(A_n)$ with equality if and only if $n \neq 6$. Moreover, $\mathrm{Aut}(A_6)$ is an extension of S_6 by C_2.*

Proof. The map $\varphi : S_n \to \mathrm{Aut}(A_n)$ defined by $s \mapsto (t \mapsto s^{-1}ts)$ for all $s \in S_n$ and $t \in A_n$ is an injective group homomorphism since $C_{S_n}(A_n) = 1$, and φ is surjective when $n \neq 6$ (see [23, Theorem 8.2A]). The remaining claim follows from [38]; see also [72, 3.2.19]. □

Let H and K be groups, and suppose that K acts on H in such a way that $(h_1h_2)^\kappa = h_1^\kappa h_2^\kappa$ for all $h_1, h_2 \in H$ and $\kappa \in K$. Note that this is equivalent to the existence of a homomorphism from K to $\mathrm{Aut}(H)$. Then we may define the *semidirect product* of H and K, denoted by $H \rtimes K$, to be the group whose underlying set is the Cartesian product $H \times K$ and whose multiplication is defined by $(h_1, \kappa_1)(h_2, \kappa_2) = (h_1 h_2^{\kappa_1^{-1}}, \kappa_1\kappa_2)$. Often,

we write $h\kappa$ for the element $(h, \kappa) \in H \rtimes K$. Observe that H is a normal subgroup of $H \rtimes K$, and so a group G is a split extension of H by K if and only if $G \simeq H \rtimes K$.

Now suppose that H and K are groups where K acts on $[r]$ for some r. Then K also acts on $H^r = H \times \cdots \times H$ by permuting the coordinates. That is, the element $\kappa^{-1} \in K$ maps $(h_1, \ldots, h_r) \in H^r$ to $(h_{1\kappa}, \ldots, h_{r\kappa})$. As a result, we may define the *wreath product* of H and K, denoted by $H \wr_r K$, to be the semidirect product $H^r \rtimes K$. Elements of $H \wr_r K$ are normally written in the form $(h_1, \ldots, h_r)\kappa$, where $(h_1, \ldots, h_r) \in H^r$ and $\kappa \in K$.

There are two standard actions of a wreath product, and these give examples of primitive and imprimitive actions. Let H act transitively on Δ, and let K act transitively on $[r]$. Then $H \wr_r K$ acts on Δ^r by sending $(\delta_1, \ldots, \delta_r)$ to $(\delta_{1\kappa}^{h_{1\kappa}}, \ldots, \delta_{r\kappa}^{h_{r\kappa}})$ for every $(\delta_1, \ldots, \delta_r) \in \Delta^r$ and $(h_1, \ldots, h_r)\kappa^{-1} \in H \wr_r K$. This is called the *product action*. If H is primitive but not regular on Δ, then the product action is primitive [23, Lemma 2.7A]. On the other hand, $H \wr_r K$ acts on $\Delta \times [r]$ by sending (δ, i) to $(\delta h_i, i\kappa)$ for every $(\delta, i) \in \Delta \times [r]$ and $(h_1, \ldots, h_r)\kappa \in H \wr_r K$. This action is transitive, and the sets $\Gamma_i := \{(\delta, i) : \delta \in \Delta\}$ for $i \in [r]$ are blocks that partition Δ, so this action is imprimitive. In fact, if H is any imprimitive subgroup of S_n with r blocks of size m, then H is permutation isomorphic to a subgroup of $S_m \wr_r S_r$ in its imprimitive action on $[m] \times [r]$.

2.3 Bases of permutation groups

Let G be a permutation group on a set Ω. As in the Introduction, a *base* $\mathscr{B}$ for G is a non-empty subset of Ω with the property that if $g \in G$ and $\omega g = \omega$ for all $\omega \in \mathscr{B}$, then g must be the identity. The *base size* of G is the minimal cardinality of a base for G, and we denote this by $b_\Omega(G)$. The subscript Ω will be omitted when the context permits.

We begin with the following elementary result.

Lemma 2.3.1. *Let G be a permutation group on Ω, and let $\mathscr{B} \subseteq \Omega$. Let $g \in G$. Then $\mathscr{B}$ is a base for G if and only if $\mathscr{B}g$ is a base for G.*

Proof. Suppose that $\mathscr{B}$ is a base for G. If some $h \in G$ fixes every element of $\mathscr{B}g$, then ghg^{-1} fixes every element of $\mathscr{B}$, so $h = 1$. Thus $\mathscr{B}g$ is a base for G. □

In particular, if G is a transitive permutation group on Ω and ω is some nice element of Ω, then to find a base for G, Lemma 2.3.1 implies that we may restrict our attention to those subsets of Ω that contain ω.

The following result provides a useful lower bound on the base size of a group, which we will exploit on several occasions. In particular, this result motivates Pyber's conjecture, which was described in the Introduction.

Lemma 2.3.2. *Let G be a permutation group of degree n. Then*

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

Proof. Suppose that $\{\omega_1, \ldots, \omega_{b(G)}\}$ is a base of minimal size for G. Let $G^{[0]} := G$ and $G^{[i]} := (G^{[i-1]})_{w_i}$ for $1 \leqslant i \leqslant b(G)$. Note that $G^{[b(g)]} = 1$. Then since $[G^{[i]} : G^{[i+1]}] \leqslant n - i$ for all $0 \leqslant i \leqslant b(G) - 1$ by the orbit-stabiliser theorem and $|G| = \prod_{i=0}^{b(G)-1} [G^{[i]} : G^{[i+1]}]$, it follows that $|G| \leqslant n(n-1)\cdots(n-b(G)+1)$. Thus $|G| \leqslant n^{b(G)}$, and the result follows. □

We mentioned in the Introduction that a primitive permutation group G has base size 1 if and only if G has prime order and degree. This we now prove.

Lemma 2.3.3. *Let G be a non-trivial primitive permutation group on Ω. Then $b(G) = 1$ if and only if $G = C_p$ for some prime p. When these conditions hold, $|\Omega| = p$.*

Proof. If $G = C_p$ for some prime p, then since G acts faithfully and transitively on Ω, the orbit-stabiliser theorem forces $|\Omega| = p$ and $G_\omega = 1$ for any $\omega \in \Omega$. Thus $b(G) = 1$. Conversely, if $b(G) = 1$, then there exists $\omega \in \Omega$ such that $G_\omega = 1$, and G_ω is a maximal subgroup of G by Proposition 2.2.1, so $G \simeq C_p$ for some prime p. □

2.4 The O'Nan-Scott Theorem

Both the structure and action of a primitive permutation group are largely controlled by the action of a certain normal subgroup called the socle, and a close analysis of this action results in the O'Nan-Scott Theorem, which classifies primitive permutation groups into one of five types. The theorem first appeared under a different guise as the classification of the maximal subgroups of the symmetric group [67]. In this section, we provide a rough description of the more recent version. Further details may be found in [17, 23, 49].

Let G be a group. The *socle* of G is defined to be the subgroup generated by the set of all minimal normal subgroups of G, where a *minimal normal subgroup* N of G is a non-trivial normal subgroup of G with the property that N is the only non-trivial normal subgroup of G contained in N. Distinct minimal normal subgroups centralise one another, and it turns out that every minimal normal subgroup is a direct product of isomorphic simple groups [23, Theorem 4.3A]. Hence the socle of G is itself isomorphic to a direct product of (possibly non-isomorphic) simple groups.

In fact, the structure of the socle of a primitive permutation group is even more restricted, for if G is such a group, then G has at most two minimal normal subgroups. This occurs because any non-trivial normal subgroup of a primitive permutation group must

act transitively, and it follows that if there are two distinct minimal normal subgroups, then one must be the centraliser of the other. Moreover, if there are two minimal normal subgroups, then they must be isomorphic. Consequently, the socle of G is isomorphic to T^k for some simple group T and positive integer k (see [49] for more details).

Using the restricted structure of the socle, primitive permutation groups can then be classified into one of five types. This classification is the O'Nan-Scott Theorem, which we now state. Note that its proof relies upon the classification of the finite simple groups.

Theorem 2.4.1 (O'Nan-Scott [49, 67])**.** *A finite primitive permutation group is permutation isomorphic to a group that is either of diagonal type, twisted wreath type, product type, affine type or almost simple type.*

Groups of diagonal type, twisted wreath type and affine type are defined in Sections 4.1, 5.1 and 6.1 respectively, and groups of product type are defined in [49]. For all of these types, the structure and action of the group can be described explicitly. However, an explicit action is not given for groups of almost simple type, though we can say something about the structure of these groups.

An arbitrary group G is said to be *almost simple* if $T \leqslant G \leqslant \mathrm{Aut}(T)$ for some non-abelian simple group T; equivalently, G is almost simple if it has a non-abelian simple socle. For example, S_n is almost simple for $n \geqslant 5$ as a consequence of either Proposition 2.2.2 or the observation that A_n is the socle of S_n. Then a group G is said to be of *almost simple type* if G is an almost simple group acting primitively on some unspecified set.

By considering the various possibilities for the socle T^k, we can see when the various types of Theorem 2.4.1 arise. Suppose that G is a primitive permutation group on Ω with socle T^k where T is a simple group and k is a positive integer. When T is abelian, the group G is of affine type. (In particular, the only primitive permutation groups with base size 1 are of affine type by Lemma 2.3.3.) When T is non-abelian and $k = 1$, the group G is of almost simple type. Now suppose that T is non-abelian and $k > 1$. When T^k acts regularly on Ω, the group G is of twisted wreath type. Otherwise, there are two possibilities. Roughly speaking, either the stabiliser in T^k of a point is precisely the diagonal subgroup of T^k, in which case G is a group of diagonal type, or there exists a positive integer r dividing k so that $T^{k/r}$ is the socle of some primitive permutation group H on Δ such that H is of almost simple or diagonal type and G is a subgroup of $H \wr_r S_r$ that acts via the product action on Δ^r, in which case G is a group of product type.

Hence the study of primitive permutation groups amounts to the study of the five types of Theorem 2.4.1. We will study the bases of groups of diagonal type, twisted wreath type and certain groups of affine type.

Part I

The non-affine case

Chapter 3

Preliminaries for the non-affine case

Though groups of diagonal type and groups of twisted wreath type are constructed very differently, their bases can be studied in similar ways for several reasons. Firstly, all primitive permutation groups of non-affine type share the feature that their socles are products of non-abelian simple groups, and since the socle influences the action of a primitive permutation group, we must naturally study non-abelian simple groups for both cases. Secondly, the method for proving probabilistic results about bases is the same in both cases. Thirdly, the primitive actions of groups of diagonal and twisted wreath type are both largely controlled by a smaller permutation group, referred to in both cases as the top group. In the diagonal case, the top group can be any primitive permutation group, whereas in the twisted wreath case, the top group can be primitive or imprimitive. When the top group P is a primitive permutation group that is not the alternating or symmetric group, there are various general results at our disposal, which, for example, bound the size of P, or bound the minimum number of points moved by elements of P. These results can then be used to prove results about bases of groups of diagonal and twisted wreath type.

Accordingly, in this chapter we gather together some technical definitions and prove some technical results that will be used to study the bases of both types. All of the material in this chapter has been published by the author [25], with the exceptions of Lemmas 3.1.1 and 3.1.2, which are basic results, and Lemma 3.1.3, which appeared in [25] in a weaker form without proof. We include a proof here for the sake of completeness.

This chapter is organised as follows. In Section 3.1, we prove some results concerning non-abelian simple groups. In Section 3.2, we consider how to approach bases proba-

bilistically, and in Section 3.3, we provide some notation and basic facts for counting conjugacy classes. We then prove a technical result in Section 3.4 that will be used in both the diagonal and twisted wreath cases.

3.1 Non-abelian simple groups

The classification of the finite simple groups, hereafter referred to as the CFSG, states that a finite non-abelian simple group is either an alternating group A_n for $n \geqslant 5$, a group of Lie type, or one of 26 sporadics. The groups of Lie type consist of ten families of exceptional simple groups as well as the classical simple groups, which are the linear groups $L_n(q)$, the symplectic groups $PSp_{2n}(q)$, the unitary groups $U_n(q)$, and the three classes of orthogonal groups, namely $\Omega_{2n+1}(q)$ where q is odd, $P\Omega^+_{2n}(q)$ and $P\Omega^-_{2n}(q)$. A considerable amount of information about these groups is contained in Kleidman and Liebeck [45], with which our notation is consistent.

We begin by describing the centralisers of almost simple groups.

Lemma 3.1.1. *If T is a non-abelian simple group, then $C_{\mathrm{Aut}(T)}(T)$ is trivial.*

Proof. Let $\sigma \in C_{\mathrm{Aut}(T)}(T)$ and fix $t \in T$. Define $\varphi_t : T \to T$ by $x \mapsto t^{-1}xt$ for all $x \in T$. Then $t^{-1}xt = x\varphi_t = x\sigma^{-1}\varphi_t\sigma = (t\sigma)^{-1}x(t\sigma)$ for all $x \in T$, so $(t\sigma)t^{-1} \in Z(T) = \{1\}$. □

Consequently, subgroups of $\mathrm{Aut}(T)$ that are normalised by T are almost simple, as the following shows.

Lemma 3.1.2. *Let T be a non-abelian simple group. If N is a non-trivial subgroup of $\mathrm{Aut}(T)$ that is normalised by T, then $T \leqslant N$.*

Proof. Suppose that $T \nleqslant N$. Then $N \cap T = 1$ since T is simple and $N \cap T \trianglelefteq T$. But $[n, t] \in N \cap T$ for all $n \in N$ and $t \in T$, so $N \leqslant C_{\mathrm{Aut}(T)}(T) = 1$ by Lemma 3.1.1. □

Next we see that the size of the outer automorphism group of a non-abelian simple group T is quite small with respect to the size of T.

Lemma 3.1.3. *Let T be a non-abelian simple group. Then $|\mathrm{Out}(T)|^3 < |T|$. Moreover, $|\mathrm{Out}(T)|^4 < 2|T|$.*

Proof. Note that $|\mathrm{Out}(T)|$ and $|T|$ are listed in [45, Section 5.1], for example. Certainly the lemma is true if T is sporadic or alternating as $|\mathrm{Out}(T)| \leqslant 2$ or is 4 when $T = A_6$. If T is an exceptional group of Lie type over $\mathbb{F}_q$ that is not one of $E_6(q)$, ${}^3D_4(q)$ or ${}^2E_6(q)$, then $|\mathrm{Out}(T)| \leqslant q$ and $|T| > q^4$, as desired. If T is one the remaining exceptional groups,

then $|\operatorname{Out}(T)| \leqslant 3q$ and $|T| > q^{12}$, but $3^4 < q^7$, so the claim follows. Thus we may assume that T is a classical group of Lie type over $\mathbb{F}_q$.

Suppose that T is a symplectic group $PSp_{2n}(q)$ where $n \geqslant 2$ or an orthogonal group in odd dimension $\Omega_{2n+1}(q)$ where $n \geqslant 3$. Then $|\operatorname{Out}(T)| \leqslant q$ and $|T| > q^4$, so we are done. Moreover, if T is $P\Omega^-_{2n}(q)$ where $n \geqslant 4$, then $|\operatorname{Out}(T)| \leqslant 4q \leqslant q^3$ and $|T| > q^{n(n-1)} \geqslant q^{12}$, and if T is $P\Omega^+_{2n}(q)$ where $n \geqslant 4$, then $|\operatorname{Out}(T)| \leqslant 12q \leqslant q^5$ and $|T| > q^{12}(q^2-1)(q^4-1)(q^6-1) > q^{21}$.

Suppose that T is a unitary group $U_n(q)$ where $n \geqslant 3$. If $n \neq 3$, then $|\operatorname{Out}(T)| \leqslant q(q+1)$ and $|T| \geqslant q^6(q^3+1)(q^4-1) > q^4(q+1)^4$, as desired. Suppose then that $n = 3$, in which case $q \neq 2$, or else T is not simple. If $q = 3$, then $|\operatorname{Out}(T)| = 2$, and if $q \geqslant 4$, then $|\operatorname{Out}(T)|^4 < |T|$ since $|\operatorname{Out}(T)| \leqslant 3q$ and $|T| \geqslant q^3(q^2-1)(q^3+1)/3$.

Lastly, suppose that T is a linear group $L_n(q)$ where $n \geqslant 2$. If $n \geqslant 4$, then $|\operatorname{Out}(T)| \leqslant q^2$ and $|T| > q^6(q+1)(q^3-1) > q^8$, as desired. Suppose that $n = 2$. If $q = 2^f$, then $|\operatorname{Out}(T)| = f$ and $|T| = q(q^2-1) = 2^f(4^f-1)$, so $|\operatorname{Out}(T)|^4 < |T|$. If q is an odd prime, then $|\operatorname{Out}(T)| = 2$, so we may assume that $q = p^f$ where p is an odd prime and $f \geqslant 2$. Then $|\operatorname{Out}(T)| = 2f$ and $|T| \geqslant 3^f(9^f-1)/2$, so $|\operatorname{Out}(T)|^4 < |T|$. Thus we may assume that $n = 3$. Then $|\operatorname{Out}(T)| \leqslant 3q$ and $|T| \geqslant q^3(q^2-1)(q^3-1)/3$, so $|\operatorname{Out}(T)|^4 < |T|$ if $q \geqslant 5$. If $q = 2$ or $q = 3$, then $|\operatorname{Out}(T)| = 2$, so we may assume that $q = 4$. Then $|\operatorname{Out}(T)| = 12$ and $|T| = 20160$. Since $12^3 = 1728$ and $12^4 = 2 \cdot 10368$, we are done. □

Our last result of this section shows that the size of the outer automorphism group of a non-abelian simple group T is so small that it can be bounded above by the minimal index of a proper subgroup of T, which is typically quite small itself compared to T. We denote the minimal index by $p(T)$. Also, we denote by $l(T)$ the untwisted Lie rank of a simple group T of Lie type; when T is a twisted group, this is simply the Lie rank of the corresponding untwisted group. The untwisted Lie rank was used to bound the number of conjugacy classes in a simple group of Lie type in [50, Theorem 1], and we will use these results together in Section 4.3. Note that $l(T)$ can differ between certain pairs of isomorphic simple groups such as $L_3(2) \simeq L_2(7)$. However, there are only finitely many such exceptions, so the presence of the absolute constant C in Lemma 3.1.4 below allows us to choose the more convenient value of $l(T)$ in such cases.

Lemma 3.1.4. *Let T be a non-abelian simple group of Lie type over $\mathbb{F}_q$ where $T \neq L_n(2)$ for any n. Then*

$$|\operatorname{Out}(T)|^2(6q)^{l(T)} \leqslant Cp(T)^{11/4}$$

for some absolute constant C.

Proof. Note that the presence of the absolute constant C allows us to ignore finitely many T. Write $q = p^f$ where p is a prime and f is a positive integer. Values for $|\operatorname{Out}(T)|$ may be found in [45, Section 5.1].

Suppose that T is an exceptional group. Since $l(T)$ is constant and $|\operatorname{Out}(T)|$ is bounded above by a constant multiple of q, it suffices to show that $l(T) + 2$ is at most $(11/4)b(T)$ for some constant $b(T)$ for which $p(T) \geqslant q^{b(T)}$. If T is ${}^2B_2(q)$ or ${}^2G_2(q)$, then $l(T) = 2$ and we may take $b(T) = 2$ by [75]. Otherwise, we have $l(T) \leqslant 8$ and we may take $b(T) = 4$ by [73–75]. In both cases, the desired inequality is satisfied.

Let T be one of the following groups: $PSp_{2n}(q)$ where $n \geqslant 2$, $\Omega_{2n+1}(q)$ where $n \geqslant 3$, $P\Omega^+_{2n}(q)$ where $n \geqslant 4$, or $P\Omega^-_{2n}(q)$ where $n \geqslant 4$. Then $l(T) = n$, $p(T) \geqslant q^{2n-2}$ by [59, 76], and $|\operatorname{Out}(T)|$ is at most a constant multiple of q. Since $q^2(6q)^n$ is at most $36q^{2(2n-2)}$, it follows that T satisfies the desired inequality.

Let T be $U_n(q)$ where $n \geqslant 3$. Then $l(T) = n - 1$, $p(T) \geqslant q^{2n-4}$ by [59], and $|\operatorname{Out}(T)|$ is at most a constant multiple of $(q + 1)f$. Since $(q + 1)^2 f^2 \leqslant q^{7/2}$ and $q^{7/2}(6q)^{n-1} \leqslant 36q^{(11/4)(2n-4)}$, we have verified the desired inequality.

Finally, suppose that T is $L_n(q)$ where $n \geqslant 2$. We may assume that $T \neq L_2(9)$. Then $l(T) = n-1$, $p(T) \geqslant q^{n-1}$ by [59], and $|\operatorname{Out}(T)|$ is at most a constant multiple of $(q-1)f$. Note that $(q - 1)^2 f^2 \leqslant q^{7/2}$. If $n \geqslant 3$, then since $q \geqslant 3$ (by assumption), it follows that $q^{7/2}(6q)^{n-1}$ is at most $36q^{(11/4)(n-1)}$, so T satisfies the desired inequality. If $n = 2$, then $|\operatorname{Out}(T)|$ is at most a constant multiple of f, and $f^2 q \leqslant q^{11/4}$, as desired. □

3.2 Probabilistic methods

In this section, we describe the method for proving probabilistic results about bases of groups of diagonal and twisted wreath type. This is done by counting fixed points, as we see in Lemma 3.2.1. In fact, this lemma will be used to prove that certain groups of twisted wreath type have base size 2, and it will appear in a different incarnation in Part II as well (see Section 6.3).

For a transitive permutation group G on Ω and an integer $b \geqslant 1$, let $Q(G, b)$ denote the proportion of b-tuples in Ω^b that are not (ordered) bases for G. The following argument has been made by Liebeck and Shalev [52].

Lemma 3.2.1 ([52])**.** *Let G be a transitive permutation group on Ω. Then for any integer $b \geqslant 1$ and $\omega \in \Omega$,*

$$Q(G, b) \leqslant \sum_{i=1}^{n} \frac{|x_i^G \cap G_\omega|^b |C_G(x_i)|^{b-1}}{|G|^{b-1}},$$

where $\{x_1, \ldots, x_n\}$ is any set of representatives for the G-conjugacy classes of elements of prime order in G_ω.

Proof. If $x \in G$, the proportion of points in Ω that are fixed by x is $|\operatorname{fix}(x)|/|\Omega|$, so the proportion of b-tuples that are fixed by x is $(|\operatorname{fix}(x)|/|\Omega|)^b$. Moreover, if a b-tuple is not a base for G, then it is fixed by some element in G of prime order. Let X be the set of elements in G of prime order, and let $x_1, \ldots, x_n$ be a set of representatives for the G-conjugacy classes of elements in X. Then since $|\operatorname{fix}(x)|/|\Omega| = |x^G \cap G_\omega|/|x^G|$ for any $\omega \in \Omega$ by transitivity,

$$Q(G,b) \leqslant \sum_{x \in X} \left(\frac{|\operatorname{fix}(x)|}{|\Omega|} \right)^b = \sum_{x \in X} \left(\frac{|x^G \cap G_\omega|}{|x^G|} \right)^b = \sum_{i=1}^{n} \frac{|x_i^G \cap G_\omega|^b}{|x_i^G|^{b-1}},$$

as desired. Lastly, we may assume that $x_1, \ldots, x_n$ are elements of G_ω since $|x^G \cap G_\omega| = 0$ if no G-conjugate of x lies in G_ω. □

Thus we have a bound on the proportion of pairs of points that are not bases for G. In particular, if we have a class $\mathscr{C}$ of transitive permutation groups whose orders are unbounded, then it follows from Lemma 3.2.1 that if there exists $\omega \in \Omega$ such that

$$\sum_{i=1}^{n} \frac{|x_i^G \cap G_\omega|^2 |C_G(x_i)|}{|G|} \to 0$$

as $|G| \to \infty$ over $G \in \mathscr{C}$, then almost any pair of elements in Ω forms a base for sufficiently large $G \in \mathscr{C}$.

3.3 Counting conjugacy classes

As a result of Lemma 3.2.1, there are several occasions when we will need to bound the number of conjugacy classes of elements of prime order in a group, so we set up some notation for this. Let G be a group. If $\mathcal{C}$ is a union of conjugacy classes of G, we write $f_{\mathcal{C}}(G)$ for the number of conjugacy classes contained in $\mathcal{C}$. Also, we write $f(G)$ for $f_G(G)$, and when $\mathcal{C}$ consists of the elements of prime order in G, we write $f_p(G)$ for $f_{\mathcal{C}}(G)$. Let H be a subgroup of G. Gallagher noted in [29] that $f(G) \leqslant [G:H] f(H)$ and $f(H) \leqslant [G:H] f(G)$ and gave elementary proofs of these facts. The latter can easily be generalised to $f_{\mathcal{C}}(H)$ for any union of conjugacy classes $\mathcal{C}$ in H, which we now do.

Lemma 3.3.1. *Let G be a group with subgroup H. Let $\mathcal{C} \subseteq \mathcal{C}'$ be unions of conjugacy classes of H and G respectively. Then $f_{\mathcal{C}}(H) \leqslant [G:H] f_{\mathcal{C}'}(G)$. In particular, it follows that $f_p(H) \leqslant [G:H] f_p(G)$.*

Proof. We adapt Gallagher's proof in [29] as follows. First we obtain a formula for $f_{\mathcal{C}}(H)$:

$$\frac{1}{|H|}\sum_{h\in\mathcal{C}}|C_H(h)| = \sum_{h\in\mathcal{C}}\frac{1}{|h^H|} = f_{\mathcal{C}}(H).$$

Of course, this formula can be used to determine $f_{\mathcal{C}'}(G)$ as well. Since $\mathcal{C}\subseteq\mathcal{C}'$ and $C_H(h)\leqslant C_G(h)$ for all $h\in\mathcal{C}$, the result follows. □

Focusing on the symmetric and alternating groups, we have the following basic but useful result.

Lemma 3.3.2. *$f_p(S_n)\leqslant n^2/2$ and $f_p(A_n)\leqslant n^2$.*

Proof. Since conjugacy in S_n is determined by cycle type, and since there are $\lfloor n/p\rfloor$ different cycle types of elements of order p for each prime $p\leqslant n$, it follows that

$$f_p(S_n) = \sum_{\substack{2\leqslant p\leqslant n\\ p \text{ prime}}}\left\lfloor\frac{n}{p}\right\rfloor \leqslant \sum_{\substack{2\leqslant p\leqslant n\\ p \text{ prime}}}\frac{n}{2} \leqslant \frac{n^2}{2}.$$

The result for $f_p(A_n)$ then follows. □

3.4 A useful technical result

Now we state and prove a result that will be used to prove probabilistic results about bases of groups of diagonal and twisted wreath type. This result may appear to have little connection with Lemma 3.2.1, but we will see its importance in Sections 4.3 and 5.3. In both cases, the group P will be taken to be the top group. Note that we write C for some absolute constant that need not and will not be determined (though it could be). This methodology will also apply to another absolute constant $c>1$, though it will be obvious what c needs to be.

Lemma 3.4.1 ([25])**.** *Let P be a primitive subgroup of S_k not containing A_k, and let T be a non-abelian simple group. Then for some absolute constants C and $c>1$,*

$$\sum_{\pi\in R(P)}\frac{|\pi^P|}{|T|^{k-r_\pi-\frac{5}{3}}}\leqslant C\left(\frac{1}{c^k}+\frac{1}{\sqrt{k}}\right),$$

where $R(P)$ denotes a set of representatives for the conjugacy classes of elements of prime order in P, and r_π denotes the number of cycles in the full cycle decomposition of π in S_k, including fixed points.

Note that our assumption in Lemma 3.4.1 that T is a non-abelian simple group is much stronger than necessary; in fact, we can replace $|T|$ with any integer at least 60.

Proof. For $\pi \in P$ of prime order p, let $f_\pi := \mathrm{fix}_{[k]}(\pi)$, and let c_π be the number of non-trivial cycles of π so that $c_\pi = (k - f_\pi)/p$. Then $r_\pi = c_\pi + f_\pi$. Also, note that $r_\pi = k - 1$ for some $\pi \in R(P)$ if and only if P contains a transposition, and this occurs if and only if $P = S_k$ since P is primitive (see [23, Theorem 3.3A] for a proof of this well-known fact). Thus $k - r_\pi \geqslant 2$. In particular, $k - r_\pi - 5/3$ is always positive.

Let $\pi \in R(P)$ have order p. We may write $pc_\pi = \mu(P) + i$ for some non-negative integer i where $\mu(P)$ denotes the minimal degree of P, which is the minimal number of points moved by an element of P. Then $c_\pi = \mu(P)/p + i/p$ and $f_\pi = k - \mu(P) - i$. Since $i/p - i \leqslant 0$ and $p \geqslant 2$, it follows that

$$\max_{\pi \in R(P)} r_\pi \leqslant \left\lfloor \frac{\mu(P)}{2} \right\rfloor + k - \mu(P) = k - \left\lceil \frac{\mu(P)}{2} \right\rceil.$$

We wish to prove that

$$\sum_{\pi \in R(P)} \frac{|\pi^P|}{|T|^{k - r_\pi - \frac{5}{3}}} \leqslant C \left(\frac{1}{c^k} + \frac{1}{\sqrt{k}} \right) \tag{$*$}$$

for some absolute constants C and $c > 1$, and we conclude that this holds whenever

$$\frac{|P|}{|T|^{\left\lceil \frac{\mu(P)}{2} \right\rceil - \frac{5}{3}}} \leqslant C \left(\frac{1}{c^k} + \frac{1}{\sqrt{k}} \right). \tag{$\dagger$}$$

The proof now divides into two cases according to whether $\mu(P) \geqslant k/3$ or not. In the first case, we bound the left-hand side of $(*)$ or $(\dagger)$ by C/c^k, and in the second case, we bound the left-hand side of $(*)$ or $(\dagger)$ by $C/\sqrt{k}$.

Case 1: $\mu(P) \geqslant k/3$.

Suppose first of all that $|T| \geqslant |L_3(3)| = 5616$ and $k > 6$. Since $|P| \leqslant 4^k$ by a classification-free result of Praeger and Saxl [63] and $\lceil k/6 \rceil - 5/3$ is positive,

$$\frac{|P|}{|T|^{\left\lceil \frac{\mu(P)}{2} \right\rceil - \frac{5}{3}}} \leqslant \frac{4^k}{5616^{\left\lceil \frac{k}{6} \right\rceil - \frac{5}{3}}} \leqslant 5616^{\frac{5}{3}} \left(\frac{4}{\sqrt[6]{5616}} \right)^k,$$

which is the upper bound we desire. Suppose instead that $|T| < 5616$. For sufficiently large k, we know that $|P|$ is at most $\exp(4\sqrt{k}(\log k)^2)$ by [3, Corollary 1.2], a classification-free result of Babai. Since k is eventually larger than $24\sqrt{k}(\log k)^2$, it follows that

$$\frac{|P|}{|T|^{\left\lceil \frac{\mu(P)}{2} \right\rceil - \frac{5}{3}}} \leqslant 60^{\frac{5}{3}} \left(\frac{e^{24\sqrt{k}(\log k)^2}}{60^k} \right)^{\frac{1}{6}} \leqslant 60^{\frac{5}{3}} \left(\frac{e}{60} \right)^{\frac{k}{6}}$$

for sufficiently large k, which is again the upper bound we desire. Lastly, suppose that $k = 5$ or $k = 6$, which we may do since P must contain A_k when $k \leqslant 4$. Note that the left-hand side of $(*)$ is bounded above by $|P||T|^{5/3-k+r_{\pi^*}}$ where $\pi^* \in R(P)$ achieves the maximum. Since $k - r_{\pi^*} \geqslant 2$, we may replace $|T|$ by 60, and since $|P|$ and r_{π^*} are constant, this establishes equation $(*)$. Only finitely many G have been excluded from our argument, so this case is complete.

Case 2: $\mu(P) < k/3$.

Let $\Omega_{m,l}$ denote the set of subsets of $[m]$ of size l. Then by Liebeck and Saxl [51, Theorem 2], our assumption on $\mu(P)$ forces P to be a subgroup of $S_m \wr_r S_r$ that contains A_m^r and acts by the product action on $\Omega_{m,l}^r$ for some $m \geqslant 5$, $r \geqslant 1$ and $1 \leqslant l < m/2$. Note that this action is primitive and faithful, that (r, l) is not $(1, 1)$ by assumption, and that $k = \binom{m}{l}^r$. Let

$$g(m, r, l) := \binom{m-2}{l-1}\binom{m}{l}^{r-1}.$$

Observe that $((12), 1, \ldots, 1) \in S_m^r$ moves $2g(m, r, l)$ points of $\Omega_{m,l}^r$ while no element of $S_m \wr_r S_r$ moves fewer; hence $g(m, r, l) \leqslant \mu(P)/2$. It is certainly true that $m^{mr} \geqslant \sqrt{k}$ and $|P| \leqslant m^{mr} r^r$, so since $g(m, r, l) \neq 1$ and $|T| \geqslant 60$, it follows that $(\dagger)$ is true if we can show that

$$2mr \log m + r \log r \leqslant g(m, r, l) \log 60 + C$$

for some absolute constant C. If $r \geqslant 3$, then this is true since $g(m, r, l) \geqslant m^{r-1}$; if $r = 2$ and $l \geqslant 2$, then then is true since $g(m, 2, l) \geqslant m^2$; and if $r = 1$ and $l \geqslant 3$, then this is true since $g(m, 1, l) \geqslant (m-3)^2/2$ (and since $l < m/2$ forces $m > 6$). Thus the cases when (r, l) is $(1, 2)$ or $(2, 1)$ remain; note that for either one, the left-hand side of equation $(\dagger)$ tends to infinity if T is fixed and m tends to infinity. We therefore establish equation $(*)$ instead.

Suppose that (r, l) is $(1, 2)$. Recall that P is S_m or A_m acting (faithfully) on the set $\Omega_{m,2}$ of 2-subsets of $[m]$ where $m \geqslant 5$. Then $f_p(P) \leqslant m^2$ by Lemma 3.3.2. But $m \geqslant \sqrt{k}$, so equation $(*)$ will be true if we can show that $|\pi^P| 60^{r_\pi - k}$ is bounded above by m^{-3} for each $\pi \in R(P)$. To this end, let π be an element of P of prime order p. Then the full cycle decomposition of π in S_m consists of t cycles of length p for some t such that $1 \leqslant t \leqslant \lfloor m/p \rfloor$. Certainly $|\pi^P| \leqslant m^{pt}$. Moreover, we have $k - r_\pi = (1 - 1/p)(k - f_\pi) \geqslant (k - f_\pi)/2$ and $\log 60 > 4$, so it suffices to show that $(pt + 3) \log m \leqslant 2(k - f_\pi)$. Let i and j be distinct points of $[m]$. Clearly π fixes $\{i, j\}$ if and only if either both i and j are members of $\mathrm{fix}_{[m]}(\pi)$, or the full cycle decomposition of π in S_m contains the transposition

(ij). Hence

$$f_\pi = |\operatorname{fix}_{\Omega_{m,2}}(\pi)| = \begin{cases} \binom{m-pt}{2} & \text{if } p \geqslant 3, \\ \binom{m-2t}{2} + t & \text{if } p = 2. \end{cases}$$

By evaluating $2(k-f_\pi)$ and rearranging $(pt+3)\log m \leqslant 2(k-f_\pi)$, it follows that equation $(*)$ is true if

$$(pt+3)\log m + p^2t^2 + pt + \left\{ \begin{array}{ll} 0 & \text{if } p \geqslant 3 \\ 2t & \text{if } p = 2 \end{array} \right\} \leqslant 2mpt$$

for all primes p and integers t such that $1 \leqslant t \leqslant \lfloor m/p \rfloor$. This holds if $p = 2$ and $t = 1$, so we assume otherwise. Then $pt + 3 \leqslant 2pt$, and since $\log m \leqslant m/3$, we obtain that $(pt+3)\log m \leqslant 2mpt/3$. Clearly $pt + 1 \leqslant m + 1 \leqslant 4m/3$, and this implies that $p^2t^2 + pt \leqslant 4mpt/3$, so we have the desired result when $p \neq 2$. Suppose then that $p = 2$. Note that if $m \geqslant 6$, then $2t + 2 \leqslant m + 2 \leqslant 4m/3$, and if $m = 5$, then $2t + 2 \leqslant 6 \leqslant 4m/3$. Hence $2^2t^2 + 4t \leqslant 8mt/3$, as desired.

The remaining case to consider is when (r, l) is $(2, 1)$. Recall that here P is a subgroup of $S_m^2 \rtimes C_2$ that contains A_m^2 and acts via the product action on $[m]^2$ for $m \geqslant 5$. Let $Q := S_m^2 \rtimes C_2$ and let τ denote the generator for C_2. First we determine the conjugacy classes of elements of prime order in Q.

Let $\mathcal{C}$ be the union of those elements of prime order in Q whose projection onto C_2 is trivial, and let $\mathcal{C}_\tau$ be the union of those elements of prime order in Q whose projection onto C_2 is τ. Then the elements in $\mathcal{C}$ with order p have the form (s_1, s_2) where s_1 and s_2 are elements of S_m such that $s_i^p = 1$ for both i and s_1 or s_2 is non-trivial, and the elements of $\mathcal{C}_\tau$ have the form $(s, s^{-1})\tau$ for any $s \in S_m$. Note that both $\mathcal{C}$ and $\mathcal{C}_\tau$ are unions of conjugacy classes of Q since $S_m^2 \trianglelefteq Q$. In fact, since $(s, u)^{-1}(s, s^{-1})\tau(s, u) = (u, u^{-1})\tau$ for any $s, u \in S_m$, it follows that $f_{\mathcal{C}_\tau}(Q) = 1$.

Let $(s_1, s_2) \in \mathcal{C}$. Since we may conjugate (s_1, s_2) by (u_1, u_2) or $(u_1, u_2)\tau$ for any $u_1, u_2 \in S_m$, it follows that $(s_1, s_2)^Q = (s_1^{S_m} \times s_2^{S_m}) \cup (s_2^{S_m} \times s_1^{S_m})$. Fix a prime $p \leqslant m$. Then in Q there are $m_p := \lfloor m/p \rfloor$ conjugacy classes $(s_1, s_1)^Q$ where s_1 has order p, and since $(s_1, s_2)^Q = (s_2, s_1)^Q$, there are $\binom{m_p+1}{2}$ conjugacy classes $(s_1, s_2)^Q$ where (s_1, s_2) has order p but s_1 and s_2 have a different number of p-cycles on $[m]$ (allowing for the identity, which has no p-cycles). This accounts for all of the elements in $\mathcal{C}$ with order p. Then since $m_p \leqslant m/2$ for any prime p, we obtain

$$f_{\mathcal{C}}(Q) = \sum_{\substack{2 \leqslant p \leqslant m \\ p \text{ prime}}} m_p + \binom{m_p + 1}{2} \leqslant \sum_{\substack{2 \leqslant p \leqslant m \\ p \text{ prime}}} \frac{m^2 + 6m}{8} \leqslant \frac{m^3 + 6m^2}{8}.$$

Thus $f_{\mathcal{C}}(Q) \leqslant (3/8)m^3$.

Since P has index at most 8 in Q, Lemma 3.3.1 implies that $f_{\mathcal{C}\cap P}(P) \leqslant 3m^3$ and that $f_{\mathcal{C}_\tau\cap P}(P) \leqslant 8$. But $m = \sqrt{k}$, so equation $(*)$ is true if $|\pi^P|60^{r_\pi - k}$ is at most a constant multiple of m^{-4} for all $\pi \in R(P) \cap \mathcal{C}$ and at most a constant multiple of m^{-1} for all $\pi \in R(P) \cap \mathcal{C}_\tau$ where both constants are absolute.

We prove the latter requirement first. Let $\pi \in \mathcal{C}_\tau \cap P$. Then $|\pi^P| \leqslant m^{m-1}$ since $|\mathcal{C}_\tau| = |S_m|$. Moreover, if $\pi = (s, s^{-1})\tau$, then the set of fixed points of π on $[m]^2$ is $\{(i, is) : i \in [m]\}$, so $2(k - r_\pi) = k - f_\pi = m^2 - m$. Since $2\log m \leqslant (m-1)\log 60$, we have that $|\pi^P|60^{r_\pi - k}$ is bounded above by m^{-1}, as desired.

Now let $\pi = (s_1, s_2)$ be an element of prime order p in $\mathcal{C} \cap P$, and suppose that for each i the full cycle decomposition of s_i in S_m consists of t_i p-cycles where $0 \leqslant t_i \leqslant \lfloor m/p \rfloor$ and t_1 or t_2 is non-zero. Then $|(s_1, s_2)^P| \leqslant 2|s_1^{S_m}||s_2^{S_m}| \leqslant 2m^{pt_1+pt_2}$. Moreover, the element (s_1, s_2) fixes $(i, j) \in [m]^2$ if and only if s_1 fixes i and s_2 fixes j, so $f_{(s_1,s_2)} = (m - pt_1)(m - pt_2)$. Again, since $k - r_\pi \geqslant (k - f_\pi)/2$ and $\log 60 > 4$, if we can show that

$$(pt_1 + pt_2 + 4)\log m + 2p^2 t_1 t_2 \leqslant 2m(pt_1 + pt_2),$$

then $|\pi^P|60^{r_\pi - k}$ is bounded above by $2m^{-4}$, as desired. Clearly $x := pt_1 + pt_2$ is at least 2, so $1/3 \leqslant x/(x+4)$, and $\log m/m$ is at most $1/3$, so $(x+4)\log m \leqslant mx$. Since $pt_i \leqslant m$ for both i, it follows that $2p^2 t_1 t_2 \leqslant mx$. This completes the proof. □

Chapter 4

The diagonal case

In this chapter, we study the bases of groups of diagonal type. Note that all of the material in this chapter has been published by the author [25], with the exceptions of Theorem 4.0.6 and part of Theorem 4.0.5.

Let T be a non-abelian simple group, and let k be an integer that is at least 2. A group of diagonal type G with socle T^k acts primitively on a set $\Omega(k, T)$ with degree $|T|^{k-1}$ and is a (not necessarily split) extension of T^k by a subgroup of $\mathrm{Out}(T) \times S_k$; precise definitions will be given in Section 4.1. The permutation group induced by the conjugation action of G on the k factors of T^k is called the top group of G and is denoted by P_G. The group P_G is either primitive in its action on k points, or possibly trivial when $k = 2$, and it plays a large part in determining the base size of G. Recall that if the top group P_G does not contain the alternating group A_k, then we necessarily have $k \geqslant 5$ since S_k and A_k are the only primitive permutation groups of degree k when $k = 3$ or $k = 4$, and the only permutation groups when $k = 2$.

Theorem 4.0.1. *Let G be a group of diagonal type with socle T^k for some non-abelian simple group T. If the top group P_G is not S_k or A_k, then $b(G) = 2$.*

This is the best result we could hope for since a group of diagonal type never has base size 1 by Lemma 2.3.3. The proof of Theorem 4.0.1 is constructive, though it depends on a non-constructive result of Seress [69] that determines exactly when a primitive permutation group has a regular orbit on the power set of the domain of its action. Note that as a consequence of [69], Lemma 4.2 of Gluck, Seress and Shalev [33] constructs a base of size 3 for a group of diagonal type whose top group is neither symmetric, nor alternating, nor of degree less than 32.

The situation is markedly different, however, when the top group P_G is either the symmetric group S_k or the alternating group A_k. Note that groups of diagonal type can be constructed for any non-abelian simple group T and for arbitrarily large k.

Theorem 4.0.2. *Let G be a group of diagonal type with socle T^k for some non-abelian simple group T where the top group P_G contains A_k. If $k \geqslant 3$ then*

$$b(G) = \left\lceil \frac{\log\ k}{\log |T|} \right\rceil + a_G,$$

where $a_G \in \{1, 2\}$ and $a_G = 1$ if $|T|^l < k \leqslant |T|^l + |T| - 1$ for some positive integer l. If $k = 2$, then $b(G) = 3$ when $P_G = 1$, and $b(G) \in \{3, 4\}$ otherwise.

Hence $b(G) \to \infty$ when $k \to \infty$ with $|T|$ fixed. We will see in Proposition 4.2.12 that if either $k = |T|$, or $\mathrm{Inn}(T)^k \rtimes S_k \leqslant G$ and k is $|T|^l$ or $|T|^l - 1$ for some positive integer l, then $a_G = 2$. Also, at the end of Section 4.2 we give examples when $k = 2$ and $P_G = S_2$ of two groups G with $b(G) = 3$ and two groups G with $b(G) = 4$ (see also Appendix A.1). Thus Theorem 4.0.2 is essentially best possible. However, it remains unclear precisely when the two possibilities occur. In particular, we do not know when $b(G) = 2$, though $2 < k < |T|$ is a necessary condition.

Theorems 4.0.1 and 4.0.2 also allow us to prove a conjecture of Pyber in the case of groups of diagonal type. Recall that as a result of Lemma 2.3.2, the base size of G is bounded below by $\lceil \log |G| / \log n \rceil$, and recall from the Introduction that Pyber [64] conjectured there exists an absolute constant c for which the base size of a primitive permutation group G of degree n is at most $c \log |G| / \log n$.

Theorem 4.0.3. *Let G be a group of diagonal type. Then G satisfies Pyber's conjecture. In fact,*

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

where n is the degree of G.

We remark that in Gluck, Seress and Shalev [33], a base for groups of diagonal type is constructed and it is claimed there that the argument can be improved to construct a base of size $\lceil \log |G| / \log n \rceil + 3$ (where G is a group of diagonal type with degree n), but the details of the proof of this weaker result are not given.

Let us now consider the probabilistic side of the theory. We have several results, all of which are proved using Lemma 3.2.1. Firstly, not only do groups of diagonal type whose top groups are not alternating or symmetric have bases of size 2 by Theorem 4.0.1, but

these groups also have the property that almost every pair of points forms a base. Note that the order of a group of diagonal type with socle T^k tends to infinity if and only if k or $|T|$ tend to infinity.

Theorem 4.0.4. *Let G be a group of diagonal type with socle T^k for some non-abelian simple group T, and suppose that the top group P_G is not S_k or A_k. Then the proportion of pairs of points from $\Omega(k,T)$ that are bases for G tends to 1 as $|G| \to \infty$.*

Similarly, we have a partial result that includes the case when the top group P_G contains the alternating group A_k. Note that Theorem 4.0.2 implies that if the top group contains A_k and $|T|$ is fixed as k tends to infinity, then G does not have base size 2, while if k is small enough with respect to $|T|$, then a base of size 2 is possible. This motivates the following result. One consequence of this result is that for any fixed k at least 5, there are only finitely many groups of diagonal type with a degree k top group that do not have base size 2.

Theorem 4.0.5. *Let G be a group of diagonal type with socle T^k for some non-abelian simple group T where $k \geqslant 5$. The proportion of pairs of points from $\Omega(k,T)$ that are bases for G tends to 1 if either k is fixed as $|G| \to \infty$, or $k^4 \leqslant |T|$ as $|G| \to \infty$.*

Lastly, we can say something when $2 \leqslant k \leqslant 4$ as well.

Theorem 4.0.6. *Let G be a group of diagonal type with socle T^k for some non-abelian simple group T. The proportion of b-tuples of points from $\Omega(k,T)$ that are bases for G tends to 1 as $|G| \to \infty$ if either $b = 3$ and $3 \leqslant k \leqslant 4$, or $b = 5$, $k = 2$ and the top group $P_G = 1$.*

This chapter is organised as follows. Section 4.1 describes the groups of diagonal type in detail. Theorems 4.0.1, 4.0.2 and 4.0.3 are then proved in Section 4.2: Theorem 4.0.1 follows from Propositions 4.2.3 and 4.2.7, while Theorem 4.0.2 essentially follows from Propositions 4.2.8, 4.2.10 and 4.2.12. The proof of Theorem 4.0.4 will take up most of Section 4.3, and Theorems 4.0.5 and 4.0.6 are proved at the end of that section. Note that Sections 4.2 and 4.3 are essentially independent of each other. Note also that most of the results in this chapter depend upon the CFSG.

4.1 Groups of diagonal type

The following definitions for groups of diagonal type may be found in [49]. Let k be an integer that is at least 2, and let T be a non-abelian simple group. Note that for

$\alpha \in \mathrm{Aut}(T)$, we write $\overline{\alpha}$ for the coset $\alpha\,\mathrm{Inn}(T)$. Then we define

$$\begin{aligned} W(k,T) &:= \{(\alpha_1,\ldots,\alpha_k)\pi \in \mathrm{Aut}(T) \wr_k S_k : \overline{\alpha}_1 = \overline{\alpha}_i \text{ for all } i \in [k]\},\\ D(k,T) &:= \{(\alpha,\ldots,\alpha)\pi \in \mathrm{Aut}(T) \wr_k S_k\},\\ \Omega(k,T) &:= (W(k,T) : D(k,T)),\\ A(k,T) &:= W(k,T) \cap \mathrm{Aut}(T)^k. \end{aligned}$$

Observe that $W(k,T) = A(k,T) \rtimes S_k$ and that $W(k,T)$ is an extension of T^k by $\mathrm{Out}(T) \times S_k$. Moreover, $W(k,T)$ acts faithfully on the right coset space $\Omega(k,T)$ since $\mathrm{Inn}(T)^k$ is the unique minimal normal subgroup of $W(k,T)$. If the context permits, we write D, W and Ω for $D(k,T)$, $W(k,T)$ and $\Omega(k,T)$ respectively.

We say that a group G has *diagonal type* if there exists an integer k and a non-abelian simple group T such that $\mathrm{Inn}(T)^k \leqslant G \leqslant W(k,T)$ and G acts primitively on $\Omega(k,T)$. Any such G has socle T^k and degree $|T|^{k-1}$.

Let G be a subgroup of $W(k,T)$ containing $\mathrm{Inn}(T)^k$. Then the primitivity of such a group is controlled by the *top group* P_G of G, which is the subgroup of S_k consisting of those $\pi \in S_k$ for which there exists $(\alpha_1,\ldots,\alpha_k) \in A(k,T)$ such that $(\alpha_1,\ldots,\alpha_k)\pi \in G$. Note that P_G is permutation isomorphic to the image of the action of G on $\{T_1,\ldots,T_k\}$ by conjugation, where T_i is the i-th direct factor of $\mathrm{Inn}(T)^k$, since for any $w := (\alpha_1,\ldots,\alpha_k)\pi \in W(k,T)$, we have $w^{-1}T_i w = T_{i\pi}$ for all $i \in [k]$. See [23, Theorem 4.5A] for a proof of the following result, which determines when a subgroup of $W(k,T)$ containing $\mathrm{Inn}(T)^k$ is primitive.

Proposition 4.1.1. *Let T be a non-abelian simple group and $k \geqslant 2$ an integer. If $\mathrm{Inn}(T)^k \leqslant G \leqslant W(k,T)$, then G is a group of diagonal type if and only if either*

(i) P_G is primitive on $[k]$, or

(ii) $k = 2$ and $P_G = \{1\}$.

Thus we are only interested in subgroups of $W(k,T)$ containing $\mathrm{Inn}(T)^k$ whose top groups have the form of (i) or (ii) in Proposition 4.1.1. In particular, we are interested in the group $W(k,T)$ itself since its top group is S_k.

Let us briefly examine Ω. Its elements have the form $\omega := D(\alpha_1,\ldots,\alpha_k)\pi$ for some $(\alpha_1,\ldots,\alpha_k)\pi \in W$. Now $(\alpha_i,\ldots,\alpha_i)\pi \in D(k,T)$ for any $i \in [k]$, so fixing i we see that $\omega = D(\alpha_{i\pi^{-1}}^{-1}\alpha_{1\pi^{-1}},\ldots,1,\ldots,\alpha_{i\pi^{-1}}^{-1}\alpha_{k\pi^{-1}})$ where 1 is in the i-th coordinate. Since $\overline{\alpha}_l = \overline{\alpha}_j$ for all l and j, elements of Ω actually have the form $D(\varphi_{t_1},\ldots,\varphi_{t_k})$, where for each $t \in T$, the map $\varphi_t : T \to T$ is defined to be conjugation by t. Moreover, every element of Ω has $|T|$ representatives in $\mathrm{Inn}(T)^k$, and for each element of Ω, we may choose one coordinate to be any element of $\mathrm{Inn}(T)$ should we wish to do so. In particular, fixing the same

coordinate and element of $\mathrm{Inn}(T)$ and allowing all $(k-1)$-tuples with entries in $\mathrm{Inn}(T)$ yields the $|T|^{k-1}$ elements of Ω.

4.2 Base sizes for groups of diagonal type

For this section, let G be a group of diagonal type with socle T^k where T is a non-abelian simple group. By Lemma 2.3.1 and the transitivity of G on Ω, there is no loss of generality in restricting our attention to those subsets of Ω that contain D. We begin by determining the pointwise stabiliser in G of any two element subset of Ω containing D.

Lemma 4.2.1. *Let $\omega := D(\varphi_{t_1}, \ldots, \varphi_{t_k}) \in \Omega$ and write $t^{i,j}$ for $t_i^{-1}t_j$. Then for any $j_0 \in [k]$, we have $G_\omega \cap D = \{(\alpha, \ldots, \alpha)\pi \in G : t^{i,j_0}\alpha = t^{i\pi,j_0\pi} \text{ for all } i \in [k]\}$.*

Proof. Fix $j_0 \in [k]$. Then $(\alpha, \ldots, \alpha)\pi \in G$ fixes ω if and only if $\varphi_{t_{j_0}}\alpha\varphi_{t_{j_0\pi}}^{-1} = \varphi_{t_i}\alpha\varphi_{t_{i\pi}}^{-1}$ for all $i \in [k]$. This is equivalent to $\varphi_{t^{i,j_0}}\alpha = \alpha\varphi_{t^{i\pi,j_0\pi}}$ for all $i \in [k]$. Evaluating this last expression at t for each $t \in T$, we see it is equivalent to the statement that $(t^{i,j_0}\alpha)(t^{i\pi,j_0\pi})^{-1}$ centralises $t\alpha$ for all $t \in T$. Since the centre of T is trivial, the proof is complete. □

Lemma 4.2.1 then has the following useful, easy corollary.

Lemma 4.2.2. *Suppose that $(\alpha, \ldots, \alpha)\pi \in G$ fixes $D(\varphi_{t_1}, \ldots, \varphi_{t_k}) \in \Omega$. If there exists $j_0 \in [k]$ for which t_{j_0} and $t_{j_0\pi}$ are trivial, then $t_i\alpha = t_{i\pi}$ for all $i \in [k]$.*

Lemma 4.2.1 motivates the following notation. For $\omega := D(\varphi_{t_1}, \ldots, \varphi_{t_k}) \in \Omega$, let $\mathcal{O}_\omega$ denote the $k \times k$ matrix whose (i,j)-th entry is the order of $t^{i,j} = t_i^{-1}t_j$. If $(\alpha, \ldots, \alpha)\pi \in G_\omega$, then since $t^{i,j_0}\alpha = t^{i\pi,j_0\pi}$ for all $i \in [k]$ and for any fixed $j_0 \in [k]$ by Lemma 4.2.1, the $j_0\pi$-th column of $\mathcal{O}_\omega$ must be a permutation of the entries of the j_0-th column. Note that $\mathcal{O}_\omega$ is a symmetric matrix whose diagonal entries are all 1.

Now we prove Theorem 4.0.1 for $k > 32$. The proof relies mainly on a theorem of Seress [69] that determines precisely when a regular orbit on the power set of the domain of a primitive action exists; his work is based on work by Cameron, Neumann and Saxl [19] who proved using the CFSG that such a regular orbit exists for all but finitely many degrees as long as the action is not the natural action of the symmetric or alternating group. Note that the result of [69] can be applied to [33, Lemma 4.2] of Gluck, Seress and Shalev to construct a base of size 3 for a group of diagonal type whose top group has degree at least 33 and does not contain the alternating group (and a larger base otherwise). However, the proof of Proposition 4.2.3 below proceeds somewhat differently to construct a base of size 2.

Proposition 4.2.3. *If $A_k \not\leqslant P_G$ and $k > 32$, then $b(G) = 2$.*

Proof. Since P_G is primitive and does not contain A_k, and also since $k > 32$, [69, Theorem 1] implies that $[k]$ can be partitioned into two non-empty subsets Δ and Γ such that the setwise stabiliser of Δ in P_G is trivial. Since the setwise stabiliser of Γ must then also be trivial, we may assume without loss of generality that $|\Delta| \geqslant |\Gamma|$. Clearly $|\Delta| \geqslant 4$, so we may partition Δ into two non-empty subsets Δ_1 and Δ_2 such that neither $|\Delta_1|$ nor $|\Delta_2|$ is $|\Gamma|$. Let x and y be generators for T, which is possible by [1], and define t_i to be 1 if $i \in \Delta_1$, x if $i \in \Delta_2$, and y if $i \in \Gamma$. Let $\omega := D(\varphi_{t_1}, \ldots, \varphi_{t_k})$.

Let $(\alpha, \ldots, \alpha)\pi$ be an element of G fixing ω. Define a function $g : \{1, \ldots, k\} \to \mathbb{N}$ by mapping i to the number of entries in column i of $\mathcal{O}_\omega$ that are 1, where $\mathcal{O}_\omega$ is as defined above. Writing $\Delta_3 = \Gamma$, we have $g(i) = |\Delta_j|$ if $i \in \Delta_j$. Then $g(i) \neq g(j)$ for all $i \in \Gamma$ and $j \in \Delta$, but $g(i) = g(i\pi)$ for all $i \in [k]$ since by Lemma 4.2.1 the entries of column $i\pi$ are a permutation of the entries of column i. Hence $\Gamma\pi = \Gamma$, so π is the identity. But then for any $i \in \Delta_1$, $t_{i\pi} = t_i = 1$, so by Lemma 4.2.2, α must fix both x and y and is therefore the identity. Thus $\{D, D(\varphi_{t_1}, \ldots, \varphi_{t_k})\}$ is a base for G. □

For k smaller than 32, we need some more lemmas. This first lemma will also be useful in the case when the top group is symmetric or alternating.

Lemma 4.2.4. *Let $t_1, \ldots, t_k$ denote elements of T such that at least two of the t_i are trivial, at least one is non-trivial, and if t_i and t_j are non-trivial and $i \neq j$ then $t_i \neq t_j$. If $(\alpha, \ldots, \alpha)\pi \in G$ fixes $D(\varphi_{t_1}, \ldots, \varphi_{t_k})$, then $t_i\alpha = t_{i\pi}$ for all $i \in [k]$.*

Proof. Let $\omega := D(\varphi_{t_1}, \ldots, \varphi_{t_k})$, and let r_i denote the order of t_i. Also, let m be the number of non-trivial t_i. To begin, assume that $t_i \neq 1$ if $i \in [m]$ and that $t_i = 1$ otherwise. Then

$$\mathcal{O}_\omega = \begin{pmatrix} A & B \\ B^T & 1_{k-m} \end{pmatrix},$$

where A is a symmetric $m \times m$ matrix whose diagonal entries are 1 and whose remaining entries are integers at least 2, B is an $m \times (k-m)$ matrix with i-th row $(r_i, \ldots, r_i)$, and 1_{k-m} is a $(k-m) \times (k-m)$ matrix in which every entry is 1. Since $k - m \geqslant 2$, columns $m+1$ through k each have at least two entries that are 1, and these are the only such columns; hence π must permute these columns, which implies that $t_{i\pi} = 1$ for $i \geqslant m+1$. The result then follows from Lemma 4.2.2. The proof of the general case is essentially the same since then the entries in each column of $\mathcal{O}_\omega$ will be a permutation of the entries in a column of the matrix above. □

A result of Malle, Saxl and Weigel [57] states that every finite non-abelian simple group other than $U_3(3)$ is generated by an involution and a strongly real element, which is an element that can be conjugated to its inverse by an involution. Since $U_3(3)$ is generated by an involution and an element of order 6 by [20], it follows that every finite non-abelian simple group is generated by two elements, one of which can be taken to be an involution. Since two involutions generate a dihedral group, the two generators must have different orders. This makes the next two lemmas useful. For $x, y \in T$, let $T(x, y)$ denote the set of non-trivial elements of T whose orders are different to the orders of x and y.

Lemma 4.2.5. *Suppose that $T = \langle x, y \rangle$ where x and y have different orders, and suppose that $k \geqslant 4$ and $P_G \neq S_k$. If P_G has base size at most $|T(x, y)| + 2$ in its action on $[k]$, then $b(G) = 2$.*

Proof. We may assume without loss of generality that $\{1, 2, \ldots, m\}$ is a base of minimal size for P_G. Since P_G is primitive and $P_G \neq S_k$, it follows that P_G contains no transpositions [23, Theorem 3.3A]; thus $k \geqslant m + 2$. Let $t_1 := x$, $t_2 := y$, $t_i := 1$ for $\max\{3, m + 1\} \leqslant i \leqslant k$, and when $m \geqslant 3$, choose $t_3, \ldots, t_m$ to be distinct elements of $T(x, y)$. Suppose that $(\alpha, \ldots, \alpha)\pi \in G$ fixes $D(\varphi_{t_1}, \ldots, \varphi_{t_k})$. Then the conditions of Lemma 4.2.4 are met, so $t_i\alpha = t_{i\pi}$ for all $i \in [k]$. But α preserves order, so α fixes x and y and is therefore the identity. Then since the t_i are distinct for $i \in [m]$, π is the identity on $[m]$. Hence π is the identity, and it follows that $\{D, D(\varphi_{t_1}, \ldots, \varphi_{t_k})\}$ is a base for G. □

There is a classical result of Bochert [7] from the nineteenth century which states that every primitive permutation group of degree k that does not contain A_k has a base of size at most $k/2$ (see [23, Theorem 3.3B] for a proof). This makes the following consequence of Lemma 4.2.5 possible.

Lemma 4.2.6. *Suppose that $T = \langle x, y \rangle$ where x and y have different orders, and let C be a non-trivial conjugacy class of T with minimal cardinality. If $A_k \not\leqslant P_G$ and $k \leqslant 2|C| + 4$, then $b(G) = 2$.*

Proof. Certainly $|C| \leqslant |T(x, y)|$ since 3 distinct primes divide $|T|$ by Burnside's $p^a q^b$ Theorem [42, Theorem 31.4], while P_G has a base of size at most $k/2$ by Bochert [7]. Thus the assumption that $k \leqslant 2|C| + 4$ implies that P_G has base size at most $|T(x, y)| + 2$ in its action on $[k]$. Note that $k \geqslant 5$ since $A_k \not\leqslant P_G$ and P_G is primitive. Hence we may apply Lemma 4.2.5. □

Proposition 4.2.7. *If $A_k \not\leqslant P_G$ and $k \leqslant 32$, then $b(G) = 2$.*

Proof. By Malle, Saxl and Weigel [57, Theorem B] and [20], T is generated by elements x and y with different orders. Recall that $p(T)$ denotes the minimal index of a proper subgroup of T. Then by Lemma 4.2.6, G has base size 2 if $32 \leqslant 2p(T) + 4$, so we may assume that $p(T) \leqslant 13$. Note that $|T| \leqslant 13!/2$ since T can be embedded in the alternating group on $p(T)$ points. If T is a classical group of Lie type, then values for $p(T)$ can be found in [59, 76], and if T is an exceptional group of Lie type, then values for $p(T)$ can be found in [73–75]. Of course $p(A_m) = m$, and if T is sporadic (and of order less than $13!/2$), then values for $p(T)$ can be found in [20]. Using these, we see that T must be one of $L_2(7)$, $L_2(8)$, $L_2(11)$, $L_3(3)$, M_{11}, M_{12} or A_m for $5 \leqslant m \leqslant 13$. However, it can be seen using [20] that, with the exception of A_5, none of these groups has a conjugacy class of size less than 13, and so $b(G) = 2$ by Lemma 4.2.6. Lastly, A_5 is $(2, 3)$-generated and has 24 elements of order 5, while P_G has a base of size at most $32/2$ by Bochert [7], so $b(G) = 2$ by Lemma 4.2.5. □

Together, Propositions 4.2.3 and 4.2.7 imply that $b(G) = 2$ when $A_k \nleqslant P_G$, which establishes Theorem 4.0.1. Note that Pyber's conjecture (Theorem 4.0.3) is therefore true when $A_k \nleqslant P_G$.

We now move on to consider those diagonal type groups G for which P_G does contain the alternating group A_k. Here it is readily seen that we will not always have base size 2: if $k > |T|$, then every element of $\Omega \setminus \{D\}$ is determined by a k-tuple of elements of T whose coordinates contain at least one repeat, and so $W(k, T)$ does not have base size 2. In fact, we will see that $b(G) \neq 2$ when $k \geqslant |T|$. We begin by constructing a base for G.

Proposition 4.2.8. *G has a base of size*

$$\left\lceil \frac{\log\left(k - |T| + 1\right)}{\log |T|} \right\rceil + 2$$

if $k > |T|$, and a base of size 3 if $5 \leqslant k \leqslant |T|$.

Proof. Assume that $k \geqslant 5$. Then $m := \min\left(|T| - 1, k - 2\right)$ is at least 3. Define the positive integer

$$r := \begin{cases} \left\lceil \frac{\log\left(k - |T| + 1\right)}{\log |T|} \right\rceil & \text{if } \ k > |T|, \\ 1 & \text{if } \ k \leqslant |T|. \end{cases}$$

For j such that $m < j \leqslant k$, let $d_{j,0}, \ldots, d_{j,r-1}$ denote the first r digits of the base $|T|$ representation of $j - m - 1$; this is reasonable since $|T|^{r-1} \leqslant k - m - 1 < |T|^r$. Let x and y be generators for T [1]. Since $|T|$ is divisible by at least 3 distinct primes by Burnside's $p^a q^b$ Theorem [42, Theorem 31.4], we may choose some non-trivial z from T whose order

is different to that of x and y. Enumerating the elements of T as $t_0, \ldots, t_{|T|-1}$ where $t_0 := 1$, $t_1 := x$, $t_2 := y$ and $t_3 := z$, we may define

$$u_{i,j} := \begin{cases} t_j & \text{if } i = 2 \text{ and } 1 \leqslant j \leqslant m, \\ x & \text{if } i = 3 \text{ and } j = 1, \\ z & \text{if } i = 3 \text{ and } j = 2, \\ t_{d_{j,i-3}} & \text{if } 3 \leqslant i \leqslant r+2 \text{ and } m < j \leqslant k, \\ 1 & \text{otherwise,} \end{cases}$$

where $1 \leqslant i \leqslant r+2$ and $1 \leqslant j \leqslant k$. For $i \in [r+2]$, let ω_i denote the element $D(\varphi_{u_{i,1}}, \ldots, \varphi_{u_{i,k}})$ of Ω. We claim that $\mathscr{B} := \{\omega_1, \ldots, \omega_{r+2}\}$ is a base for G. Note that $|\mathscr{B}| = r+2$, for if $\omega_i = \omega_{i'}$ for some distinct i and i', then there exists $t \in T$ for which $u_{i,j} = tu_{i',j}$ for all j. But then we must have $i, i' \geqslant 4$, which implies that $t = 1$, and so $d_{j,i-3} = d_{j,i'-3}$ for every $j > m$. This is certainly not the case; for example, take $j = |T|^{i-3} + m + 1$.

Let $(\alpha, \ldots, \alpha)\pi$ be an element of G_{ω_1} that fixes ω_i for all $2 \leqslant i \leqslant r+2$. Since $u_{2,1}, \ldots, u_{2,k}$ satisfy the conditions of Lemma 4.2.4, we get that $u_{2,j}\alpha = u_{2,j\pi}$ for all $j \in [k]$, and so $[m]\pi = [m]$. Now $u_{2,3} = z$ has order different to that of $u_{2,1} = x$ and $u_{2,2} = y$, so $3 \leqslant 3\pi \leqslant m$. Hence $u_{3,3\pi} = 1 = u_{3,3}$, which implies that $u_{3,j}\alpha = u_{3,j\pi}$ for all $j \in [k]$ by Lemma 4.2.2. But $1\pi \leqslant m$, so $u_{3,1\pi} \in \{x, z, 1\}$; this together with the fact that $u_{3,1}\alpha = u_{3,1\pi}$ forces $1\pi = 1$. Similarly, $2\pi = 2$, but then $u_{2,j}\alpha$ equalling $u_{2,j\pi}$ for $j \in \{1, 2\}$ implies that $x\alpha = x$ and $y\alpha = y$, so α is the identity. Moreover, for any $i \geqslant 4$ we have that $u_{i,1\pi} = u_{i,1} = 1$, so it follows from Lemma 4.2.2 that $u_{i,j\pi} = u_{i,j}$ for all i and j. In other words, for every $j \in [k]$, the j-th and $j\pi$-th columns of the $(r+2) \times k$ matrix whose (i,j)-th entry is $u_{i,j}$ are the same. However, by construction columns $1, \ldots, m$ are distinct from one another, as are columns $m+1, \ldots, k$. Recalling that $[m]\pi = [m]$, it follows that π is the identity. □

Note that the CFSG was only used in the proof above to obtain that T is 2-generated. This assumption can be removed if k is sufficiently larger than $|T|$: let $x_1, \ldots, x_s$ be a set of generators for T, and in the construction of $\mathscr{B}$ above, change x to x_1, y to x_2, and $u_{i+1,2}$ to x_i for $3 \leqslant i \leqslant s$. The proof remains unchanged until we obtain $x_1\alpha = x_1$ and $x_2\alpha = x_2$. Since $u_{i,1\pi} = u_{i,1} = 1$ for $i \geqslant 4$, Lemma 4.2.2 implies that $u_{i,j}\alpha = u_{i,j\pi}$ for all i and j, but $2\pi = 2$, so $x_i\alpha = x_i$ for all i. The remainder of the proof is the same. To get a crude idea of how large k needs to be, note that T has a generating set of size at most $\log_2 |T|$ (as any finite group does), so we need $\log_2 |T| + 1$ to be at most $r+2$ for this argument to work. Hence for $k \geqslant |T|^{\log_2 |T|}$, the upper bound on the base size of G

in Proposition 4.2.8 can be obtained without the CFSG.

Now we consider small values for k. The following will be used when $k = 2$.

Lemma 4.2.9. *If $\{D, D(\varphi_{t_1}, \ldots, \varphi_{t_k})\}$ is a base of size 2 for G, then $\bigcap_{i=1}^{k} C_T(t_i) = \{1\}$.*

Proof. If $t \in \bigcap_{i=1}^{k} C_T(t_i)$, then $(t_i^{-1}t_1)\varphi_t = t_i^{-1}t_1$ for all $i \in [k]$. But $(\varphi_t, \ldots, \varphi_t) \in G$, and $(\varphi_t, \ldots, \varphi_t)$ fixes $D(\varphi_{t_1}, \ldots, \varphi_{t_k})$ by Lemma 4.2.1, so $t = 1$. □

Proposition 4.2.10. *If $P_G = A_k$, then $b(G) = 3$ when $k = 2$, and $b(G) = 2$ when k is 3 or 4. If $P_G = S_k$, then $b(G) \in \{3, 4\}$ when $k = 2$, and $b(G) \in \{2, 3\}$ when k is 3 or 4.*

Proof. Let x and y be generators for T [1]. First assume that $k = 2$. Then either $\{D, D(\varphi_x, 1), D(\varphi_y, 1)\}$ or $\{D, D(\varphi_x, 1), D(\varphi_y, 1), D(\varphi_{xy}, 1)\}$ is a base for G when P_G is 1 or S_2 respectively by Lemma 4.2.1. Moreover, $b(G) \neq 2$ in these cases since $\{D, D(\varphi_t, 1)\}$ is not a base for G for any $t \in T$ by Lemma 4.2.9. Let z be a non-trivial element of T with order different to that of x, and suppose that $k = 3$ or $k = 4$. Then Lemma 4.2.4 implies that $\{D, D(\varphi_x, 1, 1), D(1, \varphi_y, 1)\}$ or $\{D, D(\varphi_x, \varphi_z, 1, 1), D(1, 1, \varphi_y, 1)\}$ is a base for G when P_G is S_3 or S_4 respectively. Since the natural action of A_4 has base size 2, it follows from Lemma 4.2.5, [57, Theorem B] and [20] that $b(G) = 2$ when $k = 4$ and $P_G = A_4$. This leaves us with the case $k = 3$ and $P_G = A_3$. By [57, Theorem B] and [20], we may assume that y is an involution. Then a consideration of the matrix $\mathcal{O}_{D(\varphi_x, \varphi_y, 1)}$ shows that $\{D, D(\varphi_x, \varphi_y, 1)\}$ is a base for G. □

We are now able to prove Pyber's conjecture for groups of diagonal type.

Proof of Theorem 4.0.3. Let G be a group of diagonal type with socle T^k. Note that $k^k/e^{k-1} \leqslant k!$ since $\log k! = \sum_{x=2}^{k} \log x \geqslant \int_1^k \log x \, dx = \log(k^k/e^{k-1})$. If $A_k \leqslant P_G$, then

$$\left(\frac{k|T|}{e}\right)^{k-1} \leqslant \frac{1}{2}\left(\frac{k^k}{e^{k-1}}\right)|T|^{k-1} \leqslant |P_G||T|^{k-1} \leqslant |G_D||T|^{k-1} = |G|,$$

from which we obtain

$$\frac{\log\left(k|T|/e\right)}{\log|T|} \leqslant \frac{\log|G|}{\log|T|^{k-1}}.$$

But $k - |T| + 1 \leqslant k|T|/e$, so when $A_k \leqslant P_G$ and $k > |T|$, Proposition 4.2.8 implies that G satisfies Pyber's conjecture and, in particular, the bound in the statement of Theorem 4.0.3. Since $b(G)$ is constant and at most 4 when $A_k \not\leqslant P_G$ or $k \leqslant |T|$ by Propositions 4.2.3, 4.2.7, 4.2.8 and 4.2.10, and since we always have $\lceil \log|G| / \log|T|^{k-1} \rceil \geqslant 2$, the proof is complete. □

In fact, since $\log|G|/\log|T|^{k-1} \leqslant b(G)$ by Lemma 2.3.2, this proof provides a lower bound for $b(G)$ whose value is the case $a_G = 1$ of Theorem 4.0.2 when $e|T|^l < k \leqslant |T|^{l+1}$ for some non-negative integer l. However, this can be improved upon. To do so, we need to know more about the structure of G.

Lemma 4.2.11. *If $A_k \leqslant P_G$ and there exists an odd integer s with $1 < s \leqslant k$ such that s is relatively prime to the order of every element of* $\mathrm{Out}(T)$*, then* $\mathrm{Inn}(T)^k \rtimes A_k \leqslant G$.

Proof. If π is an s-cycle, then $\pi \in A_k \leqslant P_G$, so $(\alpha, \ldots, \alpha)\pi \in G$ for some $\alpha \in \mathrm{Aut}(T)$ whose image $\overline{\alpha}$ in $\mathrm{Out}(T)$ has order r, say. Certainly $(\alpha^r, \ldots, \alpha^r)\pi^r \in G$, but G contains $\mathrm{Inn}(T)^k$, so π^r is an element of G. Hence π is as well. As π was an arbitrary s-cycle, the group G contains every s-cycle. But the s-cycles generate A_k, so $\mathrm{Inn}(T)^k \rtimes A_k \leqslant G$. □

The next result provides a lower bound on $b(G)$ that will allow us to prove that $b(G) \geqslant \lceil \log k/\log|T| \rceil + 1$ for Theorem 4.0.2. In fact, several other lower bounds are proved under somewhat specialised conditions; this is done to show that Theorem 4.0.2 is essentially best possible.

Proposition 4.2.12. *Suppose that $A_k \leqslant P_G$, and let l be a positive integer. Suppose that either $k > |T|^l$, or $l = 1$ and $k = |T|$, or $\mathrm{Inn}(T)^k \rtimes S_k \leqslant G$ and k is $|T|^l$ or $|T|^l - 1$. Then $b(G) \geqslant l + 2$.*

Proof. Suppose that one of the four assumptions on k and G in the statement of the proposition is true. Then certainly $k \geqslant |T| - 1$, but $|\mathrm{Out}(T)|$ is much smaller than $|T|$ by the CFSG; see Lemma 3.1.3, for example, so we may take the s of Lemma 4.2.11 to be $|\mathrm{Out}(T)|+1$ if $|\mathrm{Out}(T)|$ is even and $|\mathrm{Out}(T)|+2$ otherwise. Thus $\mathrm{Inn}(T)^k \rtimes A_k \leqslant G$.

For ease of notation, let $\mathscr{C}$ denote the set of the $|T|^l$ columns of length l with entries in T, and for M an $l \times m$ matrix with entries in T, let $\mathscr{C}_M$ denote the subset of $\mathscr{C}$ whose elements are the columns of M. Note that $\mathrm{Aut}(T)$ acts naturally on $\mathscr{C}$. Suppose that the columns of M are pairwise distinct. If $\mathscr{C}_M^\alpha = \mathscr{C}_M$ for some $\alpha \in \mathrm{Aut}(T)$, then α determines a permutation on $[m]$; this we denote by $\pi_{\alpha,M}$. Observe that for each row $(t_1, \ldots, t_m)$ of M, we have $t_i\alpha = t_{i\pi_{\alpha,M}}$ for all $i \in [m]$.

Choose l distinct elements $\omega_1, \ldots, \omega_l$ from $\Omega \setminus \{D\}$, and let $\mathscr{B}$ be the set $\{\omega_i : 1 \leqslant i \leqslant l\}$. We must show that $\mathscr{B}$ is not a base for G_D. For each i, let $(t_{i,1}, \ldots, t_{i,k})$ be one of the $|T|$ choices of k-tuples of elements in T that correspond to ω_i. Let B be the $l \times k$ matrix whose (i,j)-th entry is $t_{i,j}$. Note that for each i, $(t, \ldots, t)\omega_i = \omega_i$ for any $t \in T$. This allows us either to choose one element from $\mathscr{C}$ to be column j of B for any one $j \in [k]$,

or, when an element of $\mathscr{C}$ is not in $\mathscr{C}_B$, to choose any one element from $\mathscr{C}$ to be in $\mathscr{C} \setminus \mathscr{C}_B$ (with appropriate repercussions for the columns of B in either case).

Suppose that B has three identical columns, say j_1, j_2 and j_3. Then $(1, \dots, 1)(j_1\ j_2\ j_3)$ is an element of G_D that fixes $\mathscr{B}$ pointwise, so $\mathscr{B}$ is not a base for G_D. Similarly, if B has two pairs of identical columns, then $\mathscr{B}$ is not a base for G_D, so we may assume that neither scenario occurs in B. In particular, $k \leqslant |T|^l + 1$.

Suppose that B has exactly one pair of repeated columns. By relabelling if necessary, we may assume that the indices of these columns are $k-1$ and k. If $\mathrm{Inn}(T)^k \rtimes S_k \leqslant G$, then clearly $\mathscr{B}$ is not a base for G_D, so assume otherwise, in which case $k = |T|^l + 1$, or $l = 1$ and $k = |T|$. Then $\mathscr{C}_B$ is $\mathscr{C}$ in the former case and $\mathscr{C} \setminus \{(t)\}$ for some $t \in T$ in the latter. We may assume by the note above that every entry of column $k-1$ is the identity, and therefore the same is true for column k. Let B^* be the $l \times (k-2)$ matrix whose j-th column is the j-th column of B for $j \in [k-2]$. If $k = |T|^l + 1$, let α be any non-trivial element of $\mathrm{Inn}(T)$, and if $l = 1$ and $k = |T|$, let α be any non-trivial element of $\mathrm{Inn}(T)$ that fixes t. Then $\mathscr{C}^\alpha_{B^*} = \mathscr{C}_{B^*}$ in either case. Since the columns of B^* are pairwise distinct by assumption, the permutation π_{α,B^*} on $[k-2]$ exists as defined above. Moreover, π_{α,B^*} can be made into an even permutation π of $[k]$ by either fixing or interchanging $k-1$ and k. Then $(\alpha, \dots, \alpha)\pi \in G_D$. Since $t_{i,j}\alpha = t_{i,j\pi}$ for all i and j, Lemma 4.2.1 implies that $(\alpha, \dots, \alpha)\pi$ fixes $\mathscr{B}$ pointwise. Thus $\mathscr{B}$ is not a base for G_D.

Hence we may assume that the columns of B are pairwise distinct. Then $k \leqslant |T|^l$. If $k = |T|^l$, then $\mathscr{C}_B = \mathscr{C}$, and if $k = |T|^l - 1$, then $\mathscr{C}_B = \mathscr{C} \setminus \{c\}$ for some $c \in \mathscr{C}$; we may assume that all of the entries of c are the identity. Let α be an element of $\mathrm{Inn}(T)$ for which $\alpha^2 \neq 1$. Then $\mathscr{C}^\alpha_B = \mathscr{C}_B$ in either case. Again, since the entries of B are pairwise distinct, we have a permutation $\pi := \pi_{\alpha,B}$ of $[k]$. Since $t_{i,j}\alpha = t_{i,j\pi}$ for all i and j, Lemma 4.2.1 implies that $(\alpha, \dots, \alpha)\pi \in D$ fixes $\mathscr{B}$ pointwise; hence the non-trivial element $(\alpha, \dots, \alpha)^2\pi^2$ of $\mathrm{Inn}(T)^k \rtimes A_k$ does so as well, and thus $\mathscr{B}$ is not a base for G_D. □

Proof of Theorem 4.0.2. By Propositions 4.2.8 and 4.2.10, we have the desired result if $k \leqslant |T|$, so we may assume that $|T|^l < k \leqslant |T|^{l+1}$ for some positive integer l. It follows immediately from Proposition 4.2.8 that $b(G) \leqslant \lceil \log k / \log |T| \rceil + 2$. Moreover, $b(G) \geqslant l + 2$ by Proposition 4.2.12, so $b(G) \geqslant \lceil \log k / \log |T| \rceil + 1$. If we also assume that $k \leqslant |T|^l + |T| - 1$, then the upper bound of Proposition 4.2.8 is equal to $\lceil \log k / \log |T| \rceil + 1$ since $k > |T|^l$ implies that $k - |T| + 1 > |T|^{l-1}$, so $a_G = 1$ and the proof is complete. □

Note that Proposition 4.2.12 provides several infinite classes of groups for which the a_G of Theorem 4.0.2 is 2; namely, $a_G = 2$ when $k = |T|$ or when G contains $\mathrm{Inn}(T)^k \rtimes S_k$

and k is $|T|^l$ or $|T|^l - 1$ for any positive integer l. Additionally, it can be shown that if $m = 5$ or $m = 6$, then $b(\mathrm{Inn}(A_m)^2 \rtimes S_2) = 3$ while $b(W(2, A_m)) = 4$. This can be proved using GAP [30]; see Appendix A.1. Thus Theorem 4.0.2 is essentially best possible.

Furthermore, Proposition 4.2.12 implies that $b(G) \neq 2$ when $k \geqslant |T|$, and if $2 < k < |T|$, then we know that $b(G) \in \{2, 3\}$ by Propositions 4.2.8 and 4.2.10. At this stage, it remains unclear whether we can determine when $b(G) = 2$ more precisely than this. The main difficulty here lies with the possibility of the existence of two groups of diagonal type with the same socle and top group but different base sizes; indeed, none of the methods we have seen so far can distinguish the base sizes of two such groups. However, we will see in Section 4.3 that for a particular fixed k that is at least 5, there are only finitely many groups of diagonal type with a degree k top group that do not have base size 2.

4.3 Probabilistic results

For this section, let T be a non-abelian simple group and $k \geqslant 2$ an integer. We begin by defining some notation that will facilitate the use of Lemma 3.2.1, which bounds the proportion of b-tuples not forming bases for a given group.

Let G be a group of diagonal type with socle T^k and $R(G)$ a set of representatives for the G-conjugacy classes of elements with prime order in the stabiliser G_D of D in G. Let

$$\begin{aligned}
R_1(G) &:= \{(\alpha, \dots, \alpha)\pi \in R(G) : \pi \text{ is fixed-point-free on } [k]\},\\
R_2(G) &:= \{(\alpha, \dots, \alpha)\pi \in R(G) : \pi = 1\},\\
R_3(G) &:= \{(\alpha, \dots, \alpha)\pi \in R(G) : \pi \neq 1 \text{ and } i\pi = i \text{ for some } i \in [k]\},
\end{aligned}$$

and for $1 \leqslant i \leqslant 3$, let

$$r_i(G, b) := \sum_{x \in R_i(G)} \frac{|x^G \cap G_D|^b |C_G(x)|^{b-1}}{|G|^{b-1}}.$$

Recall the definition of $Q(G, b)$ from Section 3.2. Then

$$Q(G, b) \leqslant r_1(G, b) + r_2(G, b) + r_3(G, b)$$

for all integers $b \geqslant 1$ by Lemma 3.2.1. For simplicity, we write $r_i(G)$ for $r_i(G, 2)$ for all $1 \leqslant i \leqslant 3$, and we write $\overrightarrow{\alpha}$ for the tuple $(\alpha, \dots, \alpha)$. As in Section 3.2, we also write C for some absolute constant that need not and will not be determined (though it could be), and we apply the same methodology to another absolute constant $c > 1$, though it will be obvious what c needs to be.

We need to prove the following three lemmas. For the second, recall that $p(T)$ denotes the minimal index of a proper subgroup of T.

Lemma 4.3.1. *Let P be a primitive subgroup of S_k that does not contain A_k, and let $G := A(k,T) \rtimes P$. Then*

$$r_1(G) \leqslant \frac{C}{c^k |T|^{\frac{1}{6}}}$$

for some absolute constants C and $c > 1$.

Lemma 4.3.2. *Let P be a primitive subgroup of S_k where $k \geqslant 5$, and let $G := A(k,T) \rtimes P$. Then*

$$r_2(G) \leqslant \frac{C}{p(T)^{k-\frac{19}{4}}}$$

for some absolute constant C.

Lemma 4.3.3. *Let P be a primitive subgroup of S_k that does not contain A_k, and let $G := A(k,T) \rtimes P$. Then*

$$r_3(G) \leqslant \frac{C}{|T|^{\frac{1}{3}}} \left(\frac{1}{c^k} + \frac{1}{\sqrt{k}} \right)$$

for some absolute constants C and $c > 1$.

If we assume that Lemmas 4.3.1, 4.3.2 and 4.3.3 are true, then Theorem 4.0.4 can be proved easily, as we now see.

Proof of Theorem 4.0.4. Note that $k \geqslant 5$ since for $k \leqslant 4$ the only primitive permutation groups of degree k are S_k and A_k. Then by Lemmas 3.2.1, 4.3.1, 4.3.2 and 4.3.3,

$$Q((A(k,T) \rtimes P_G), 2) \leqslant C \left(\frac{1}{c^k |T|^{\frac{1}{6}}} + \frac{1}{p(T)^{k-\frac{19}{4}}} + \frac{1}{|T|^{\frac{1}{3}} c^k} + \frac{1}{|T|^{\frac{1}{3}} \sqrt{k}} \right)$$

for some absolute constants C and $c > 1$. Because T can be embedded in the alternating group on $p(T)$ points, it follows that $p(T) \to \infty$ as $|T| \to \infty$. Thus $Q((A(k,T) \rtimes P_G), 2)$ converges to 0 as $|T| \to \infty$ or $k \to \infty$. Since $G \leqslant A(k,T) \rtimes P_G \leqslant W(k,T)$, any base for $A(k,T) \rtimes P_G$ is also a base for G. Thus $Q(G,2) \leqslant Q((A(k,T) \rtimes P_G), 2)$. Also, clearly $|G| \leqslant |\operatorname{Aut}(T)||T|^{k-1}|P_G| \leqslant |T|!|T|^{k-1}k!$, so $|T| \to \infty$ or $k \to \infty$ when $|G| \to \infty$. Thus $Q(G,2)$ will indeed converge to 0 as $|G|$ tends to infinity. □

In order to prove the three lemmas, we first need to calculate the sizes of conjugacy classes and centralisers of various elements of $D(k,T)$.

Lemma 4.3.4. *Let P be a subgroup of S_k, let $G := A(k,T) \rtimes P$, and let $(\alpha, \dots, \alpha)\pi \in G$ where π has a fixed point on $[k]$. Then*

$$(\alpha, \dots, \alpha)\pi^G \cap G_D = \{(\alpha', \dots, \alpha')\pi' : \alpha' \in \alpha^{\operatorname{Aut}(T)}, \pi' \in \pi^P\}.$$

In particular, $|(\alpha, \dots, \alpha)\pi^G \cap G_D| = |\alpha^{\operatorname{Aut}(T)}||\pi^P|$.

Proof. Suppose that $\alpha' := \beta^{-1}\alpha\beta$ for any $\beta \in \mathrm{Aut}(T)$ and $\pi' := \sigma^{-1}\pi\sigma$ for any $\sigma \in P$. Then $(\beta, \dots, \beta)\sigma$ conjugates $(\alpha, \dots, \alpha)\pi$ to $(\alpha', \dots, \alpha')\pi'$ in G. On the other hand, if $(\alpha_1, \dots, \alpha_k)\sigma$ conjugates $(\alpha, \dots, \alpha)\pi$ to $(\alpha', \dots, \alpha')\pi'$ in G, then $\sigma^{-1}\pi\sigma = \pi'$ and $\alpha_i^{-1}\alpha\alpha_{i\pi} = \alpha'$ for all $i \in [k]$. Since π has a fixed point, the result follows. □

The proof of Lemma 4.3.4 should give the reader some indication of why it is not only convenient to work with the group $A(k,T) \rtimes P$ but also necessary, as we lose control of the sizes of $R_2(G)$ and $R_3(G)$ for an arbitrary group of diagonal type G.

Lemma 4.3.5. *Let P be a subgroup of S_k, let $G := A(k,T) \rtimes P$, and let $(\alpha, \dots, \alpha)\pi$ be an element of G of prime order p. Then*

$$|C_G((\alpha, \dots, \alpha)\pi)| = |C_P(\pi)||C_{\mathrm{Out}(T)}(\overline{\alpha})||T|^{\frac{k}{p}}$$

when π is fixed-point-free on $[k]$, and

$$|C_G((\alpha, \dots, \alpha)\pi)| = |C_P(\pi)||C_{\mathrm{Aut}(T)}(\alpha)||C_{\mathrm{Inn}(T)}(\alpha)|^{\mathrm{fix}_{[k]}(\pi)-1}|T|^{\frac{1}{p}(k-\mathrm{fix}_{[k]}(\pi))}$$

when π has a fixed point on $[k]$.

Note that the division into two cases in Lemma 4.3.5 is necessary because there exist $\alpha, \beta \in \mathrm{Aut}(T)$ for which $\overline{\beta} \in C_{\mathrm{Out}(T)}(\overline{\alpha})$ but $\beta \notin C_{\mathrm{Aut}(T)}(\alpha)$. In fact, if π is fixed-point-free, then the two expressions for $|C_G((\alpha, \dots, \alpha)\pi)|$ agree precisely when $C_{\mathrm{Aut}(T)}(\alpha)/C_{\mathrm{Inn}(T)}(\alpha)$ is isomorphic to $C_{\mathrm{Out}(T)}(\overline{\alpha})$.

Proof. Let $f_\pi := \mathrm{fix}_{[k]}(\pi)$, let c_π be the number of non-trivial cycles of π so that $c_\pi = (k - f_\pi)/p$, and let $r_\pi := c_\pi + f_\pi$. The element $(\alpha_1, \dots, \alpha_k)\sigma \in \mathrm{Aut}(T)^k \wr_k S_k$ is in G and centralises $(\alpha, \dots, \alpha)\pi$ if and only if all three of the following conditions occur: σ centralises π in P, $\alpha^{-1}\alpha_i\alpha = \alpha_{i\pi}$ for all $i \in [k]$, and α_i and α_j are in the same coset of $\mathrm{Inn}(T)$ for all i and j. There are precisely $|C_P(\pi)|$ elements of P satisfying the first condition, and this condition is independent from the other two, so we assume that σ is fixed and count how many occurrences of the latter conditions are possible.

If α is trivial, then $\alpha^{-1}\alpha_i\alpha = \alpha_{i\pi}$ for all $i \in [k]$ if and only if $\alpha_i = \alpha_j$ whenever i and j are in the same cycle of the full cycle decomposition of π. Thus there are $|\mathrm{Out}(T)||T|^{r_\pi}$ k-tuples $(\alpha_1, \dots, \alpha_k)$ satisfying both conditions. The desired equality then follows in either case for π, so we may assume that α is non-trivial, in which case α has prime order p.

Suppose, first of all, that i_0 is moved by π. Then i_0 is contained in a p-cycle in the full cycle decomposition of π as π must have the same prime order as α. Let us assume that this p-cycle is $(12\cdots p)$ and that i_0 is 1. If $\alpha^{-1}\alpha_i\alpha = \alpha_{i\pi}$ and $\overline{\alpha}_1 = \overline{\alpha}_i$ for all i, then,

in particular, $[\alpha_1, \alpha] \in \mathrm{Inn}(T)$ and the elements $\alpha_2, \ldots, \alpha_p$ are determined by α_1 and α. Conversely, if we are given $\alpha_1 \in \mathrm{Aut}(T)$ such that $[\alpha_1, \alpha] \in \mathrm{Inn}(T)$, define $\alpha_{i+1} := \alpha^{-i}\alpha_1\alpha^i$ for each $i \in [p-1]$. Then $\alpha^{-1}\alpha_i\alpha = \alpha_{i\pi}$ for all $i \in [p]$ since α has order p. Moreover, $[\alpha_1, \alpha^i] \in \mathrm{Inn}(T)$ for all $i \in [p]$ since $[\alpha_1, \alpha^i] = [\alpha_1, \alpha^{i-1}]\alpha^{1-i}[\alpha_1, \alpha]\alpha^{i-1}$ for all such i; thus $\overline{\alpha}_1 = \overline{\alpha}_i$ for all $i \in [p]$. Since this argument does not depend on the choice of i_0 or on the letters of the p-cycle, and since for $\beta \in \mathrm{Aut}(T)$, the commutator $[\beta, \alpha] \in \mathrm{Inn}(T)$ if and only if $\overline{\beta} \in C_{\mathrm{Out}(T)}(\overline{\alpha})$, it follows that there are at most $|C_{\mathrm{Out}(T)}(\overline{\alpha})|$ choices for the coset of $\mathrm{Inn}(T)$ from which the α_i can be chosen, and for each such coset there are at most $|T|$ choices corresponding to each non-trivial cycle of π. If π is fixed-point-free, then all of these choices are possible. Hence $|C_G((\alpha, \ldots, \alpha)\pi)| = |C_P(\pi)||C_{\mathrm{Out}(T)}(\overline{\alpha})||T|^{k/p}$.

Suppose then that π has a fixed point i_0. Certainly $\alpha^{-1}\alpha_i\alpha = \alpha_{i\pi}$ and $\overline{\alpha}_{i_0} = \overline{\alpha}_i$ for all fixed points i if and only if $\alpha_{i_0} \in C_{\mathrm{Aut}(T)}(\alpha)$ and $\alpha_{i_0}^{-1}\alpha_i \in C_{\mathrm{Inn}(T)}(\alpha)$ for all fixed points $i \neq i_0$. Hence there are at most $|C_{\mathrm{Aut}(T)}(\alpha)||C_{\mathrm{Inn}(T)}(\alpha)|^{f_\pi - 1}$ choices for $\{\alpha_i : i\pi = i\}$, and if π is trivial, then all of these choices are possible, and we obtain the desired result. Suppose that $\pi \neq 1$, and let $\{\alpha_i : i\pi = i\}$ be one of the choices described above. Then since $\overline{\alpha}_{i_0} \in C_{\mathrm{Out}(T)}(\overline{\alpha})$ for any i_0 fixed by π, any element of the coset $\overline{\alpha}_{i_0}$ can be chosen to determine the α_j corresponding to any non-trivial cycle of π as above. Thus each of the choices for $\{\alpha_i : i\pi = i\}$ not only occurs but does so $|T|^{c_\pi}$ times, as desired. □

We are now in a position to prove the three lemmas. We begin with Lemma 4.3.1.

Proof of Lemma 4.3.1. If $\overrightarrow{\alpha}\pi \in R_1(G)$ where π has prime order p, then k/p is an integer and is therefore bounded above by $\lfloor k/2 \rfloor$. Since $P = P_G$, Lemma 4.3.5 then implies that

$$\max_{\overrightarrow{\alpha}\pi \in R_1(G)} |C_G(\overrightarrow{\alpha}\pi)| \leqslant |\,\mathrm{Out}(T)||P||T|^{\lfloor \frac{k}{2} \rfloor}.$$

Note that $|G_D| = |\,\mathrm{Out}(T)||T||P|$ and $|G| = |G_D||T|^{k-1}$. Then

$$r_1(G) \leqslant \frac{|G_D|^2}{|G|} \max_{\overrightarrow{\alpha}\pi \in R_1(G)} |C_G(\overrightarrow{\alpha}\pi)| \leqslant \frac{|\,\mathrm{Out}(T)|^2|P|^2}{|T|^{\lceil \frac{k}{2} \rceil - 2}}.$$

By a classification-free result of Praeger and Saxl [63], since P is primitive and does not contain A_k, we know that the order of P is bounded above by 4^k. Moreover, we have $|\,\mathrm{Out}(T)|^2 \leqslant |T|^{2/3}$ by Lemma 3.1.3. Recall that $k \geqslant 5$, for if $k \leqslant 4$ then the primitivity of P implies that P is S_k or A_k; thus $\lceil k/2 \rceil - 17/6$ is positive. Suppose that T is not A_5 or $L_2(7)$. Then $|T| \geqslant 360$, so

$$\frac{|\,\mathrm{Out}(T)|^2|P|^2}{|T|^{\lceil \frac{k}{2} \rceil - 2}} \leqslant \frac{16^k}{|T|^{\frac{1}{6}} 360^{\lceil \frac{k}{2} \rceil - \frac{17}{6}}} \leqslant \frac{360^{\frac{17}{6}}}{|T|^{\frac{1}{6}}} \left(\frac{16}{\sqrt{360}}\right)^k,$$

which is our desired bound. Furthermore, since P is primitive and does not contain A_k, a classification-free result of Babai [3, Corollary 1.2] implies that $|P| \leqslant \exp(4\sqrt{k}(\log k)^2)$ for sufficiently large k. Note that k is eventually larger than $8\sqrt{k}(\log k)^2$. Suppose that T is A_5 or $L_2(7)$. Then $|\operatorname{Out}(T)| = 2$, so

$$\frac{|\operatorname{Out}(T)|^2|P|^2}{|T|^{\lceil \frac{k}{2} \rceil - 2}} \leqslant \frac{4e^{8\sqrt{k}(\log k)^2}}{|T|^{\frac{1}{6}} 60^{\lceil \frac{k}{2} \rceil - \frac{13}{6}}} \leqslant \frac{4 \cdot 60^{\frac{13}{6}}}{|T|^{\frac{1}{6}}} \left(\frac{e}{\sqrt{60}} \right)^k$$

for sufficiently large k. Since only finitely many G have been omitted from our argument, the proof is complete. □

Next we prove Lemma 4.3.2 using Lemma 3.1.4 and [50, Theorem 1].

Proof of Lemma 4.3.2. Let $R(T)$ be a set of representatives for the conjugacy classes of elements of prime order in $\operatorname{Aut}(T)$. Then we may assume that $R_2(G) = \{\overrightarrow{\alpha} : \alpha \in R(T)\}$ by Lemma 4.3.4. By applying Lemmas 4.3.4 and 4.3.5 with $\pi = 1$, we obtain the following.

$$\begin{aligned} |G| r_2(G) &= \sum_{\alpha \in R(T)} \left(|\operatorname{Aut}(T)|^2 |C_{\operatorname{Aut}(T)}(\alpha)|^{-2} \right) \left(|P| |C_{\operatorname{Aut}(T)}(\alpha)| |C_{\operatorname{Inn}(T)}(\alpha)|^{k-1} \right) \\ &\leqslant |\operatorname{Aut}(T)|^2 |P| \sum_{\alpha \in R(T)} |C_{\operatorname{Inn}(T)}(\alpha)|^{k-2} \\ &\leqslant |\operatorname{Out}(T)|^2 |T|^2 |P| f_p(\operatorname{Aut}(T)) \left(\max_{\alpha \in R(T)} |C_{\operatorname{Inn}(T)}(\alpha)| \right)^{k-2}, \end{aligned}$$

where $f_p(H)$ denotes the number of conjugacy classes of elements of prime order in a group H, as defined in Section 3.3. Since $k - 2$ is positive and $[T : C_{\operatorname{Inn}(T)}(\alpha)] \geqslant p(T)$ for every $1 \neq \alpha \in \operatorname{Aut}(T)$, if we divide by $|G|$, then we see that $r_2(G)$ is at most $|\operatorname{Out}(T)| f_p(\operatorname{Aut}(T)) p(T)^{2-k}$. It therefore suffices to show that

$$|\operatorname{Out}(T)| f_p(\operatorname{Aut}(T)) \leqslant C p(T)^{11/4}$$

for some absolute constant C. Note that the presence of the constant allows us to ignore finitely many simple groups T. In particular, we may ignore the sporadic groups and A_6.

Suppose that $T = A_m$ and $m \neq 6$. Then $\operatorname{Aut}(A_m) = S_m$ by Proposition 2.2.2, and since $f_p(S_m) \leqslant m^2$ by Lemma 3.3.2 and $p(T) = m$, it follows that $f_p(\operatorname{Aut}(T)) p(T)^{-11/4}$ is bounded above by $m^{-3/4}$. Since $|\operatorname{Out}(T)| = 2$, we have verified the desired inequality.

Let us assume, then, that T is a simple group of Lie type over $\mathbb{F}_q$. As noted in Section 3.3, for any group H and subgroup K, it is elementary to show that $f(H) \leqslant [H : K] f(K)$. (Lemma 3.3.1 provides an upper bound on $f(K)$ rather than on $f(H)$; see [29] for a proof of the upper bound on $f(H)$.) Hence $f_p(\operatorname{Aut}(T)) \leqslant f(T) |\operatorname{Out}(T)|$. Moreover, from [50,

Theorem 1] we know that $f(T) \leqslant (6q)^{l(T)}$ where $l(T)$ is the untwisted Lie rank of T. If T is not $L_m(2)$ for any m, then $|\operatorname{Out}(T)|^2(6q)^{l(T)} \leqslant Cp(T)^{11/4}$ for some absolute constant C by Lemma 3.1.4, and we have verified the desired inequality. If T is $L_m(2)$, then $|\operatorname{Out}(T)| = 2$, $p(T) \geqslant 2^{m-1}$ by [59], and $f(T) \leqslant 2^m$ by [58, Lemma 5.9], so the proof is complete. □

Lastly, we prove Lemma 4.3.3 using Lemma 3.4.1.

Proof of Lemma 4.3.3. Note that $R_3(G)$ may be empty, in which case the result is true, so we assume otherwise. For $\pi \in P$ of prime order p, let $f_\pi := \operatorname{fix}_{[k]}(\pi)$, let c_π be the number of non-trivial cycles of π so that $c_\pi = (k - f_\pi)/p$, and let $r_\pi := c_\pi + f_\pi$. Then r_π is the number of cycles in the full cycle decomposition of π in S_k, including fixed points. Since $|C_{\operatorname{Inn}(T)}(\alpha)| \leqslant |T|$, Lemmas 4.3.4 and 4.3.5 imply that

$$\begin{aligned} |G|r_3(G) &\leqslant \sum_{\overrightarrow{\alpha}\pi \in R_3(G)} |\alpha^{\operatorname{Aut}(T)}|^2 |\pi^P|^2 |C_P(\pi)||C_{\operatorname{Aut}(T)}(\alpha)||T|^{r_\pi - 1} \\ &= |\operatorname{Out}(T)||P| \sum_{\overrightarrow{\alpha}\pi \in R_3(G)} |\alpha^{\operatorname{Aut}(T)}||\pi^P||T|^{r_\pi}. \end{aligned}$$

Let $R(T)$ denote a set of representatives for the conjugacy classes of elements of prime order in $\operatorname{Aut}(T)$ together with the identity, and let $R(P)$ denote a set of representatives for the conjugacy classes of elements of prime order in P that fix a point of $[k]$. Then by Lemma 4.3.4 we may assume without loss of generality that $R_3(G) \subseteq \{\overrightarrow{\alpha}\pi : \alpha \in R(T), \pi \in R(P)\}$, so

$$\sum_{\overrightarrow{\alpha}\pi \in R_3(G)} |\alpha^{\operatorname{Aut}(T)}||\pi^P||T|^{r_\pi} \leqslant \sum_{\alpha \in R(T)} |\alpha^{\operatorname{Aut}(T)}| \sum_{\pi \in R(P)} |\pi^P||T|^{r_\pi} \leqslant |T|^{\frac{4}{3}} \sum_{\pi \in R(P)} |\pi^P||T|^{r_\pi}$$

since $|\operatorname{Aut}(T)| \leqslant |T|^{4/3}$ by Lemma 3.1.3. Thus the proof is complete by Lemma 3.4.1. □

Having proved the three lemmas, we now move on to prove Theorem 4.0.5.

Proof of Theorem 4.0.5. Recall from the proof of Theorem 4.0.4 that if $|G| \to \infty$, then $k \to \infty$ or $|T| \to \infty$. Thus if $k^4 \leqslant |T|$ and $|G| \to \infty$, then either k is bounded above by some absolute constant and $|T| \to \infty$, or $k \to \infty$ and $|T| \to \infty$. Note that $G \leqslant W(k,T) = A(k,T) \rtimes S_k$. Therefore, as in the proof of Theorem 4.0.4, it suffices to show that if $G = A(k,T) \rtimes S_k$ and $k \geqslant 5$, then $r_i(G)$ converges to 0 for each i as either $|T|$ tends to infinity with k bounded above by some absolute constant, or k tends to infinity with $k^4 \leqslant |T|$. Note that in the latter case we may ignore finitely many k and T if needed. Accordingly, suppose that $G = A(k,T) \rtimes S_k$.

Recall from the proof of Theorem 4.0.4 that $p(T) \to \infty$ as $|T| \to \infty$. Then Lemma 4.3.2 implies that $r_2(G) \to 0$ as either $|T| \to \infty$ with k bounded above by some absolute constant, or $k \to \infty$ with $k^4 \leqslant |T|$. Moreover, in the proof of Lemma 4.3.1, we saw that $r_1(G) \leqslant k!^2/|T|^{\lceil k/2 \rceil - 8/3}$ since $|\operatorname{Out}(T)|^2 < |T|^{2/3}$ by Lemma 3.1.3. But k is at least 5, so $r_1(G) \to 0$ as $|T| \to \infty$ with k bounded above by some absolute constant. If $k^4 \leqslant |T|$, then $r_1(G) \leqslant k!^2/k^{2k-32/3} \leqslant (k!k^6/k^k)^2$. A simple induction argument shows that $k!k^6 \leqslant k^{k-1}$ for k large enough, and so $r_1(G) \leqslant 1/k^2$. Hence $r_1(G) \to 0$ as $k \to \infty$ with $k^4 \leqslant |T|$. Thus it remains to consider $r_3(G)$; this will require some extra work.

For $\pi \in S_k$ of prime order p, as we have done before, let $f_\pi := \operatorname{fix}_{[k]}(\pi)$, $c_\pi := (k - f_\pi)/p$ and $r_\pi := c_\pi + f_\pi$. Also, let $R(S_k)$ denote a set of representatives for the conjugacy classes of elements of prime order in S_k that also fix a point. By Lemma 4.3.4, we may assume that if $\overrightarrow{\alpha}\pi \in R_3(G)$, then $\pi \in R(S_k)$. Moreover, we may assume for simplicity that if $\pi \in R(S_k)$ is a transposition, a double transposition or a 3-cycle, then π is (12), (12)(34) or (123) respectively.

For $\pi \in R(S_k)$, let $R_4(G, \pi) := \{\overrightarrow{\alpha}\pi \in R_3(G)\}$, and let $r_4(G, \pi)$ be the sum of $r_3(G)$ restricted to elements of $R_4(G, \pi)$. Also, let $R_4(T, \pi) := \{\alpha \in \operatorname{Aut}(T) : \overrightarrow{\alpha}\pi \in R_4(G, \pi)\}$. Then $R_4(T, \pi)$ consists of the identity and a set of representatives for the conjugacy classes of elements in $\operatorname{Aut}(T)$ with the same prime order as π. By Lemmas 4.3.4 and 4.3.5,

$$r_4(G, \pi) = |\pi^{S_k}| \sum_{\alpha \in R_4(T, \pi)} \frac{|\alpha^{\operatorname{Aut}(T)}||C_{\operatorname{Inn}(T)}(\alpha)|^{f_\pi - 1}}{|T|^{k - c_\pi - 1}}$$

for all $\pi \in R(S_k)$. In particular,

$$r_4(G, (12)) = |(12)^{S_k}| \sum_{\alpha \in R_4(T, (12))} \frac{|\alpha^{\operatorname{Aut}(T)}|}{|T|} \left(\frac{|C_{\operatorname{Inn}(T)}(\alpha)|}{|T|} \right)^{k-3} \leqslant k^2 \left(\frac{1}{|T|} + \frac{|\operatorname{Out}(T)|}{p(T)^{k-3}} \right)$$

since $[T : C_{\operatorname{Inn}(T)}(\alpha)] \geqslant p(T)$ if $\alpha \neq 1$. But $|\operatorname{Out}(T)| \leqslant Cp(T)^{11/8}$ for some absolute constant C by Lemma 3.1.4 since $|\operatorname{Out}(T)|$ is constant if T is either $L_m(2)$, an alternating group or a sporadic group [45, Section 5.1], so

$$r_4(G, (12)) \leqslant \frac{k^2}{|T|} + \frac{Ck^2}{p(T)^{k - \frac{35}{8}}} \tag{$*$}$$

for some absolute constant C. Moreover, $|C_{\operatorname{Inn}(T)}(\alpha)| \leqslant |T|$, so for any $\pi \in R(S_k)$,

$$r_4(G, \pi) \leqslant |\pi^{S_k}| \sum_{\alpha \in R_4(T, \pi)} \frac{|\alpha^{\operatorname{Aut}(T)}|}{|T|^{k - r_\pi}} \leqslant \frac{|\pi^{S_k}|}{|T|^{k - r_\pi - \frac{4}{3}}} \tag{$\dagger$}$$

since $|\operatorname{Aut}(T)| \leqslant |T|^{4/3}$ by Lemma 3.1.3.

First we claim that $r_3(G) \to 0$ when $|T| \to \infty$ with k bounded above by some absolute constant. It follows from equations $(*)$ and $(\dagger)$ that

$$r_3(G) \leqslant \frac{k^2}{|T|} + \frac{Ck^2}{p(T)^{k-\frac{35}{8}}} + \sum_{\pi \in R(S_k)\setminus\{(12)\}} \frac{|\pi^{S_k}|}{|T|^{k-r_\pi-\frac{4}{3}}}$$

for some absolute constant C. The claim then follows since $k \geqslant 5$ and $k - r_\pi \geqslant 2$ when π is not a transposition.

Now we claim that $r_3(G) \to 0$ when k tends to infinity with $k^4 \leqslant |T|$. Again since $[T : C_{\mathrm{Inn}(T)}(\alpha)] \geqslant p(T)$ if $\alpha \neq 1$,

$$\begin{aligned} r_4(G,(12)(34)) &= |(12)(34)^{S_k}| \sum_{\alpha \in R_4(T,(12)(34))} \frac{|\alpha^{\mathrm{Aut}(T)}|}{|T|^2} \left(\frac{|C_{\mathrm{Inn}(T)}(\alpha)|}{|T|}\right)^{k-5} \\ &\leqslant k^4 \left(\frac{1}{|T|^2} + \frac{|\operatorname{Out}(T)|}{|T|p(T)^{k-5}}\right). \end{aligned}$$

But $|\operatorname{Out}(T)| \leqslant |T|^{1/3}$ by Lemma 3.1.3, and certainly $p(T) \geqslant 5$, so

$$r_4(G,(12)(34)) \leqslant k^4 \left(\frac{1}{|T|^2} + \frac{1}{|T|^{\frac{2}{3}}5^{k-5}}\right) \leqslant \frac{1}{k^4} + \frac{k^{\frac{4}{3}}}{5^{k-5}}$$

since $|T| \geqslant k^4$. Similarly,

$$\begin{aligned} r_4(G,(123)) &= |(123)^{S_k}| \sum_{\alpha \in R_4(T,(123))} \frac{|\alpha^{\mathrm{Aut}(T)}|}{|T|^2} \left(\frac{|C_{\mathrm{Inn}(T)}(\alpha)|}{|T|}\right)^{k-4} \\ &\leqslant k^3 \left(\frac{1}{|T|^2} + \frac{|\operatorname{Out}(T)|}{|T|p(T)^{k-4}}\right) \\ &\leqslant k^3 \left(\frac{1}{|T|^2} + \frac{1}{|T|^{\frac{2}{3}}5^{k-4}}\right) \\ &\leqslant \frac{1}{k^5} + \frac{k^{\frac{1}{3}}}{5^{k-4}}. \end{aligned}$$

Lastly, equation $(*)$ implies that

$$r_4(G,(12)) \leqslant \frac{k^2}{|T|} + \frac{Ck^2}{p(T)^{k-\frac{35}{8}}} \leqslant \frac{1}{k^2} + \frac{Ck^2}{5^{k-\frac{35}{8}}}$$

for some absolute constant C.

Let $R(S_k)^* := R(S_k) \setminus \{(12),(12)(34),(123)\}$. Let $\pi \in R(S_k)^*$ have order p. Note that $k - r_\pi = (k - f_\pi) - c_\pi = pc_\pi - c_\pi$. Then since $|T| \geqslant k^4$ and $k - r_\pi \geqslant 2$, equation $(\dagger)$ implies that

$$r_4(G,\pi) \leqslant \frac{|\pi^{S_k}|}{|T|^{k-r_\pi-\frac{4}{3}}} \leqslant \frac{k^{pc_\pi}}{k^{4(k-r_\pi)-\frac{16}{3}}} = \frac{1}{k^{(3p-4)c_\pi-\frac{16}{3}}}.$$

Since $\pi \in R(S_k)^*$, it follows that $c_\pi \neq 1, 2$ when $p = 2$ and $c_\pi \neq 1$ when $p = 3$. Then $(3p-4)c_\pi - 16/3 \geqslant 8/3$ unless $p = 2$ and $c_\pi = 3$, in which case $(3p-4)c_\pi - 16/3 = 2/3$. Also, $|R(S_k)^*| < f_p(S_k) \leqslant k^2$ by Lemma 3.3.2. Putting these results together, we obtain

$$\sum_{\pi \in R(S_k)^*} r_4(G, \pi) \leqslant \frac{k^2}{k^{\frac{8}{3}}} + \frac{1}{k^{\frac{2}{3}}} = \frac{2}{k^{\frac{2}{3}}}.$$

Hence we have shown that

$$r_3(G) \leqslant \frac{1}{k^4} + \frac{k^{\frac{4}{3}}}{5^{k-5}} + \frac{1}{k^5} + \frac{k^{\frac{1}{3}}}{5^{k-4}} + \frac{1}{k^2} + \frac{Ck^2}{5^{k-\frac{35}{8}}} + \frac{2}{k^{\frac{2}{3}}}$$

for some absolute constant C, and so $r_3(G) \to 0$ if $k \to \infty$ with $k^4 \leqslant |T|$. □

Lastly, we finish this section by proving Theorem 4.0.6.

Proof of Theorem 4.0.6. As in the proof of Theorem 4.0.4, it suffices to prove the following two statements. First, if $G = A(k, T) \rtimes P$ where P is a primitive subgroup of S_k and $3 \leqslant k \leqslant 4$ (so P is S_k or A_k), then $r_i(G, 3)$ converges to 0 for each i as $|T|$ tends to infinity. Second, if $G = A(2, T) \rtimes 1$, then $r_2(G, 5)$ converges to 0 as $|T|$ tends to infinity.

First we consider $r_1(G, b)$. Extending the proof of Lemma 4.3.1 to general b, we obtain the following. If $\overrightarrow{\alpha}\pi \in R_1(G)$ where π has prime order p, then k/p is an integer and is therefore bounded above by $\lfloor k/2 \rfloor$. Since $P = P_G$, Lemma 4.3.5 then implies that

$$\max_{\overrightarrow{\alpha}\pi \in R_1(G)} |C_G(\overrightarrow{\alpha}\pi)| \leqslant |\operatorname{Out}(T)||P||T|^{\lfloor \frac{k}{2} \rfloor}.$$

Note that $|G_D| = |\operatorname{Out}(T)||T||P|$ and $|G| = |G_D||T|^{k-1}$. Then

$$r_1(G, b) \leqslant \frac{|G_D|^b}{|G|^{b-1}} \left(\max_{\overrightarrow{\alpha}\pi \in R_1(G)} |C_G(\overrightarrow{\alpha}\pi)| \right)^{b-1} \leqslant \frac{|\operatorname{Out}(T)|^b |P|^b}{|T|^{(b-1)\lceil \frac{k}{2} \rceil - b}} \leqslant \frac{2^{\frac{b}{4}} |P|^b}{|T|^{(b-1)\lceil \frac{k}{2} \rceil - \frac{5b}{4}}}$$

since $|\operatorname{Out}(T)|^b < (2|T|)^{b/4}$ by Lemma 3.1.3. Hence if $3 \leqslant k \leqslant 4$, then $r_1(G, 3) \leqslant C/|T|^{1/4}$ for some absolute constant C, so $r_1(G, 3) \to \infty$ as $|T| \to \infty$, as desired.

Now we consider $r_2(G, b)$ and extend the proof of Lemma 4.3.2. Let $R(T)$ be a set of representatives for the conjugacy classes of elements of prime order in $\operatorname{Aut}(T)$. Then we may assume that $R_2(G) = \{\overrightarrow{\alpha} : \alpha \in R(T)\}$ by Lemma 4.3.4. By applying Lemmas 4.3.4 and 4.3.5 with $\pi = 1$, we obtain the following.

$$\begin{aligned}
|G|^{b-1} r_2(G, b) &= \sum_{\alpha \in R(T)} \left(|\operatorname{Aut}(T)|^b |C_{\operatorname{Aut}(T)}(\alpha)|^{-b} \right) \left(|P||C_{\operatorname{Aut}(T)}(\alpha)||C_{\operatorname{Inn}(T)}(\alpha)|^{k-1} \right)^{b-1} \\
&\leqslant |\operatorname{Aut}(T)|^b |P|^{b-1} \sum_{\alpha \in R(T)} |C_{\operatorname{Inn}(T)}(\alpha)|^{(b-1)k-b} \\
&\leqslant |\operatorname{Out}(T)|^b |T|^b |P|^{b-1} f_p(\operatorname{Aut}(T)) \left(\max_{\alpha \in R(T)} |C_{\operatorname{Inn}(T)}(\alpha)| \right)^{(b-1)k-b}.
\end{aligned}$$

Since $(b-1)k-b$ is positive and $[T : C_{\mathrm{Inn}(T)}(\alpha)] \geqslant p(T)$ for every $1 \neq \alpha \in \mathrm{Aut}(T)$, if we divide by $|G|^{b-1}$, then we see that $r_2(G,b)$ is at most $|\operatorname{Out}(T)| f_p(\mathrm{Aut}(T)) p(T)^{b-(b-1)k}$. But we saw in the proof of Lemma 4.3.2 that $|\operatorname{Out}(T)| f_p(\mathrm{Aut}(T)) \leqslant Cp(T)^{11/4}$ for some absolute constant C, so

$$r_2(G,b) \leqslant C/p(T)^{(b-1)k-b-11/4}$$

for some absolute constant C. Since $p(T) \to \infty$ as $|T| \to \infty$, it follows that $r_2(G,3) \to 0$ as $|T| \to \infty$ when $3 \leqslant k \leqslant 4$, and $r_2(G,5) \to 0$ as $|T| \to \infty$ when $k = 2$.

Lastly, we consider $r_3(G,b)$ and extend the proof of Lemma 4.3.3. Note that $R_3(G)$ may be empty, in which case the result is true, so we assume otherwise. For $\pi \in P$ of prime order p, let $f_\pi := \mathrm{fix}_{[k]}(\pi)$, let c_π be the number of non-trivial cycles of π so that $c_\pi = (k - f_\pi)/p$, and let $r_\pi := c_\pi + f_\pi$. Since $|C_{\mathrm{Inn}(T)}(\alpha)| \leqslant |T|$, Lemmas 4.3.4 and 4.3.5 imply that

$$\begin{aligned} |G|^{b-1} r_3(G,b) &\leqslant \sum_{\overrightarrow{\alpha}\pi \in R_3(G)} |\alpha^{\mathrm{Aut}(T)}|^b |\pi^P|^b \left(|C_P(\pi)||C_{\mathrm{Aut}(T)}(\alpha)||T|^{r_\pi - 1}\right)^{b-1} \\ &= |\operatorname{Out}(T)|^{b-1} |P|^{b-1} \sum_{\overrightarrow{\alpha}\pi \in R_3(G)} |\alpha^{\mathrm{Aut}(T)}||\pi^P||T|^{(b-1)r_\pi}. \end{aligned}$$

Let $R(T)$ denote a set of representatives for the conjugacy classes of elements of prime order in $\mathrm{Aut}(T)$ together with the identity, and let $R(P)$ denote a set of representatives for the conjugacy classes of elements of prime order in P that fix a point of $[k]$. Then by Lemma 4.3.4 we may assume without loss of generality that $R_3(G) \subseteq \{\overrightarrow{\alpha}\pi : \alpha \in R(T), \pi \in R(P)\}$, and as $r_\pi \leqslant k-1$, we obtain that

$$\sum_{\overrightarrow{\alpha}\pi \in R_3(G)} |\alpha^{\mathrm{Aut}(T)}||\pi^P||T|^{(b-1)r_\pi} \leqslant \sum_{\alpha \in R(T)} |\alpha^{\mathrm{Aut}(T)}| \sum_{\pi \in R(P)} |\pi^P||T|^{(b-1)(k-1)} \leqslant |T|^{\frac{4}{3}} |P||T|^{(b-1)(k-1)}$$

since $|\operatorname{Aut}(T)| \leqslant |T|^{4/3}$ by Lemma 3.1.3. Dividing by $|G|^{b-1}$, we obtain that

$$r_3(G,b) \leqslant \frac{|P|}{|T|^{b-\frac{7}{3}}}.$$

Thus $r_3(G,3) \to 0$ as $|T| \to \infty$ when $3 \leqslant k \leqslant 4$. □

Note that the methods of the proof of Theorem 4.0.6 can be improved by using stronger bounds on the numbers of conjugacy classes of non-abelian simple groups from [28]. In fact, it looks likely that if $k = 2$ and $P_G = 1$, then the proportion of 3-tuples that are bases for G tends to 1 as $|G| \to \infty$.

Chapter 5

The twisted wreath case

In this chapter, we investigate the bases of groups of twisted wreath type.

Let T be a non-abelian simple group, and let k be an integer that is at least 2. A group G of twisted wreath type with socle T^k acts primitively on a set Ω with degree $|T|^k$ and is also a twisted wreath product, which is a split extension of T^k by a transitive subgroup P of S_k, where P is the stabiliser of the primitive action of G on Ω. Precise definitions will be given in Section 5.1. The group P is called the top group of G, and the study of the base size of a group of twisted wreath type divides into two cases depending on whether the top group is primitive or imprimitive.

When the top group is primitive, we find that groups of twisted wreath type always have base size 2. Note that in contrast to the diagonal case, this result includes the case where the top group is the symmetric or alternating group.

Theorem 5.0.1. *Let G be a group of twisted wreath type with socle T^k for some non-abelian simple group T. If the top group P of G is primitive on $[k]$, then $b(G) = 2$.*

As with groups of diagonal type, this is the best result we could hope for since a group of twisted wreath type never has base size 1 by Lemma 2.3.3. The proof of Theorem 5.0.1 is largely constructive, though, as in the diagonal case, it depends on the non-constructive result of Seress [69] that determines exactly when a primitive permutation group has a regular orbit on the power set of the domain of its action.

We also have a probabilistic result that is analogous to Theorem 4.0.4.

Theorem 5.0.2. *Let G be a group of twisted wreath type with socle T^k for some non-abelian simple group T. If the top group P of G is primitive on $[k]$, then the proportion of pairs of points from Ω that are bases for G tends to 1 as $|G| \to \infty$.*

In fact, we will prove some results that are stronger than Theorems 5.0.1 and 5.0.2 (Propositions 5.3.4 and 5.3.5), as we do not always require the assumption that the twisted wreath product be primitive.

However, determining the base size of a group of twisted wreath type becomes more complicated when the top group is imprimitive, as imprimitive groups can be quite large compared to most primitive groups. In particular, we must deal with the imprimitive action of the wreath product $S_m \wr_r S_r$ on $[m] \times [r]$. Since every imprimitive permutation group of degree k with r blocks is permutation isomorphic to a subgroup of the imprimitive group $S_{k/r} \wr_r S_r$, this wreath product is the largest possibility for the top group. Thus we focus on understanding the base size of a group of twisted wreath type with top group $S_m \wr_r S_r$. Our next result shows that the base size of such a group can be quite small in certain cases but unbounded in others. In particular, this base size behaves much like that of a group of diagonal type whose top group contains the alternating group. Note that groups of twisted wreath type with top group $S_m \wr_r S_r$ and socle $(A_{m-1})^{mr}$ can be constructed for arbitrarily large m and r (see Proposition 5.5.1).

Theorem 5.0.3. *Let G be a group of twisted wreath type with socle T^k for some non-abelian simple group T. Suppose that the top group P of G is $S_m \wr_r S_r$ in its imprimitive action on $[m] \times [r]$ where $k = mr$, $m \geqslant 2$ and $r \geqslant 2$. Then $T = A_{m-1}$ and*

$$\left\lceil \frac{\log r}{m \log |T|} \right\rceil + 1 \leqslant b(G) \leqslant \left\lceil \frac{\log(r + m - 1)}{\log |T|} \right\rceil + 3.$$

In particular, if $r \leqslant (m-2)!$ then $b(G) \leqslant 4$, and if $r \to \infty$ with m fixed then $b(G) \to \infty$.

In order to prove Theorem 5.0.3, we classify the groups of twisted wreath type with top group $S_m \wr_r S_r$ (Proposition 5.5.1). This requires us to determine the almost simple quotients of point stabilisers in $S_m \wr_r S_r$ (Lemma 5.4.10), and in particular, the normal subgroups of $S_m \wr_r S_r$ (Proposition 5.4.7).

Thus the base size of a group of twisted wreath type with imprimitive top group can be unbounded. However, if we restrict our attention to imprimitive top groups that are proper, which essentially means they do not involve the symmetric or alternating group (see the end of Section 5.5), then we can say the following.

Theorem 5.0.4. *Let G be a group of twisted wreath type with socle T^k for some non-abelian simple group T. Suppose that the top group P of G is a proper imprimitive permutation group on $[k]$. If $T \neq A_5$ then $b(G) = 2$, and if $T = A_5$ then $b(G) \leqslant 3$.*

The proof of Theorem 5.0.4 uses a result of Dolfi [24] that bounds the distinguishing number of a transitive permutation group (see Section 5.2). Moreover, as in the primitive

case, we can prove a result that is stronger than Theorem 5.0.4 in that it does not require the twisted wreath product to be primitive (Proposition 5.5.3).

This chapter is organised as follows. General twisted wreath products and groups of twisted wreath type are defined in Section 5.1, and then we prove various results about the base sizes of certain twisted wreath products in Section 5.2. Theorems 5.0.1 and 5.0.2 are proved in Section 5.3: Theorem 5.0.1 follows from Proposition 5.3.4, and Theorem 5.0.2 follows from Proposition 5.3.5. In Section 5.4, we divert from the base size problem to determine the almost simple quotients of stabilisers of $S_m \wr_r S_r$. Lastly, in Section 5.5 we prove Theorem 5.0.3 and obtain Theorem 5.0.4 as a consequence of Proposition 5.5.3. Note that most of the results in this chapter depend upon the CFSG.

5.1 Groups of twisted wreath type

The following definitions for groups of twisted wreath type may be found in [49]. We begin by defining the twisted wreath product. Let T and P be groups, and let Q be a subgroup of P and $\varphi : Q \to \mathrm{Aut}(T)$ a homomorphism. Define

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

Then $B(T, P, \varphi)$ is a group with multiplication defined by $fg(x) := f(x)g(x)$ for all $x \in P$ and $f, g \in B(T, P, \varphi)$. We write B for $B(T, P, \varphi)$ when the context permits. Moreover, P acts on B by $f^\pi(x) := f(\pi x)$ for all $\pi, x \in P$ and $f \in B$. Note that $(fg)^\pi = f^\pi g^\pi$ for all $\pi \in P$ and $f, g \in B$. As a result, we define the *twisted wreath product* of T and P by

$$T \operatorname{twr}_\varphi P := B(T, P, \varphi) \rtimes P.$$

The group P is called the *top group* of $T \operatorname{twr}_\varphi P$.

If L is a left transversal for Q in P, then any function $f : L \to T$ can be naturally extended to an element of $B(T, P, \varphi)$ by defining $f(lq) := f(l)(q\varphi)$ for all $l \in L$ and $q \in Q$. It follows that if $[P : Q] = k$, then $B(T, P, \varphi) \simeq T^k$.

Furthermore, suppose that T is a non-abelian simple group, P is a transitive subgroup of S_k for some $k \geqslant 2$, and $Q := P_1$. Then $B(T, P, \varphi)$ is the unique minimal normal subgroup of $T \operatorname{twr}_\varphi P$, and so $T \operatorname{twr}_\varphi P$ acts faithfully on the left coset space $(T \operatorname{twr}_\varphi P : P)$. Thus $T \operatorname{twr}_\varphi P$ is a transitive permutation group with socle T^k and degree $|T|^k$. Note that B acts regularly on $(T \operatorname{twr}_\varphi P : P)$.

We say that a group G has *twisted wreath type* if there exists a non-abelian simple group T, a transitive subgroup P of S_k for some $k \geqslant 2$, and a homomorphism $\varphi : P_1 \to \mathrm{Aut}(T)$

for which $G = T \operatorname{twr}_\varphi P$ and G acts primitively on the left coset space $(G : P)$. (In contrast to [49], we do not assume that $\mathrm{Inn}(T) \leqslant \mathrm{Im}(\varphi)$.)

The groups $T \operatorname{twr}_\varphi P$ in which P is maximal are classified by Baddeley [4, Theorem 3.5], and so we have the following classification of groups of twisted wreath type by Proposition 2.2.1. This result is more complicated than the corresponding result in the diagonal case; in particular, it shows that the primitivity of a twisted wreath product does not depend solely on the top group.

Theorem 5.1.1 ([4])**.** *Let T be a non-abelian simple group and P a transitive subgroup of S_k where $k \geqslant 2$. Let $Q := P_1$ and $\varphi : Q \to \mathrm{Aut}(T)$ a homomorphism. Let $U := \ker(\varphi)$ and $V := \mathrm{Inn}(T)\varphi^{-1}$. Suppose that $M \trianglelefteq P$ for which $MU = MV$, and let $U' := U \cap M$ and $V' := V \cap M$. Then $T \operatorname{twr}_\varphi P$ is a group of twisted wreath type if and only if*

(i) $V'/U' \simeq T$, and

(ii) $Q = N_P(U') \cap N_P(V')$, and

(iii) If R is a subgroup of M normalised by Q for which $R \cap V' = U'$, then $R = U'$.

Note that we can always take the group M in Theorem 5.1.1 to be P itself, and so this result does genuinely characterise groups of twisted wreath type.

We will only use the full power of Theorem 5.1.1 to prove Theorem 5.0.3, as the following result is normally sufficient for our purposes.

Lemma 5.1.2 ([4])**.** *Let T be a non-abelian simple group and P a transitive subgroup of S_k where $k \geqslant 2$. Let $Q := P_1$ and $\varphi : Q \to \mathrm{Aut}(T)$ a homomorphism. If $T \operatorname{twr}_\varphi P$ is a group of twisted wreath type, then $\mathrm{Inn}(T) \leqslant \mathrm{Im}(\varphi)$.*

Proof. Taking M to be P, Theorem 5.1.1 implies that $T \simeq V/U \simeq V\varphi \leqslant \mathrm{Inn}(T)$, so $\mathrm{Inn}(T) = V\varphi \leqslant \mathrm{Im}(\varphi)$. □

Groups of twisted wreath type are quite rare. Indeed, there are only finitely many groups of twisted wreath type for each k, for if $\mathrm{Inn}(T) \leqslant \mathrm{Im}(\varphi)$, then T is a composition factor of Q. In this way, the twisted wreath case differs significantly from the diagonal case, where primitive groups can be constructed for any k and T.

5.2 Base sizes for twisted wreath products

In this section, we obtain various conditions which guarantee that a twisted wreath product has base size 2, as well as some general upper bounds on the base size of a twisted

wreath product. We also determine a useful upper bound on the proportion of pairs of points that do not form bases.

For this section, let $k \geqslant 2$ be an integer, let P be a transitive subgroup of S_k, let $Q := P_1$, let T be a non-abelian simple group, and let $\varphi : Q \to \mathrm{Aut}(T)$ be a homomorphism. Let G be the twisted wreath product $T \operatorname{twr}_\varphi P$, and let $\Omega := (G : P)$. Note that we do not assume in this section that the action of G on Ω is primitive.

First we see that the base size of G on Ω and the base size of P on $B = B(T, P, \varphi)$ are closely related. (The base size of P is defined, for P acts faithfully on B since G acts faithfully on Ω and $\{(1, \pi) \in G : \pi \in P_f\} \leqslant G_{(f,1)^P}$ for all $f \in B$.) Observe that G never has base size 1 as P is non-trivial, and also that the identity of B is fixed by every element of P and so can be in no minimal base for P.

Lemma 5.2.1. $b_\Omega(G) = b_B(P) + 1$.

Proof. For any $1 \neq f \in B$, we have $P \cap G_{(f,1)^P} = \{(1, \pi) \in G : \pi \in P_f\}$, so if $f_1, \ldots, f_r$ are distinct non-trivial elements of B, then $\{f_1, \ldots, f_r\}$ is a base for P if and only if $\{P, (f_1, 1)P, \ldots, (f_r, 1)P\}$ is a base for G. Since G acts transitively, there is no loss of generality in assuming a base for G contains P by Lemma 2.3.1, and the result follows. □

As a consequence of Lemma 5.2.1, we will typically focus on the action of P on B to prove results about bases of twisted wreath products.

Now we briefly consider a useful property of the group B. We say that a left transversal $\{g_1, g_2, \ldots, g_k\}$ for Q in P is *ideal* if $g_1 = 1$ and $ig_i = 1$ for all $i \in [k]$. Such transversals always exist: the transitivity of P allows us to choose elements $g_1, \ldots, g_k$ in P for which $ig_i = 1$ for all $i \in [k]$, and these elements form a left transversal. To simplify notation, if L is any left transversal for Q in P and $\pi \in P$, we write q_π for the unique element of Q satisfying $\pi q_\pi^{-1} \in L$.

Lemma 5.2.2. *Let $g_1, \ldots, g_k$ be an ideal left transversal for Q in P. If $f \in B$ and $\pi \in P$ are such that $f^\pi = f$, then $f(g_i)(q_{\pi g_{i\pi}}\varphi) = f(g_{i\pi})$ for all $i \in [k]$.*

Proof. Fix $i \in [k]$. Since $jg_j = 1$ for all $j \in [k]$, it follows that $1g_i^{-1}\pi g_{i\pi} = i\pi g_{i\pi} = 1$, and so $g_i^{-1}\pi g_{i\pi} \in Q$. Then $\pi g_{i\pi} = g_i q_{\pi g_{i\pi}}$, and so $f(g_i)(q_{\pi g_{i\pi}}\varphi) = f(\pi g_{i\pi}) = f^\pi(g_{i\pi}) = f(g_{i\pi})$. □

To state the next few results, we need some more definitions. Let H be a permutation group on Δ. Let $D_\Delta(H)$ denote the set of those partitions of Δ for which only the identity of H fixes every part. Then the *distinguishing number* $d_\Delta(H)$ of H on Δ is defined to be the smallest number of parts in a member of $D_\Delta(H)$. Note that $d_\Delta(H) > 1$ when H is non-trivial. In addition, if $\{\delta_1, \ldots, \delta_r\}$ is a base for H, then $\{\{\delta_1\}, \ldots, \{\delta_r\}, \Delta \setminus \{\delta_1, \ldots, \delta_r\}\}$

is a partition of Δ in $D_\Delta(H)$ with $r+1$ parts, and so $d_\Delta(H) \leqslant b_\Delta(H)+1$. We also write $h(T)$ for the number of orbits of the natural action of $\mathrm{Aut}(T)$ on T.

Lemma 5.2.3. *If $d_{[k]}(P) \leqslant h(T)$, then G has base size 2.*

Proof. Let $g_1, \ldots, g_k$ be an ideal left transversal for Q in P, and let $\Delta_1, \ldots, \Delta_m$ be a partition in $D_{[k]}(P)$ where $m = d_{[k]}(P)$. Choose m representatives for the orbits of $\mathrm{Aut}(T)$ on T, and enumerate these elements as $t_1, \ldots, t_m$. Define $f \in B$ by $f(g_i) := t_j$ when $i \in \Delta_j$. Suppose that $\pi \in P$ fixes f and let $i \in \Delta_j$. Then $f(g_i)$ and $f(g_{i\pi})$ are in the same orbit of $\mathrm{Aut}(T)$ by Lemma 5.2.2, so $f(g_{i\pi}) = t_j$. Thus $i\pi \in \Delta_j$, and it follows that π is the identity. Hence G has base size 2 by Lemma 5.2.1. □

Applying the fact that $d_{[k]}(P) \leqslant b_{[k]}(P)+1$, we then obtain the following corollary.

Corollary 5.2.4. *If $b_{[k]}(P) < h(T)$, then G has base size 2.*

More generally, we have two different upper bounds on the base size of a twisted wreath product. Their proofs are similar to the proof of Proposition 4.2.8.

Lemma 5.2.5. $b_\Omega(G) \leqslant \left\lceil \frac{\log d_{[k]}(P)}{\log |T|} \right\rceil + 3$.

Proof. Let $g_1, \ldots, g_k$ be an ideal left transversal for Q in P, and let m be the positive integer $\lceil \log d_{[k]}(P) / \log |T| \rceil$. For each integer u such that $1 \leqslant u \leqslant d_{[k]}(P)$, let $d_{u,0}, \ldots, d_{u,m-1}$ denote the first m digits of the base $|T|$ representation of $u-1$; this is reasonable since $|T|^{m-1} \leqslant d_{[k]}(P) - 1 < |T|^m$. Let x and y be elements of T for which $T = \langle x, y \rangle$, which exist by [1]. Enumerate the elements of T as $t_0, \ldots, t_{|T|-1}$, and let $\Delta_1, \ldots, \Delta_{d_{[k]}(P)}$ be a partition in $D_{[k]}(P)$. We define $\mathscr{B} := \{f_1, \ldots, f_{m+2}\} \subseteq B$ as follows: let $f_{m+1}(g_j) := x$ for all j, let $f_{m+2}(g_j) := y$ for all j, and for each $i \in [m]$, let $f_i(g_j) := t_{d_{u,i-1}}$ when $j \in \Delta_u$.

Suppose that $\pi \in P$ fixes f_i for all $1 \leqslant i \leqslant m+2$. Then $x(q_{\pi g_{j\pi}}\varphi) = x$ and $y(q_{\pi g_{j\pi}}\varphi) = y$ for all $j \in [k]$ by Lemma 5.2.2, so $q_{\pi g_{j\pi}}\varphi = 1$ for all $j \in [k]$. Hence $f_i(g_{j\pi}) = f_i(g_j)$ for all $i \in [m]$ and $j \in [k]$ by Lemma 5.2.2. Next suppose that $j \in \Delta_u$ and $j\pi \in \Delta_v$. Then $t_{d_{u,i-1}} = f_i(g_j) = f_i(g_{j\pi}) = t_{d_{v,i-1}}$ for all $i \in [m]$, so $d_{u,i-1} = d_{v,i-1}$ for all $i \in [m]$. Thus $u = v$, so $j\pi \in \Delta_u$, and we conclude that $\pi = 1$. Hence $\mathscr{B}$ is a base for the action of P on B, and the result follows from Lemma 5.2.1. □

The second upper bound is a generalisation of Lemma 5.2.3. Its proof is almost identical to that of the previous result except that it does not rely on the CFSG.

Lemma 5.2.6. $b_\Omega(G) \leqslant \left\lceil \frac{\log d_{[k]}(P)}{\log h(T)} \right\rceil + 1$.

Proof. Let $g_1, \dots, g_k$ be an ideal left transversal for Q in P. Let m be the positive integer $\lceil \log d_{[k]}(P) / \log h(T) \rceil$. For each integer u such that $1 \leqslant u \leqslant d_{[k]}(P)$, let $d_{u,0}, \dots, d_{u,m-1}$ denote the first m digits of the base $h(T)$ representation of $u-1$; this is reasonable since $h(T)^{m-1} \leqslant d_{[k]}(P) - 1 < h(T)^m$. Let $t_0, \dots, t_{h(T)-1}$ be representatives of the orbits of the action of $\mathrm{Aut}(T)$ on T, and let $\Delta_1, \dots, \Delta_{d_{[k]}(P)}$ be a partition in $D_{[k]}(P)$. We define $\mathscr{B} := \{f_1, \dots, f_m\} \subseteq B$ as follows: for each $i \in [m]$, let $f_i(g_j) := t_{d_{u,i-1}}$ if $j \in \Delta_u$.

Suppose that $\pi \in P$ fixes f_i for all $i \in [m]$. Then $f_i(g_j)(q_{\pi g_{j\pi}} \varphi) = f_i(g_{j\pi})$ for all $i \in [m]$ and $j \in [k]$ by Lemma 5.2.2, so $f_i(g_j)$ and $f_i(g_{j\pi})$ are in the same orbit of $\mathrm{Aut}(T)$ for all $i \in [m]$ and $j \in [k]$. Next suppose that $j \in \Delta_u$ and $j\pi \in \Delta_v$. Then $t_{d_{u,i-1}}$ and $t_{d_{v,i-1}}$ are in the same orbit for all $i \in [m]$, so $d_{u,i-1} = d_{v,i-1}$ for all $i \in [m]$. Thus $u = v$, so $j\pi \in \Delta_u$, and we conclude that $\pi = 1$. Hence $\mathscr{B}$ is a base for the action of P on B, and the result follows from Lemma 5.2.1. □

We wish to use Lemma 3.2.1 to prove Theorems 5.0.1 and 5.0.2, so we need to calculate the sizes of conjugacy classes and centralisers of elements in the stabiliser $G_P = P$.

Lemma 5.2.7. *Suppose that $(1, \pi) \in G_P$. Then*

$$(1, \pi)^G \cap G_P = \{(1, \pi') : \pi' \in \pi^P\}.$$

In particular, $|(1, \pi)^G \cap G_P| = |\pi^P|$.

Proof. Suppose that $\pi' = \sigma^{-1}\pi\sigma$ for any $\sigma \in P$. Then $(1, \pi') = (1, \sigma)^{-1}(1, \pi)(1, \sigma)$. On the other hand, suppose that $(1, \pi') = (f, \sigma)^{-1}(1, \pi)(f, \sigma)$ for any $(f, \sigma) \in G$. Then $(1, \pi') = ((f^{-1} f^{\pi^{-1}})^\sigma, \sigma^{-1}\pi\sigma)$, so $\pi' = \sigma^{-1}\pi\sigma$. □

Lemma 5.2.8. *Suppose that $(1, \pi) \in G_P$. Then*

$$C_G((1, \pi)) = \{(f, \pi') \in G : f \in \mathrm{fix}_B(\pi), \pi' \in C_P(\pi)\}.$$

In particular, $|C_G((1, \pi))| = |\mathrm{fix}_B(\pi)||C_P(\pi)|$.

Proof. Let $(f, \pi') \in G$. Then (f, π') centralises $(1, \pi)$ if and only if $(f, \pi'\pi) = (f^{\pi^{-1}}, \pi\pi')$, and this occurs precisely when $f \in \mathrm{fix}_B(\pi)$ and $\pi' \in C_P(\pi)$. □

Lemma 5.2.9. *Let $\pi \in P$. Then $|\mathrm{fix}_B(\pi)| \leqslant |T|^{r_\pi}$ where r_π denotes the number of cycles in the full cycle decomposition of π in S_k, including fixed points.*

Proof. Let $c_1 c_2 \cdots c_r$ be a full decomposition of π into disjoint cycles c_j, including fixed points, where $r := r_\pi$. Without loss of generality, we may assume that the cycle c_j

contains the point j for each $j \in [r]$. Let $g_1, \ldots, g_k$ be an ideal left transversal for Q in P. Then we define a map $\psi : \mathrm{fix}_B(\pi) \to T^r$ by $f \mapsto (f(g_1), \ldots, f(g_r))$ for all $f \in \mathrm{fix}_B(\pi)$. We claim that ψ is injective. Suppose that $f_1, f_2 \in \mathrm{fix}_B(\pi)$ where $(f_1(g_1), \ldots, f_1(g_r)) = (f_2(g_1), \ldots, f_2(g_r))$. Then $f_1(g_j) = f_2(g_j)$ for all $j \in [r]$. It suffices to show that $f_1(g_i) = f_2(g_i)$ for all $i \in [k]$, so we fix $i \in [k]$. Then i is in the cycle c_j of π for some $j \in [r]$, so $i = j\pi^m$ for some m. Let f be f_1 or f_2. Observe that π^m fixes f since π fixes f, and so Lemma 5.2.2 implies that $f(g_{j\pi^m}) = f(g_j)(q_{\pi^m g_{j\pi^m}}\varphi)$. Let $\alpha := q_{\pi^m g_{j\pi^m}}\varphi$. Then $f_1(g_i) = f_1(g_{j\pi^m}) = f_1(g_j)\alpha = f_2(g_j)\alpha = f_2(g_{j\pi^m}) = f_2(g_i)$, as desired. □

Recall from Section 3.2 that $Q(G, 2)$ denotes the proportion of pairs in $\Omega \times \Omega$ not forming bases for G. Using the last three lemmas, we obtain the following version of Lemma 3.2.1.

Lemma 5.2.10. *Let $R(P)$ be a set of representatives for the conjugacy classes of elements of prime order in P. Then*

$$Q(G, 2) \leqslant \sum_{\pi \in R(P)} \frac{|\pi^P||T|^{r_\pi}}{|T|^k},$$

where r_π denotes the number of cycles in the full cycle decomposition of π in S_k, including fixed points.

Proof. By Lemma 5.2.7, $\{(1, \pi) \in G : \pi \in R(P)\}$ is a set of representatives for the G-conjugacy classes of elements of prime order in G_P and $|(1, \pi)^G \cap G_P| = |\pi^P|$ for all $\pi \in R(P)$. Moreover, Lemmas 5.2.8 and 5.2.9 imply that $|C_G((1, \pi))| = |\mathrm{fix}_B(\pi)||C_P(\pi)| \leqslant |T|^{r_\pi}|C_P(\pi)|$ for all $\pi \in R(P)$. Since $|G| = |T|^k|P|$, Lemma 3.2.1 implies that

$$Q(G, 2) \leqslant \sum_{\pi \in R(P)} \frac{|\pi^P|^2|T|^{r_\pi}|C_P(\pi)|}{|T|^k|\pi^P||C_P(\pi)|},$$

and the result follows. □

5.3 The primitive case

In this section, we focus on groups of twisted wreath type whose top group is primitive and prove Theorems 5.0.1 and 5.0.2. In fact, our methods only require the necessary condition given in Lemma 5.1.2 for a twisted wreath product to be primitive, so we prove some more general results instead.

For this section, let $k \geqslant 2$ be an integer, let P be a primitive subgroup of S_k, let $Q := P_1$, let T be a non-abelian simple group, and let $\varphi : Q \to \mathrm{Aut}(T)$ be a homomorphism. Let

G be the twisted wreath product $T \operatorname{twr}_\varphi P$, and let $\Omega := (G : P)$. Again, we do not assume that the action of G on Ω is primitive, nor do we always assume that $\mathrm{Inn}(T) \leqslant \mathrm{Im}(\varphi)$.

We begin by dealing with the case where the degree of the top group is large enough.

Proposition 5.3.1. *If $k > 32$ and P is not S_k or A_k, then $b_\Omega(G) = 2$.*

Proof. By the assumptions on P and [69, Theorem 1], the set $[k]$ can be partitioned into two non-empty subsets Δ and Γ such that the setwise stabiliser of Δ in P is trivial. Thus $d_{[k]}(P) = 2$. Certainly $2 \leqslant h(T)$ since the identity is fixed by every automorphism of T, so G has base size 2 by Lemma 5.2.3. □

The case where the top group is the symmetric or alternating group is easily dealt with, for there is only one possibility for T if we assume that $\mathrm{Inn}(T) \leqslant \mathrm{Im}(\varphi)$, as we now see.

Lemma 5.3.2. *If $\mathrm{Inn}(T) \leqslant \mathrm{Im}(\varphi)$ and P is S_k or A_k, then $T = A_{k-1}$ and $k \geqslant 6$.*

Proof. Clearly Q is S_{k-1} or A_{k-1}. Then $\ker(\varphi)$ is trivial, A_{k-1} or S_{k-1}. However, the latter two cases are impossible since then $\mathrm{Im}(\varphi)$ would be trivial or C_2. Thus φ is injective, so $\mathrm{Inn}(T)$ is a normal subgroup of S_{k-1} or A_{k-1}. Hence $T = A_{k-1}$ and $k \geqslant 6$. □

Using Lemma 5.3.2, we can prove that G has base size 2 when the top group is the symmetric or alternating group with large enough degree.

Proposition 5.3.3. *If $\mathrm{Inn}(T) \leqslant \mathrm{Im}(\varphi)$ and P is S_k or A_k where $k \geqslant 8$, then $b_\Omega(G) = 2$.*

Proof. By Lemma 5.3.2, the group T must be A_{k-1}. Let $m := k-1$. Certainly P has a base of size m, so it suffices by Corollary 5.2.4 to show that $m < h(A_m)$. Since $\mathrm{Aut}(A_m) = S_m$ by Proposition 2.2.2, it follows that $h(A_m)$ is the number of S_m-conjugacy classes of elements in A_m, which is precisely the number of cycle types of even permutations. Write $m+1 = 2^i r$ for some non-negative integer i and odd integer r. Then A_{m+1} contains a fixed-point-free permutation consisting of 2^i disjoint r-cycles unless $r = 1$, in which case A_{m+1} contains a fixed-point-free permutation consisting of 2^{i-1} disjoint transpositions. Thus $h(A_m) + 1 \leqslant h(A_{m+1})$. Since $h(A_7) = 8$, the desired result then follows by induction. □

Now we prove a more general version of Theorem 5.0.1 by assuming that $\mathrm{Inn}(T) \leqslant \mathrm{Im}(\varphi)$ only when the top group is the symmetric or alternating group. This is done using Lemma 5.2.10 and GAP [30]. Note that the GAP source code used in this proof may be found in Appendix A.2.

Proposition 5.3.4. *If $\mathrm{Inn}(T) \leqslant \mathrm{Im}(\varphi)$ when P is S_k or A_k, then $b_\Omega(G) = 2$.*

Proof. If $k > 32$, then we are done by Propositions 5.3.1 and 5.3.3, so we assume that $k \leqslant 32$. Suppose that G does not have base size 2. Then $Q(G,2) = 1$, so Lemma 5.2.10 implies that if $R(P)$ is a set of representatives for the conjugacy classes of elements of prime order in P and r_π is the number of cycles in the full cycle decomposition of π in S_k including fixed points, then $|T|^k \leqslant \sum_{\pi \in R(P)} |\pi^P||T|^{r_\pi}$. Suppose that $|T| \leqslant 660$, so that T is one of A_5, A_6, $L_2(7)$, $L_2(8)$ or $L_2(11)$ [20]. Using GAP [30], whose group library contains all primitive permutation groups of degree at most 50, we determine that P must be S_k or A_k where $k \geqslant 10$. But then Lemma 5.3.2 implies that $T = A_{k-1}$, so $k = 6$ or $k = 7$, a contradiction. Suppose instead that $|T| > 660$. Then $|T| \geqslant 1092$ [20], so $1 \leqslant \sum_{\pi \in R(P)} |\pi^P|/|T|^{k-r_\pi} \leqslant \sum_{\pi \in R(P)} |\pi^P|/1092^{k-r_\pi}$. Hence $1092^k \leqslant \sum_{\pi \in R(P)} |\pi^P| 1092^{r_\pi}$. Using GAP [30], we determine that there is no such P, a contradiction. □

Thus Theorem 5.0.1 has been proved, for if we assume that G is primitive, then it is always the case that $\mathrm{Inn}(T) \leqslant \mathrm{Im}(\varphi)$ by Lemma 5.1.2.

Lastly, we use Lemma 3.4.1 to prove a more general version of Theorem 5.0.2.

Proposition 5.3.5. *If* $\mathrm{Inn}(T) \leqslant \mathrm{Im}(\varphi)$ *when* P *is* S_k *or* A_k*, then the proportion of pairs of points from* Ω *that are bases for* G *tends to 1 as* $|G| \to \infty$*.*

Proof. It suffices to prove that $Q(G,2) \to 0$ as $|G| \to \infty$. Let $R(P)$ be a set of representatives for the conjugacy classes of elements of prime order in P, and let r_π be the number of cycles in the full cycle decomposition of π in S_k, including fixed points. Then Lemma 5.2.10 implies that $Q(G,2) \leqslant \sum_{\pi \in R(P)} |\pi^P|/|T|^{k-r_\pi}$. We claim that

$$\sum_{\pi \in R(P)} \frac{|\pi^P|}{|T|^{k-r_\pi}} \leqslant \frac{C}{|T|^{\frac{1}{3}}} \left(\frac{1}{c^k} + \frac{1}{\sqrt{k}} + \frac{2k^2 + 4k}{(k-1)!^{\frac{2}{3}}} \right)$$

for some absolute constants C and $c > 1$, in which case $Q(G,2) \to 0$ as $|G| \to \infty$ since the fact that $|G| \leqslant |T|^k k!$ forces $|T| \to \infty$ or $k \to \infty$ as $|G| \to \infty$.

Suppose that P is S_k or A_k. Then $T = A_{k-1}$ by Lemma 5.3.2. Without loss of generality, we may assume that $(12) \in R(S_k)$. Recall that $k - r_\pi$ is 1 when π is a transposition and at least 2 otherwise. Then

$$\sum_{\pi \in R(P)} \frac{|\pi^P|}{|T|^{k-r_\pi-\frac{1}{3}}} \leqslant \frac{2^{\frac{2}{3}} |(12)^{S_k}|}{(k-1)!^{\frac{2}{3}}} + \frac{2^{\frac{5}{3}} |S_k|}{(k-1)!^{\frac{5}{3}}} \leqslant \frac{2^{\frac{2}{3}} k^2 + 2^{\frac{5}{3}} k}{(k-1)!^{\frac{2}{3}}},$$

and so the claim follows from Lemma 3.4.1. □

As before, Theorem 5.0.2 follows directly from Proposition 5.3.5 as a consequence of Lemma 5.1.2.

5.4 Almost simple quotients of stabilisers of $S_m \wr_r S_r$

In order to prove Theorem 5.0.3, we need to know more about the structure of groups of twisted wreath type with top group $P := S_m \wr_r S_r$ acting imprimitively on $[m] \times [r]$. Since $Q := (S_m \wr_{r-1} S_{r-1}) \times S_{m-1}$ is the stabiliser of a point in $S_m \wr_r S_r$, Lemma 5.1.2 implies we need to determine which quotients of Q are almost simple.

Let T be a non-abelian simple group, and suppose that $T \trianglelefteq Q/N \leqslant \mathrm{Aut}(T)$ where $N \trianglelefteq Q$. Then T is a composition factor of Q, so we deduce that T is either A_m, A_{m-1} or A_{r-1}. As we wish to use the bounds of Lemmas 2.3.2 and 5.2.5 to prove Theorem 5.0.3, and specifically to prove $b(G) \to \infty$ when $r \to \infty$ with m fixed, we need to prove that T cannot be A_{r-1} for infinitely many r. In fact, it turns out that T must be A_{m-1}. In order to show this, which we will do in Section 5.5 using Theorem 5.1.1 [4], we must determine the normal subgroups N of Q for which Q/N is almost simple. Thus we must determine the normal subgroups of $(S_m \wr_{r-1} S_{r-1}) \times S_{m-1}$ and therefore of $S_m \wr_r S_r$. This section is devoted to these three tasks.

We begin with a trivial but useful result. For this section, if G_1 and G_2 are groups, then we denote the projection map of $G_1 \rtimes G_2$ onto G_2 by ρ. Note that ρ is a homomorphism and that $\rho(N) \trianglelefteq G_2$ if $N \trianglelefteq G_1 \rtimes G_2$.

Lemma 5.4.1. *Let $H \leqslant G_1 \rtimes G_2$ for groups G_1 and G_2, and let H_1 be a subgroup of G_1 that is normalised by $H_2 := \rho(H)$. If $H_1 \leqslant H \leqslant H_1 \rtimes H_2$, then $H = H_1 \rtimes H_2$.*

Proof. Note that $H_1 \rtimes H_2 \leqslant G_1 \rtimes G_2$. Let $(h_1, h_2) \in H_1 \rtimes H_2$. Since $h_2 \in \rho(H)$ there exists $h_1' \in G_1$ such that $(h_1', h_2) \in H \leqslant H_1 \rtimes H_2$. Then both h_1 and h_1' are in H_1, so $(h_1, 1)$ and $(h_1', 1)$ are in H, and the latter implies that $(1, h_2) \in H$, so $(h_1, h_2) \in H$. □

Let G be a direct product of groups $G_1, \ldots, G_r$ where $r \geqslant 1$. We denote the i-th projection map of G onto G_i by ρ_i. Let I be a non-empty subset of $[r]$. If $h \in G_i$ for each $i \in I$, then we denote by h^I the element of G whose i-th projection is h if $i \in I$ and 1 otherwise. Similarly, if $H \leqslant G_i$ for each $i \in I$, we denote by H^I the subgroup of G whose i-th projection is H if $i \in I$ and 1 otherwise. Note that $H^I \simeq H^{|I|}$. Using this notation, we make the following observations, the first of which generalises [61, Lemma 1].

Lemma 5.4.2. *Let $H \leqslant G_1 \times G_2$ for groups G_1 and G_2.*

(i) $[G_i, \rho_i(H)]^{\{i\}} = [G_i^{\{i\}}, H]$ for $i = 1, 2$.

(ii) If $\rho_i(H)^{\{i\}} \leqslant H$ for some i, then $H = \rho_1(H) \times \rho_2(H)$.

Proof. (i) If $g_1 \in G_1$ and $(h_1, h_2) \in H$, then $([g_1, h_1], 1) = [(g_1, 1), (h_1, h_2)]$. The result follows. (ii) Apply Lemma 5.4.1 with $H_1 = \rho_i(H)$. □

We say that a group G is *super-perfect* if $[G, N] = N$ for all normal subgroups N of G (this definition comes from [61]). Note that any non-abelian simple group is super-perfect. Now we see that the structure of a normal subgroup of a direct product of a super-perfect group with any other group is particularly nice.

Proposition 5.4.3 ([61])**.** *Let G_1 and G_2 be groups where G_1 is super-perfect. Then $N \trianglelefteq G_1 \times G_2$ if and only if $N = N_1 \times N_2$ where $N_1 \trianglelefteq G_1$ and $N_2 \trianglelefteq G_2$.*

Proof. Suppose that $N \trianglelefteq G_1 \times G_2$, and let $N_i := \rho_i(N)$. Note that $N_i \trianglelefteq G_i$. Then since G_1 is super-perfect, $N_1 = [G_1, N_1]$, but $[G_1, N_1]^{\{1\}} = [G_1^{\{1\}}, N]$ by Lemma 5.4.2(i), and $[G_1^{\{1\}}, N] \leqslant N$, so $N = N_1 \times N_2$ by Lemma 5.4.2(ii). The converse is trivial. □

Let H and K be groups where K acts on $[r]$. Note that for $h \in H$ and $i \in [r]$, we may view $h^{\{i\}}$ as an element of $H \wr_r K$, and so $h^{\{i\}\kappa} = h^{\{i\kappa\}}$ for all $\kappa \in K$. Using this observation, we obtain a useful property of normal subgroups of wreath products.

Lemma 5.4.4. *Let H and K be groups where K acts on $[r]$. Suppose that $N \trianglelefteq H \wr_r K$. If $i \in [r]$ and $\kappa \in \rho(N)$ are such that $i \neq i\kappa$, then $h^{\{i\}}(h^{-1})^{\{i\kappa\}} \in N \cap H^r$ for all $h \in H$.*

Proof. Let $h \in H$. By assumption, there exists some $n := (h_1, \dots, h_r)\kappa \in N$. Let $n^* := (h^{\{i\}}\kappa)^{-1} n (h^{\{i\}}\kappa)(\kappa^{-1} n^{-1} \kappa)$. Then $n^* \in N$ and

$$\begin{aligned} n^* &= (h^{\{i\}}\kappa)^{-1}(h_1, \dots, h_r)\kappa(h^{\{i\}}\kappa)(\kappa^{-1}((h_1, \dots, h_r)\kappa)^{-1}\kappa) \\ &= (h^{-1})^{\{i\kappa\}}(h_{1\kappa^{-1}}, \dots, h_{r\kappa^{-1}})h^{\{i\}}(h^{-1}_{1\kappa^{-1}}, \dots, h^{-1}_{r\kappa^{-1}}) \\ &= (h^{-1})^{\{i\kappa\}} h^{\{i\}}_{i\kappa^{-1}} h^{\{i\}} (h^{\{i\}}_{i\kappa^{-1}})^{-1}. \end{aligned}$$

Since $i\kappa \neq i$, it follows that $(h^{-1})^{\{i\kappa\}}$ commutes with $h^{\{i\}}_{i\kappa^{-1}} h^{\{i\}}$. Hence $h^{\{i\}}(h^{-1})^{\{i\kappa\}} = (h^{\{i\}}_{i\kappa^{-1}})^{-1} n^* h^{\{i\}}_{i\kappa^{-1}}$, but this is also in N, so we are done. □

Using Lemma 5.4.4, we can determine the structure of the normal subgroups of the wreath product $H \wr_r K$ when H is super-perfect. In particular, we find that a normal subgroup is itself a wreath product.

Proposition 5.4.5. *Let H and K be groups where H is super-perfect and K acts transitively on $[r]$. Then $N \trianglelefteq H \wr_r K$ if and only if $N = H' \wr_r K'$ where $H' \trianglelefteq H$, $K' \trianglelefteq K$, and $H' = H$ when $K' \neq 1$.*

Proof. Let N be a normal subgroup of $G := H \wr_r K$. Then $N \cap H^r$ is a normal subgroup of G contained in H^r. Since H is super-perfect, it follows from Proposition 5.4.3 and an induction argument that $N \cap H^r = N_1 \times \cdots \times N_r$ where $N_i \trianglelefteq H$ for all $i \in [r]$. If $n \in N_i$ for

some $i \in [r]$, then $n \in N_{i\kappa}$ for any $\kappa \in K$ since $n^{\{i\kappa\}} = \kappa^{-1} n^{\{i\}} \kappa \in N$. By the transitivity of the action of K on $[r]$, it follows that $N_i = N_j$ for all i and j. Thus $N \cap H^r = (H')^r$ for some $H' \trianglelefteq H$. If $\rho(N)$ is trivial, then we are done since $N = N \cap H^r = (H')^r = H' \wr_r 1$, so we assume otherwise. Then there exists $\kappa \in \rho(N)$ that moves some $i \in [r]$. Let $h \in H$. Then by Lemma 5.4.4, $h^{\{i\}}(h^{-1})^{\{i\kappa\}} \in N$ and thus in $(H')^r$, so $h \in H'$. Hence $H = H'$ and $H^r \leqslant N \leqslant H^r \rtimes \rho(N)$, so by Lemma 5.4.1, $N = H^r \rtimes \rho(N) = H \wr_r \rho(N)$. □

In order to define the normal subgroups of $S_m \wr_r S_r$, we need the following extension of the concept of the sign of a permutation. For any group L and positive integer l, let $\operatorname{sgn}_L^l : (L \rtimes C_2)^l \to \{\pm 1\}$ be defined by

$$(x_1, \ldots, x_l) \mapsto \begin{cases} -1 & \text{if } 2 \nmid |\{i : x_i \notin L\}|, \\ 1 & \text{otherwise,} \end{cases}$$

for all $(x_1, \ldots, x_l) \in (L \rtimes C_2)^l$. We omit the L and l when the context is clear. Write $\overline{x}$ for $(x_1, \ldots, x_l) \in (L \rtimes C_2)^l$. We now explore some basic properties of sgn. Note that if x and y are in $L \rtimes C_2 \setminus L$, then $xy \in L$.

Lemma 5.4.6. *Let L be a group, and let K be a group acting on $[l]$ so that K acts on $(L \rtimes C_2)^l$ by permuting the coordinates. Let $\overline{x}, \overline{y} \in (L \rtimes C_2)^l$ and $\kappa \in K$. Then*

(i) $\operatorname{sgn}(\overline{x}\ \overline{y}) = \operatorname{sgn}(\overline{x}) \operatorname{sgn}(\overline{y})$,

(ii) $\operatorname{sgn}(\overline{x}^{-1}) = \operatorname{sgn}(\overline{x})$,

(iii) $\operatorname{sgn}(\overline{x}^{\kappa}) = \operatorname{sgn}(\overline{x})$,

(iv) $\operatorname{sgn}(\overline{y}^{-1}\overline{x}\ \overline{y}) = \operatorname{sgn}(\overline{x})$.

Proof. Parts (ii) and (iii) are immediate, and part (iv) follows from (i) and (ii), so it remains to prove (i). Let

$$\begin{aligned} I &:= \{i : x_i \notin L \text{ and } y_i \notin L\}, \\ I_x &:= \{i : x_i \notin L \text{ and } y_i \in L\}, \\ I_y &:= \{i : x_i \in L \text{ and } y_i \notin L\}. \end{aligned}$$

Then $|\{i : x_i \notin L\}| = |I| + |I_x|$ and $|\{i : y_i \notin L\}| = |I| + |I_y|$, so

$$|\{i : x_i y_i \notin L\}| = |I_x| + |I_y| = |\{i : x_i \notin L\}| + |\{i : y_i \notin L\}| - 2|I|,$$

from which (i) follows. □

Let H and K be groups where K acts on $[r]$. Suppose that A is an index 2 subgroup of H, B is an index 2 subgroup of K, $t \in H \setminus A$ is an involution, and $\tau \in K \setminus B$ is an

involution. Then $H = A \rtimes \langle t \rangle$ and $K = B \rtimes \langle \tau \rangle$. Let

$$\begin{aligned} D(A,r) &:= A^r \cup \{(h_1,\dots,h_r) \in H^r : \ \operatorname{sgn}_A^1(h_i) = -1 \text{ for all } i \in [r]\}, \\ E(A,r) &:= \{(h_1,\dots,h_r) \in H^r : \operatorname{sgn}_A^r((h_1,\dots,h_r)) = 1\}, \\ F(A,B,r) &:= \{(h_1,\dots,h_r)\kappa \in H \wr_r K : \operatorname{sgn}_A^r((h_1,\dots,h_r)) = \operatorname{sgn}_B^1(\kappa)\}. \end{aligned}$$

Note that $D(A,r)$, $E(A,r)$ and $F(A,B,r)$ are normal subgroups of $H \wr_r K$ by Lemma 5.4.6. Moreover, $D(A,r)$ is a subgroup of $E(A,r)$ when r is even, and $E(A,r)$ is always a subgroup of $F(A,B,r)$. When $H = S_m$ and $K = S_r$, we write $D_{m,r}$, $E_{m,r}$ and $F_{m,r}$ for $D(A,r)$, $E(A,r)$ and $F(A,B,r)$ respectively, and if the context permits, we write D, E and F for $D(A,r)$, $E(A,r)$ and $F(A,B,r)$.

Let us investigate D more closely. Certainly $D = H$ when $r = 1$ and $D = E$ when $r = 2$, but D is a proper subgroup of E for r even and $r \geqslant 4$. Since every element of $D \setminus A^r$ can be written as $\overline{a}t^{[r]}$ for some $\overline{a} \in A^r$, it follows that $D = A^r\langle t^{[r]} \rangle$.

Now let us consider E. Note that E contains A^r (and does so properly for $r \geqslant 2$) and that $t^{\{i,j\}} \in E$ for all distinct i and j. In fact, $\{t^{\{i,j\}} : i \neq j\}$ is a generating set for $E(1,r)$, and so $E = A^r E(1,r)$ since any element of E is a product of an element of A^r with t^I for some $I \subseteq [r]$ where $|I|$ is even. Note also that if $(h_1,\dots,h_r) \in H^r \setminus E$, then $(h_1t^{-1}, h_2 \dots, h_r) \in E$ and $(h_1,\dots,h_r) = (h_1t^{-1}, h_2, \dots, h_r)t^{\{1\}}$, so $H^r = E\langle t^{\{1\}} \rangle$. In particular, E has index 2 in H^r.

Lastly, we consider F. Clearly $E \rtimes B$ is a normal subgroup of $H \wr_r K$ of index 4 since $[H^r : E] = 2$, and F properly contains $E \rtimes B$, so F has index 2 in $H \wr_r K$. Indeed, $H \wr_r K = F\langle \tau \rangle$. Furthermore, it can be shown that $F = (E \rtimes B)\langle t^{\{1\}}\tau \rangle$.

Now we are in a position to determine the normal subgroups of $S_m \wr_r S_r$.

Proposition 5.4.7. *If $m \geqslant 2$ and $r \geqslant 2$, then $N \trianglelefteq S_m \wr_r S_r$ if and only if N is $D_{m,r}$, $F_{m,r}$, $E_{m,r} \rtimes K$ where $K \trianglelefteq S_r$, or $H \wr_r K$ where $H \trianglelefteq S_m$, $K \trianglelefteq S_r$, and $H = S_m$ if $K \neq 1$.*

Proof. Let $G := S_m \wr_r S_r$. Suppose that N is a normal subgroup of G, and let $M := N \cap S_m^r$. Note that $M \trianglelefteq G$. Suppose first of all that $M \leqslant A_m^r$. We claim that $M = H^m$ where $H \trianglelefteq A_m$. If M is trivial, then the claim is certainly true, so we assume otherwise. In particular, $m \geqslant 3$. The claim follows from Proposition 5.4.5 when $m \geqslant 5$ since A_m is super-perfect, so we assume that $m = 3$ or $m = 4$. Since $M \trianglelefteq S_m^r$, it follows that $g := (123)^I(12)(34)^J \in M$ for some (possibly empty) subsets I and J of $[r]$ whose intersection is empty and union is non-empty. Let V denote the Klein four-group in S_4. If $M \not\leqslant V^r$ (when $m = 4$), then we may choose g so that $I \neq \emptyset$. Let $i \in I$. Conjugating g by $(23)^{I\setminus\{i\}}$ we obtain that $h := (123)^{\{i\}}(132)^{I\setminus\{i\}}(12)(34)^J \in M$, and so $(132)^{\{i\}} = gh \in M$. This implies that $A_m^{\{i\}} \leqslant M$, but S_r is transitive, so $M = A_m^r$, as desired. Suppose then that

$M \leqslant V^r$, so that $m = 4$ and $I = \emptyset$, and choose $j \in J$. Conjugating g by $(23)^{\{j\}}$ we obtain that $h := (13)(24)^{\{j\}}(12)(34)^{J\setminus\{j\}} \in M$, and so $(14)(23)^{\{j\}} = gh \in M$, which implies that $V^{\{j\}} \leqslant M$. Again by the transitivity of S_r, we obtain that $M = V^r$, and we are done.

Suppose now that $M \not\leqslant A_m^r$. Then there exists $(h_1, \ldots, h_r) \in M$ such that $h_{i_0} \in S_m \setminus A_m$ for some $i_0 \in [r]$. If $m \geqslant 3$, then we may choose $h \in S_m$ such that $[h, h_{i_0}] \neq 1$. Then $[h, h_{i_0}]^{\{i_0\}} = [(h_1, \ldots, h_r), h^{\{i_0\}}] \in A_m^{\{i_0\}} \cap M$, so $A_m^{\{i_0\}} \cap M$ is a non-trivial normal subgroup of $A_m^{\{i_0\}}$. Also, if $m = 4$, then h_{i_0} is either a 4-cycle or a transposition, say (1234) or (12). But $[(123), h_{i_0}]$ is then a 3-cycle in either case, so $A_4^{\{i_0\}} \cap M \neq V$. Thus $A_m^{\{i_0\}} \cap M = A_m^{\{i_0\}}$ for all $m \geqslant 2$. Since S_r is transitive, we conclude that $A_m^r \leqslant M$. Let $t := (12) \in S_m$. Then for each $h_j \in S_m \setminus A_m$, there exists $a_j \in A_m$ such that $h_j = a_j t$, and thus $t^I \in M$ for some $\emptyset \neq I \subseteq [r]$. If every element of $M \setminus A_m^r$ is of the form $\overline{a}t^{[r]}$ for some $\overline{a} \in A_m^r$, then $M = D_{m,r}$, so we may assume that $I \neq [r]$. Let $J := I \cup \{j_0\} \setminus \{i_0\}$ where $j_0 \in [r] \setminus I$ and $i_0 \in I$. Then $t^J = t^{I(i_0 j_0)} = (i_0 j_0) t^I (i_0 j_0) \in M$, and so $t^{\{i_0, j_0\}} = t^I t^J \in M$. But S_r is 2-transitive, so $t^{\{i,j\}} \in M$ for all distinct $i, j \in [r]$. Thus $E_{m,r} \leqslant M$ since $A_m^r \leqslant M$, so $M = E_{m,r}$ or S_m^r. (The latter occurs precisely when $t^{\{i\}} \in M$ for some i.)

We have proved that if $N \trianglelefteq G$ then $N \cap S_m^r$ is one of $D_{m,r}$, $E_{m,r}$, or $H \wr_r 1$ where $H \trianglelefteq S_m$. We are therefore done if $\rho(N) = 1$, so we suppose otherwise. Then the normal subgroup $\rho(N)$ must contain at least one non-trivial conjugacy class of S_r and is therefore transitive on $[r]$. Hence Lemma 5.4.4 implies that $h^{\{i\}}(h^{-1})^{\{j\}} \in N \cap S_m^r$ for any $h \in S_m$ and distinct $i, j \in [r]$. By considering the list of possibilities for $N \cap S_m^r$ given above, it follows that $N \cap S_m^r$ is $E_{m,r}$ or S_m^r. Note that if $N \leqslant (N \cap S_m^r) \rtimes \rho(N)$, then $N = (N \cap S_m^r) \rtimes \rho(N)$ by Lemma 5.4.1, in which case we are done; we assume, therefore, that $N \not\leqslant (N \cap S_m^r) \rtimes \rho(N)$. In particular, it follows that $\rho(N) \not\leqslant N$, $N \cap S_m^r = E_{m,r}$ and $t^{\{1\}} \notin N$.

We claim that if $\kappa \in \rho(N)$, then $\kappa \in N$ if and only if $t^{\{1\}}\kappa \notin N$. If $\kappa \in N$ then $t^{\{1\}}\kappa \notin N$ since $t^{\{1\}} \notin N$. On the other hand, choose any $(y_1, \ldots, y_r)\kappa \in N$. Note that if $(y_1, \ldots, y_r) \notin E_{m,r}$, then since $E_{m,r} \leqslant N$ and $S_m^r = E_{m,r}\langle t^{\{1\}}\rangle$, it follows that $t^{\{1\}}\kappa \in N$. Thus if $t^{\{1\}}\kappa \notin N$, then $(y_1, \ldots, y_r) \in E_{m,r} \leqslant N$, so $\kappa \in N$. Hence the claim is true, and we refer to this equivalence as $(*)$. We now use $(*)$ to prove that $N = F_{m,r}$.

Let $\kappa \in \rho(N)$ and $\sigma \in S_r$. If $\kappa \in N$, then $[\kappa, \sigma] \in N$. On the other hand, if $\kappa \notin N$, then $\sigma^{-1}\kappa\sigma \in \rho(N) \setminus N$, so $t^{\{1\}}\sigma^{-1}\kappa\sigma \in N$ by $(*)$. But $t^{\{1\}}\sigma^{-1}\kappa\sigma = t^{\{1\}}\kappa[\kappa, \sigma]$, and $(*)$ implies that $t^{\{1\}}\kappa \in N$ since $\kappa \notin N$, so we again have $[\kappa, \sigma] \in N$. Hence $[\rho(N), S_r] \leqslant N$. If $\rho(N) \leqslant A_r$, then $\rho(N) = [\rho(N), S_r] \leqslant N$, a contradiction, so $\rho(N) = S_r$, which then implies that $A_r = [S_r, S_r] \leqslant N$. Thus $E_{m,r} \rtimes A_r < N < G$, and this implies that N and $F_{m,r}$ have the same order. But $F_{m,r} = (E_{m,r} \rtimes A_r)\langle t^{\{1\}}\tau\rangle$ where $\tau := (12) \in S_r = \rho(N)$, and $\tau \notin N$ (or else $\rho(N) = A_r\langle\tau\rangle \leqslant N$), so $t^{\{1\}}\tau$ lies in N by $(*)$. Thus $N = F_{m,r}$. $\square$

Our next task is to determine the structure of the normal subgroups of $S_m \wr_r S_r \times S_{m-1}$. Since we know the structure of the normal subgroups of $S_m \wr_r S_r$, this can be done using a method described in [61] that finds all of the normal subgroups of a direct product $G_1 \times G_2$. We now describe this method.

Let G_1 and G_2 be groups. Note that if $N \trianglelefteq G_1 \times G_2$ and $N_i := \rho_i(N)$ for $i = 1$ and $i = 2$, then Lemma 5.4.2 and the normality of N imply that $[G_1, N_1] \times [G_2, N_2] \leqslant N \leqslant N_1 \times N_2$. Now suppose that M_i is any normal subgroup of G_i for both i. Note that $[G_1, M_1] \times [G_2, M_2] = [G_1 \times G_2, M_1 \times M_2]$. In particular, if L is a group for which $[G_1, M_1] \times [G_2, M_2] \leqslant L \leqslant M_1 \times M_2$, then L must in fact be normal in $G_1 \times G_2$. Moreover, there is a one-to-one correspondence between the subgroups of $M_1 \times M_2$ that contain $[G_1, M_1] \times [G_2, M_2]$ and the subgroups of the abelian group $(M_1 \times M_2)/[G_1 \times G_2, M_1 \times M_2] \simeq M_1/[G_1, M_1] \times M_2/[G_2, M_2]$. Therefore, in order to find all of the normal subgroups of $G_1 \times G_2$, it suffices to find, for each $M_1 \trianglelefteq G_1$ and $M_2 \trianglelefteq G_2$, all subgroups M of $M_1/[G_1, M_1] \times M_2/[G_2, M_2]$ for which $\rho_i(M) = M_i/[G_i, M_i]$, as each such M corresponds to a unique subgroup M^* of $M_1 \times M_2$ containing $[G_1 \times G_2, M_1 \times M_2]$, in which case $M^* \trianglelefteq G_1 \times G_2$ with $\rho_i(M^*) = M_i$.

To this end, we need to determine the commutator group $[S_m \wr_r S_r, N]$ for every normal subgroup N of $S_m \wr_r S_r$.

Lemma 5.4.8. *If $m \geqslant 2$, $r \geqslant 2$ and $N \trianglelefteq S_m \wr_r S_r$, then $[S_m \wr_r S_r, N] = (N \cap E_{m,r}) \rtimes (N \cap A_r)$ unless $N = D_{m,r}$ and $r \geqslant 2$, in which case $[S_m \wr_r S_r, N] = A_m^r$.*

Proof. Let $G := S_m \wr_r S_r$. Note that $[G, N]$ is a normal subgroup of G contained in N. First suppose that $N \leqslant A_m^r$. Then $N \cap E_{m,r} = N$ and $N \cap A_r = 1$, so we must show that $[G, N] = N$. But $N = M^r$ where $M \trianglelefteq A_m$ by Proposition 5.4.7, and so $[G, N] \geqslant [S_m^r, M^r] = [S_m, M]^r = M^r$, as desired. Hence we assume that $N \not\leqslant A_m^r$.

Let $(g_1, \ldots, g_r)\gamma$ and $(n_1, \ldots, n_r)\nu$ be elements of G. Write $\overline{g} := (g_1, \ldots, g_r)$ and $\overline{n} := (n_1, \ldots, n_r)$. Then

$$[\overline{g}\gamma, \overline{n}\nu] = (\overline{g}^{-1}(\overline{n}^{-1})^{\nu}\overline{g}^{\nu}\overline{n}^{\gamma^{-1}\nu})^{\gamma}[\gamma, \nu]. \tag{$*$}$$

In fact, since $\operatorname{sgn}_{A_m}^r((\overline{g}^{-1}(\overline{n}^{-1})^{\nu}\overline{g}^{\nu}\overline{n}^{\gamma^{-1}\nu})^{\gamma}) = 1$ and $\operatorname{sgn}_{A_r}^1([\gamma, \nu]) = 1$, it follows that $[G, N] \leqslant [G, G] \leqslant E_{m,r} \rtimes A_r$.

Suppose that $N = D_{m,r}$ where $r \geqslant 2$. Note that $[G, N] \geqslant [S_m^r, A_m^r] = A_m^r$. Moreover, by equation $(*)$ with $\nu = 1$, the $(i\gamma)$-th projection of $[\overline{g}\gamma, \overline{n}]$ is $g_i^{-1}n_i^{-1}g_i n_{i\gamma}$ for all $i \in [r]$, and $g_i^{-1}n_i^{-1}g_i n_{i\gamma} \in A_m$ for all $i \in [r]$ since either $n_j \in A_m$ for all $j \in [r]$, or $n_j \notin A_m$ for all $j \in [r]$. Thus $[G, N] \leqslant A_m^r$, as desired.

By Proposition 5.4.7, it follows that $E_{m,r} \leqslant N$, and if $E_{m,r} = N$, then $r \geqslant 3$ since $E_{m,2} = D_{m,2}$. Here $[G, N] \leqslant N \cap (E_{m,r} \rtimes A_r) = E_{m,r} \rtimes (N \cap A_r)$ by Lemma 2.1.1, so we must show that $[G, N]$ contains both $E_{m,r}$ and $N \cap A_r$. For the latter, since $N \cap A_r \leqslant A_r$, we have $[G, N] \geqslant [S_r, N \cap A_r] = N \cap A_r$. For the former, $[G, N] \cap S_m^r$ is a normal subgroup of G contained in $E_{m,r}$, so by Proposition 5.4.7 it suffices to show that $[G, N] \cap S_m^r$ contains some element that is not in $D_{m,r}$ when $r \geqslant 3$, and not in A_m^2 when $r = 2$.

Let $t := (12)$, and let $(g_1, \ldots, g_r)\gamma$ and $(n_1, \ldots, n_r)\nu$ be elements of G for which $g_1 = t$, $g_i = 1$ for $1 \neq i \in [r]$, $\gamma = 1$, and ν is any element moving 1. Then by equation $(*)$, $[\overline{g}, \overline{n}\nu] = t^{\{1\}}(n_1^{-1}tn_1)^{\{1\nu\}}$, and this element does not lie in $D_{m,r}$ when $r \geqslant 3$ or in A_m^2 when $r = 2$. Thus we need only show that $[\overline{g}, \overline{n}\nu]$ lies in $[G, N]$, and this is true if either $\overline{g} \in N$ or $\nu \in \rho(N)$. If $\rho(N) \neq 1$, then clearly the latter is true, and if $N = S_m^r$, then the former is true. Thus we are left with the case when $N = E_{m,r}$ and $r \geqslant 3$. In the definition of $\overline{g}\gamma$ and $\overline{n}\nu$ above, replace $g_3 = 1$ with t and set ν to be (123). Then

$$[\overline{g}, \overline{n}\nu] = t^{\{1,3\}}(n_1^{-1}tn_1)^{\{2\}}(n_3^{-1}tn_3)^{\{1\}} = ([t, n_3], n_1^{-1}tn_1, t, 1, \ldots, 1).$$

Since $\overline{g} \in N$, and since $[t, n_3] \in A_m$ but $t \notin A_m$, it follows that $[\overline{g}, \overline{n}\nu] \in [G, N] \setminus D_{m,r}$. □

For future use, Table 5.1 lists the results of Proposition 5.4.7 and Lemma 5.4.8. The only new information in this table is that $G/[G, G] \simeq C_2 \times C_2$, but this is clear since its elements are $E_{m,r} \rtimes A_r$, $(E_{m,r} \rtimes A_r)(12)^{\{1\}}$, $(E_{m,r} \rtimes A_r)(12)$ and $(E_{m,r} \rtimes A_r)(12)^{\{1\}}(12)$.

N		$[G : N]$	$[G, N]$	$N/[G, N]$
1		$m!^r r!$	1	1
A_m^r	$m \geqslant 3$	$2^r r!$	A_m^r	1
$D_{m,r}$		$2^{r-1} r!$	A_m^r	C_2
$E_{m,r}$	$r \geqslant 3$	$2r!$	$E_{m,r}$	1
S_m^r		$r!$	$E_{m,r}$	C_2
$E_{m,r} \rtimes A_r$	$r \geqslant 3$	4	$E_{m,r} \rtimes A_r$	1
$E_{m,r} \rtimes S_r$		2	$E_{m,r} \rtimes A_r$	C_2
$F_{m,r}$		2	$E_{m,r} \rtimes A_r$	C_2
$S_m \wr_r A_r$	$r \geqslant 3$	2	$E_{m,r} \rtimes A_r$	C_2
$S_m \wr_r S_r$		1	$E_{m,r} \rtimes A_r$	$C_2 \times C_2$
V^r	$m = 4$	$6^r r!$	V^r	1
$E_{m,4} \rtimes V$	$r = 4$	12	$E_{m,4} \rtimes V$	1
$S_m \wr_4 V$	$r = 4$	6	$E_{m,4} \rtimes V$	C_2

Table 5.1: The normal subgroups N of $G = S_m \wr_r S_r$ for $m \geqslant 2$ and $r \geqslant 2$.

Now we determine the normal subgroups of $(S_m \wr_r S_r) \times S_{m-1}$. We only need to determine those normal subgroups N for which N is a proper subgroup of $\rho_1(N) \times \rho_2(N)$,

for if $N = \rho_1(N) \times \rho_2(N)$, then N is the direct product of normal subgroups of $S_m \wr_r S_r$ and S_{m-1} respectively, and by Proposition 5.4.7, we know the structure of all such groups.

Lemma 5.4.9. *Suppose that $m \geqslant 3$ and $r \geqslant 1$. Let $t := (12)$ and $\tau := (12)$. If $N \trianglelefteq Q := (S_m \wr_r S_r) \times S_{m-1}$ and $N < \rho_1(N) \times \rho_2(N)$, then*

$$N = X \times A_{m-1}\langle (y,t) : y \in Y \rangle$$

where the group X and the set Y are defined in Table 5.2.

X	$y \in Y$		$[Q:N]$
A_m^r	$t^{[r]}$		$2^r r!$
$E_{m,r}$	$t^{\{1\}}$	$r \geqslant 2$	$2r!$
$E_{m,4} \rtimes V$	$t^{\{1\}}$	$r = 4$	12
$E_{m,r} \rtimes A_r$	τ	$r \geqslant 2$	4
$E_{m,r} \rtimes A_r$	$t^{\{1\}}\tau$	$r \geqslant 2$	4
$E_{m,r} \rtimes A_r$	$t^{\{1\}}$	$r \geqslant 3$	4
$E_{m,r} \rtimes A_r$	$t^{\{1\}}$, τ	$r \geqslant 2$	2
$E_{m,r} \rtimes A_r$	τ, $t^{\{1\}}\tau$	$r \geqslant 2$	2
$E_{m,r} \rtimes A_r$	$t^{\{1\}}$, $t^{\{1\}}\tau$	$r \geqslant 2$	2

Table 5.2: Normal subgroups N of Q for which $N < \rho_1(N) \times \rho_2(N)$.

Proof. We proceed with the method described earlier in this section for finding all normal subgroups of a direct product. Let $G_1 := S_m \wr_r S_r$ and $G_2 := S_{m-1}$. Let M_1 and M_2 be normal subgroups of G_1 and G_2 respectively. Recall that as M ranges over all subgroups of $M_1/[G_1, M_1] \times M_2/[G_2, M_2]$ for which $\rho_i(M) = M_i/[G_i, M_i]$ for both i, we obtain all normal subgroups M^* of Q for which $\rho_i(M^*) = M_i$ for both i, where M^* denotes the unique subgroup of $M_1 \times M_2$ containing $[G_1 \times G_2, M_1 \times M_2]$ that corresponds to M.

In fact, since we are only interested in those M^* for which $M^* < M_1 \times M_2$, it follows that $M < M_1/[G_1, M_1] \times M_2/[G_2, M_2]$. Moreover, $M_i/[G_i, M_i] \neq 1$ for both i, for if $M_i = [G_i, M_i]$ for some i, then $\rho_i(M^*) = M_i \leqslant M^*$ by Lemma 5.4.2(i), and so $M^* = M_1 \times M_2$ by Lemma 5.4.2(ii). In particular, since $[G_2, M_2] = M_2$ for all $M_2 \leqslant A_{m-1}$, we may assume that $M_2 = S_{m-1}$. Similarly, if $r = 1$ then $M_1 = S_m$, and if $r \geqslant 2$ then M_1 is one of the groups in Table 5.1 that do not have a 1 in the last column. Note that $M_2/[G_2, M_2] = C_2$ and $M_1/[G_1, M_1]$ is either C_2 or $C_2 \times C_2$. Write $C_2 = \langle c \rangle$.

Suppose that $M_1/[G_1, M_1] = C_2$. Then M is a proper subgroup of $C_2 \times C_2$ with $\rho_i(M) = C_2$ for both i, so $M = \langle (c, c) \rangle$. It follows that if $m_1 \in M_1 \setminus [G_1, M_1]$ and $m_2 \in M_2 \setminus [G_2, M_2]$, then $M^* = ([G_1, M_1] \times [G_2 \times M_2])\langle (m_1, m_2) \rangle$. We will always take m_2

to be t. The following table displays the chosen m_1 for each M_1 (including $S_m = D_{m,1}$).

$D_{m,r}$	S_m^r	$S_m \wr_4 V$	$E_{m,r} \rtimes S_r$	$F_{m,r}$	$S_m \wr_r A_r$
$t^{[r]}$	$t^{\{1\}}$	$t^{\{1\}}$	τ	$t^{\{1\}}\tau$	$t^{\{1\}}$

Note that $[G_2, M_2] = A_{m-1}$ and $[G_1, M_1] = A_m$ when $M_1 = S_m$. Since $[G_1, M_1]$ is given by Table 5.1 for all remaining M_1, we get the first six normal subgroups listed in Table 5.2.

It remains to consider the case when $M_1 = G_1$ and $G_1/[G_1, G_1] = C_2 \times C_2$. Here M is a proper subgroup of $(C_2 \times C_2) \times C_2$ with $\rho_1(M) = C_2 \times C_2$ and $\rho_2(M) = C_2$. Moreover, M must have at least four elements, so $|M| = 4$. It is a routine verification that M is one of $\langle (c, 1, c), (1, c, c) \rangle$, $\langle (1, c, c), (c, c, c) \rangle$ or $\langle (c, 1, c), (c, c, c) \rangle$. Let $R := [G_1, M_1] \times [G_2, M_2]$. We interpret the three possibilities for M above by associating the first c with $t^{\{1\}}[G_1, G_1]$, the second with $\tau[G_1, G_1]$, and the third with $t[G_2, M_2]$. Then $M^* = R\langle (y_1, t), (y_2, t) \rangle$ where (y_1, y_2) is one of $(t^{\{1\}}, \tau)$, $(\tau, t^{\{1\}}\tau)$, or $(t^{\{1\}}, t^{\{1\}}\tau)$. Since $R = (E_{m,r} \rtimes A_r) \times A_{m-1}$, we have found the three remaining normal subgroups listed in Table 5.2. □

At last we determine precisely which quotients of $(S_m \wr_r S_r) \times S_{m-1}$ are almost simple.

Lemma 5.4.10. *Suppose that $m \geqslant 2$ and $r \geqslant 1$. Let $Q := (S_m \wr_r S_r) \times S_{m-1}$ and $N \trianglelefteq Q$. Then Q/N is almost simple if and only if N is as listed in Table 5.3.*

N	Q/N	
$S_m \wr_r S_r \times 1$	S_{m-1}	$m \geqslant 6$
$S_m^r \times S_{m-1}$	S_r	$r \geqslant 5$
$1 \times S_{m-1}$	S_m	$m \geqslant 5$, $r = 1$

Table 5.3: $N \trianglelefteq Q$ for which Q/N is almost simple.

Proof. Suppose that Q/N is almost simple. Then there exists a non-abelian simple group T for which $T \trianglelefteq Q/N \leqslant \mathrm{Aut}(T)$, and so T is a composition factor of Q. Hence $T = A_n$ where $n \in \{m, m-1, r\}$ and $n \geqslant 5$. Then $\mathrm{Aut}(A_n) = S_n$ when $n \neq 6$ and $|\mathrm{Aut}(A_6)| = 2|S_6|$ by Proposition 2.2.2.

Let $N_i := \rho_i(N)$ and suppose that $N < N_1 \times N_2$. Then $m \geqslant 3$ and N is one of the subgroups listed in Table 5.2. But $[Q : N]$ must be at least 60, so N is one of the first two groups listed. However, the only non-abelian composition factor of Q/N in either case is A_r with $r \geqslant 5$, so $Q/N \leqslant \mathrm{Aut}(A_r)$. By considering the orders of $[Q : N]$, it follows that $r = 6$ and $N = E_{m,6} \times A_{m-1}\langle (t^{\{1\}}, t) \rangle$. Then $N\langle (1, t) \rangle = S_m^6 \times S_{m-1} \trianglelefteq Q$, so $C_2 \simeq N\langle (1, t) \rangle / N \trianglelefteq Q/N$, contradicting Lemma 3.1.2.

Hence we may assume that $N = N_1 \times N_2$. Suppose, first of all, that N_2 is a proper subgroup of S_{m-1}. Note that $m \geqslant 3$. If N_2 is also non-trivial, then $S_{m-1}/N_2 = C_2$ (or S_3 when $m = 5$), in which case C_2 (or S_3) is a normal subgroup of Q/N, contradicting Lemma 3.1.2. If instead $N_2 = 1$, then $Q/N \simeq C \times S_{m-1}$ for some C, so $C = 1$ by Lemma 3.1.2. Thus $N = S_m \wr_r S_r \times 1$ and $Q/N = S_{m-1}$, as desired.

We may assume therefore that $N_2 = S_{m-1}$ where $m \geqslant 2$. Then $Q/N = (S_m \wr_r S_r)/N_1$. Let $G := S_m \wr_r S_r$. Since $[G : N_1] \geqslant 60$, a quick consideration of Table 5.1 reveals that $N_1 \leqslant S_m^r$ (for $r \geqslant 1$). If N_1 is non-trivial, then only A_r can be a non-abelian composition factor of G/N_1, so $G/N_1 \leqslant \mathrm{Aut}(A_r)$ and $r \geqslant 5$. Thus N_1 is either $E_{m,6}$ or S_m^r with $r \geqslant 5$. In the latter case, $N = S_m^r \times S_{m-1}$ and $Q/N = S_r$, as desired, so we may assume that $N_1 = E_{m,6}$. Then $C_2 \simeq S_m^6/N_1 \trianglelefteq G/N_1$, contradicting Lemma 3.1.2. Hence $N_1 = 1$ and G is almost simple. But Proposition 5.4.7 implies that A_m^r (or V^r when $m = 4$) is a minimal normal subgroup of G, and any such group equals A_n by Lemma 3.1.2, so $r = 1$ and $m \geqslant 5$. Then $N = 1 \times S_{m-1}$ and $Q/N = S_m$, as desired. □

5.5 The imprimitive case

In this section, we focus on groups of twisted wreath type whose top group is imprimitive. In particular, we focus on the case when the top group is as large as possible, namely the group $S_m \wr_r S_r$ acting imprimitively on $[m] \times [r]$, and we prove Theorem 5.0.3. We also prove Theorem 5.0.4 at the end of this section.

In order to prove Theorem 5.0.3, we wish to use the results of the last section to determine the structure of a group G of twisted wreath type with top group $S_m \wr_r S_r$. Like when the top group is the alternating or symmetric group, there are very few possibilities for the socle of G. In fact, up to permutation isomorphism, there is exactly one group of twisted wreath type with top group $S_m \wr_r S_r$ for each m and r.

Proposition 5.5.1. *Suppose that $m \geqslant 2$ and $r \geqslant 1$. Let $P := S_m \wr_{r+1} S_{r+1}$ where P acts imprimitively on $[m] \times [r+1]$. If $s \in S_{m-1}$, let $\varphi_s : A_{m-1} \to A_{m-1}$ be defined by $t \mapsto s^{-1}ts$ for all $t \in A_{m-1}$, and define*

$$\begin{aligned} \varphi : (S_m \wr_r S_r) \times S_{m-1} &\to \mathrm{Aut}(A_{m-1}) \\ ((h_1, \ldots, h_r)\pi, s) &\mapsto \varphi_s. \end{aligned}$$

Then $A_{m-1} \operatorname{twr}_\varphi P$ is a group of twisted wreath type when $m \geqslant 6$. Moreover, if G is a group of twisted wreath type with top group P, then $m \geqslant 6$ and G is permutation isomorphic to $A_{m-1} \operatorname{twr}_\varphi P$.

To prove Proposition 5.5.1, we will need the following technical result.

Lemma 5.5.2. *Let R be a subgroup of S_m for which $S_{m-1} \leqslant N_{S_m}(R)$ and $R \cap A_{m-1} = 1$, where S_{m-1} and A_{m-1} fix the same point of $[m]$ and $m \geqslant 5$. Then $R = 1$.*

Proof. Suppose that R is not trivial, and let 1 be the point that is fixed by S_{m-1} and A_{m-1}. Let s be a non-trivial element of R, and suppose that $1s = i$. If $i = 1$, then $s \notin A_{m-1}$ as $R \cap A_{m-1} = 1$, but $s^2 \in R \cap A_{m-1}$, so s is an odd involution. Then $s^{S_{m-1}} \subseteq R$ since $S_{m-1} \leqslant N_{S_m}(R)$, but the elements of $s^{S_{m-1}}$ generate S_{m-1}, so $S_{m-1} \leqslant R$, a contradiction. Thus $i \neq 1$, and no non-trivial element of R fixes 1. If $js = 1$ where $j \neq i$, then for any $k \notin \{1, i, j\}$, the element $s(jk)s^{-1}(jk) \in R$ fixes 1 and moves j to k, a contradiction. Thus $is = 1$. Then s is an involution, or else s^2 is a non-trivial element of R fixing 1. Suppose that s fixes some j. Then $(1ij) = s(ij)s^{-1}(ij) \in R$, but we have already seen that the existence of such an element in R leads to a contradiction. Thus s is fixed-point-free; in particular, $m \geqslant 6$. Without loss of generality, the full cycle decomposition of s has the form $(1i)(23)(45)s'$ for some involution s'. Since $S_{m-1} \leqslant N_{S_m}(R)$, it follows that $(1i)(23)(45)s'(1i)(24)(35)s'$ is a non-trivial element of R fixing 1, a contradiction. □

Now we prove Proposition 5.5.1 by using Theorem 5.1.1 [4] to determine when we have a group of twisted wreath type.

Proof of Proposition 5.5.1. Let $Q := (S_m^r \times S_{m-1}) \rtimes S_r$. Then Q is the stabiliser of the point $(m, r+1)$ under the imprimitive action of P on $[m] \times [r+1]$. Clearly the groups Q and $(S_m \wr_r S_r) \times S_{m-1}$ are naturally isomorphic, but this latter group is easier to work with, so we will often view Q as $(S_m \wr_r S_r) \times S_{m-1}$.

Suppose that $m \geqslant 6$. We claim that $A_{m-1} \operatorname{twr}_\varphi P$ is a group of twisted wreath type, and we will prove this by establishing conditions (i)-(iii) of Theorem 5.1.1 [4]. Let $M := S_m^{r+1}$, $U := \ker(\varphi) = S_m \wr_r S_r \times 1$ and $V := \operatorname{Inn}(A_{m-1})\varphi^{-1} = (S_m \wr_r S_r) \times A_{m-1}$. Then $M \trianglelefteq P$ and $MU = MV$. Let $U' := M \cap U = S_m^r \times 1$ and $V' := M \cap V = S_m^r \times A_{m-1}$. Clearly $V'/U' \simeq A_{m-1}$, so (i) is true, and (ii) is true since $Q = N_P(V')$ and $Q \leqslant N_P(U')$. Let R be as in (iii). Then $S_m^r \leqslant R \leqslant S_m^{r+1}$, so by Lemma 5.4.2(ii), $R = S_m^r \times R_1$ where R_1 is some subgroup of S_m. But $R \cap V' = U'$, so $R_1 \cap A_{m-1} = 1$, and R is normalised by Q, so R_1 is normalised by S_{m-1}. Thus $R_1 = 1$ by Lemma 5.5.2, so $R = S_m^r = U'$, as desired. Hence $A_{m-1} \operatorname{twr}_\varphi P$ is a group of twisted wreath type.

Now let G be any group of twisted wreath type with top group P. Then $G = T \operatorname{twr}_\theta P$ for some non-abelian simple group T and homomorphism $\theta : Q \to \operatorname{Aut}(T)$. We claim that G is permutation isomorphic to $A_{m-1} \operatorname{twr}_\varphi P$. Let $U := \ker(\theta)$ and $V := \operatorname{Inn}(T)\theta^{-1}$.

Since G acts primitively on $(G : P)$, Lemma 5.1.2 implies that $\mathrm{Inn}(T) \leqslant \mathrm{Im}(\theta)$, and so Q/U is almost simple. Then U is as listed in Table 5.3 of Lemma 5.4.10.

Suppose that $U = S_m^r \times S_{m-1}$. Then $Q/U = S_r$ where $r \geqslant 5$, so $T = A_r$. Since $S_{m-1} \leqslant U \leqslant V$, Lemma 5.4.2(ii) implies that $V = V_1 \times S_{m-1}$ for some $V_1 \trianglelefteq S_m \wr_r S_r$. Then V_1 contains S_m^r, but $V_1/S_m^r \simeq V/U \simeq A_r$ since $\mathrm{Inn}(T) \leqslant \mathrm{Im}(\theta)$, so Proposition 5.4.7 (or Table 5.1) implies that $V_1 = S_m \wr_r A_r$. Now let $R := S_m^{r+1}$. Then $R \cap V = U$ and R is normalised by Q since it is normal in P. However, $R \neq U$, so $T \operatorname{twr}_\theta P$ is not a group of twisted wreath type by Theorem 5.1.1 [4] with M taken to be P, a contradiction.

Suppose that $U = 1 \times S_{m-1}$. Then $Q/U = S_m$ where $m \geqslant 5$ and $r = 1$, so $T = A_m$. Using a similar argument to the one above, we see that $V = V_1 \times S_{m-1}$ for some $V_1 \trianglelefteq S_m$, and so $V_1 \simeq V/U \simeq A_m$. Let $R := 1 \times S_m$. Then $R \cap V = U$ and R is clearly normalised by $Q = S_m \times S_{m-1}$, but $R \neq U$, so we again have a contradiction.

Hence $U = S_m \wr_r S_r \times 1$. Then $Q/U = S_{m-1}$ and $m \geqslant 6$, so $T = A_{m-1}$. As above, we obtain that $V = S_m \wr_r S_r \times A_{m-1}$. Let $\psi : V/U \to A_{m-1}$ be the isomorphism defined by $U(1,t) \mapsto t$ for $t \in A_{m-1}$. Since P is maximal in $A_{m-1} \operatorname{twr}_\theta P$ by Proposition 2.2.1, Baddeley [4, Lemma 3.4] implies that $A_{m-1} \operatorname{twr}_\theta P$ is permutation isomorphic to $A_{m-1} \operatorname{twr}_\eta P$ where $\eta : Q \to \mathrm{Aut}(A_{m-1})$ is defined by $(s_1, s_2) \mapsto (U(1,t)\psi \mapsto U(s_1,s_2)^{-1}(1,t)(s_1,s_2)\psi)$ for all $(s_1, s_2) \in Q$ and $U(1,t) \in V/U$. In other words, for any $(s_1, s_2) \in Q$, the automorphism $(s_1, s_2)\eta$ maps t to $s_2^{-1} t s_2$ for all $t \in A_{m-1}$, and so $(s_1, s_2)\eta = \varphi_{s_2}$. Thus $\eta = \varphi$, and the proof is complete. □

At last, we are in a position to prove Theorem 5.0.3.

Proof of Theorem 5.0.3. By Proposition 5.5.1, we may assume that $G = T \operatorname{twr}_\varphi P$ where $T = A_{m-1}$, $P = S_m \wr_r S_r$, and φ is as defined in Proposition 5.5.1. In particular, $m \geqslant 6$. Let Ω be the set of left cosets of P in G, and let $\Gamma := [m] \times [r]$.

First we bound the distinguishing number of P on Γ. Let $X_i := \{(i,j) : j \in [r]\}$ for $i \in [m-1]$, and let $Y_j := \{(m,j)\}$ for $j \in [r]$. Then $\mathscr{P} := \{X_1, \ldots, X_{m-1}, Y_1, \ldots, Y_r\}$ is a partition of Γ. Suppose that $(s_1, \ldots, s_r)\pi \in P$ fixes the parts of $\mathscr{P}$ setwise. Then $(m,j) = (m,j)(s_1, \ldots, s_r)\pi = (ms_j, j\pi)$ for all $j \in [r]$, so π is the identity. Moreover, if $(i,j) \in [m] \times [r]$ and $i \neq m$, then $(is_j, j) = (i,j)(s_1, \ldots, s_r) \in X_i$, so $is_j = i$. It follows that $\mathscr{P} \in D_\Gamma(P)$, and so $d_\Gamma(P) \leqslant r + m - 1$.

Since $d_\Gamma(P) \leqslant r+m-1$, the desired upper bound on $b_\Omega(G)$ follows from Lemma 5.2.5. In particular, if $r \leqslant (m-2)!$, then $r + m - 1 \leqslant (m-1)!/2$, so $b_\Omega(G) \leqslant 4$.

On the other hand, Lemma 2.3.2 implies that $b_\Omega(G) \geqslant \log|G| / \log|T|^k$ since $|T|^k$ is

the degree of G. The group G has size $|B||P| = |T|^k|P|$ and $r! \geqslant (r/e)^r$, so

$$b_\Omega(G)-1 \geqslant \frac{\log|P|}{k\log|T|} = \frac{\log m!^r r!}{mr\log|T|} \geqslant \frac{r\log m!}{mr\log m!} + \frac{\log r!}{mr\log|T|} \geqslant \frac{1}{m} + \frac{\log r - 1}{m\log|T|} \geqslant \frac{\log r}{m\log|T|}.$$

Thus we have the desired lower bound on $b_\Omega(G)$. In particular, $b_\Omega(G) \to \infty$ when $r \to \infty$ with m fixed. □

To finish this section, we briefly consider the base sizes of another class of groups of twisted wreath type with imprimitive top group.

The following definition was made by Dolfi in [24]. Let G be a permutation group on Ω. Let Γ be a block of G containing at least two elements, and choose a partition of Γ into G-blocks that are maximal among the G-blocks contained in Γ. Then the setwise stabiliser G_Γ of Γ in G acts primitively on Γ^*, where Γ^* is the set consisting of the parts of the chosen partition. Let $(G_\Gamma)^{\Gamma^*}$ denote the induced permutation group on Γ^*. We say that (H, Δ) is a *primitive constituent* of G if H is a permutation group on Δ that is permutation isomorphic to $(G_\Gamma)^{\Gamma^*}$ on Γ^* for some Γ and Γ^*. We say that G is a *proper* permutation group if no primitive constituent (H, Δ) of G contains $\mathrm{Alt}(\Delta)$ when $\Delta \geqslant 5$.

Now we prove a more general version of Theorem 5.0.4 which includes twisted wreath products that do not necessarily act primitively.

Proposition 5.5.3. *Let T be a non-abelian simple group, let P be a proper imprimitive subgroup of S_k, let $Q := P_1$, and let $\varphi : Q \to \mathrm{Aut}(T)$ be a homomorphism. If $T \neq A_5$ then $T\,\mathrm{twr}_\varphi P$ has base size 2, and if $T = A_5$ then $T\,\mathrm{twr}_\varphi P$ has base size at most 3.*

Proof. Dolfi [24, Corollary 6] implies that $d_{[k]}(P) \leqslant 5$. Certainly $h(T) \geqslant 4$ since automorphisms preserve order and 3 distinct primes divide the order of T by Burnside's p^aq^b Theorem [42, Theorem 31.4]. In addition, $h(T) = 4$ only when $T = A_5$ by [71, Theorem 2.3]. Thus $T\,\mathrm{twr}_\varphi P$ has base size 2 when $T \neq A_5$ by Lemma 5.2.3, and base size at most 3 when $T = A_5$ by Lemma 5.2.6. □

In the future, we hope that a closer analysis of those imprimitive permutation groups whose primitive constituents include S_n and A_n for some $n \geqslant 5$ will enable us to determine the base sizes of all groups of twisted wreath type with imprimitive top group.

Appendix A

Source code of GAP functions

In this appendix, we provide some source code for GAP functions that were used in the diagonal and twisted wreath cases. In Appendix A.1, we define some functions that determine the base sizes of groups of diagonal type in the somewhat exceptional case when $k = 2$. In particular, these functions allow us to confirm the claims made about the base sizes of certain diagonal groups at the end of Section 4.2. In Appendix A.2, we provide the source code to justify the claims made in the proof of Proposition 5.3.4.

A.1 The diagonal case

For this section, let T be a non-abelian simple group. Recall the definitions concerning groups of diagonal type made in Section 4.1, and in particular the definition of the somewhat exceptional group $W(2, T)$. We wish to have some methods in GAP [30] for determining the base size of this group. Since Theorem 4.0.2 implies that $W(2, T)$ has base size 3 or 4, it suffices to determine whether a base of size 3 is possible. To do this, we define two GAP functions. The first function, called ProveBase3(T), is best used for finding a base of size 3, while the second function, called ProveNotBase3(T), is best used to prove that a base of size 3 is impossible.

Recall that elements of $\Omega(2, T)$ have the form $D(\varphi_x, 1)$ where $x \in T$ and $\varphi_x : T \to T$ is conjugation by x. By transitivity and Lemma 2.3.1, it suffices to consider subsets of $\Omega(2, T)$ that contain D. Moreover, if G is any subgroup of $W(2, T)$ containing $\mathrm{Inn}(T)^2$, then Lemma 4.2.1 implies that for any distinct non-trivial elements x and y of T, the

intersection of the pointwise stabilisers of D, $D(\varphi_x, 1)$ and $D(\varphi_y, 1)$ in G is

$$G_{x,y} := \{(\alpha, \alpha) \in G : x\alpha = x, y\alpha = y\} \cup \{(\alpha, \alpha)(12) \in G : x\alpha = x^{-1}, y\alpha = y^{-1}\}.$$

Thus $\{D, D(\varphi_x, 1), D(\varphi_y, 1)\}$ is a base of size 3 for G if and only if $G_{x,y}$ is trivial. In particular, we see that $\{D, D(\varphi_x, 1), D(\varphi_y, 1)\}$ is not a base for $W(2, T)$ if and only if there exists $\alpha \in \mathrm{Aut}(T)$ for which either $x\alpha = x^{-1}$ and $y\alpha = y^{-1}$, or $\alpha \neq 1$, $x\alpha = x$ and $y\alpha = y$. This observation, referred to hereafter as $(*)$, will be crucial to the design of both GAP functions.

First we define the function ProveBase3(T), whose input is T and output is either the pair (x, y), in which case $\{D, D(\varphi_x, 1), D(\varphi_y, 1)\}$ is a base for $W(2, T)$, or a statement confirming that $W(2, T)$ has base size 4. For every ordered pair (x, y) of distinct non-trivial elements x and y of T, the function is designed to either reject (x, y) if it finds an automorphism of T satisfying $(*)$, or return the pair (x, y) if no such automorphism is found. If an automorphism satisfying $(*)$ is found for every such pair, then the function returns a statement that $W(2, T)$ has base size 4.

```
ProveBase3 := function( T )

local Aut, U, x, y, a ;
Aut := AutomorphismGroup(T);

for x in T do
  if x = Identity( T ) then
    continue;
  fi;
  for y in T do
    if y = Identity( T ) or x = y then
      continue;
    fi;
    U:=0;
    for a in Aut do
      if x^a=Inverse(x) and y^a=Inverse(y) then
        U:=1;
        break;
      fi;
      if a = Identity( Aut ) then
        continue;
      fi;
      if x^a=x and y^a=y then
        U:=1;
        break;
      fi;
```

```
    od;
    if U=0 then
      Print( "W(2,T) has a base of size 3 defined by: " , "\n" );
      Print( (x,y) , "\n" ) ;
      return ;
    fi;
  od;
od;
Print( "W(2,T) has base size 4" , "\n" );
return ;
end;;
```

Now we define the function ProveNotBase3(T), whose input is T and output is either a statement that $W(2,T)$ has base size 4, or a statement that $W(2,T)$ has a certain number of bases of size 3. Note that if $W(2,T)_{x,y}$ is non-trivial for some non-trivial distinct elements x and y of T, then $W(2,T)_{x,y}$ contains an element of prime order. Since an element $(\alpha,\alpha)(12)$ of $W(2,T)$ has prime order if and only if α is trivial or an involution, it follows that $(*)$ is equivalent to the existence of $\alpha \in \mathrm{Aut}(T)$ where either $\alpha^2 = 1$ and $x\alpha = x^{-1}$ and $y\alpha = y^{-1}$, or α has prime order and $x\alpha = x$ and $y\alpha = y$. Using this fact, the function ProveNotBase3(T) computes the set NotBase of unordered pairs $\{x,y\}$ where x and y are non-trivial distinct elements in T for which $\{D, D(\varphi_x,1), D(\varphi_y,1)\}$ is not a base for $W(2,T)$. If the size of NotBase equals $\binom{|T|-1}{2}$, which is the number of unordered pairs of non-trivial distinct elements in T, then the function returns a statement that $W(2,T)$ has base size 4, and if not, then the function returns a statement that $W(2,T)$ has $\binom{|T|-1}{2} - |\mathrm{NotBase}|$ bases of size 3.

```
ProveNotBase3:= function( T )

local Aut, L, U, V, a, x, NotBase ;
Aut := AutomorphismGroup(T);
L:=[];

for a in Aut do
  U:=[];
  V:=[];
  if Order( a ) = 1 then
    for x in T do
      if x = Identity( T ) then
        continue;
      fi;
      if x^a = Inverse( x ) then
        Add(U,x);
```

```
      fi;
    od;
  elif IsPrimeInt( Order( a ) ) then
    if Order( a ) = 2 then
      for x in T do
        if x = Identity( T ) then
          continue;
        fi;
        if x^a = Inverse( x ) then
          Add(U,x);
        fi;
        if x^a = x then
          Add(V,x);
        fi;
      od;
    else
      for x in T do
        if x = Identity( T ) then
          continue;
        fi;
        if x^a = x then
          Add(V,x);
        fi;
      od;
    fi;
  else
    continue;
  fi;
  if Size(U) >= 2 then
    Append(L,Combinations(U,2));
  fi;
  if Size(V) >= 2 then
    Append(L,Combinations(V,2));
  fi;
od;
NotBase:=AsSSortedList( L );
if Size( NotBase ) = (Size( T ) - 1) * (Size( T ) - 2) / 2 then
  Print( "W(2,T) has base size 4" , "\n" );
else
  Print( "W(2,T) has", " " , (Size( T ) - 1) * (Size( T ) - 2) / 2
        - Size( NotBase ), " " , "bases of size 3",  "\n"  );
fi;
end;;
```

At the end of Section 4.2, we claimed that if $m = 5$ or $m = 6$, then $b(\mathrm{Inn}(A_m)^2 \rtimes S_2) = 3$ while $b(W(2, A_m)) = 4$. Applying the function ProveNotBase3 to A_m for $m = 5$ and

$m = 6$, we determine that $W(2, A_m)$ has base size 4, as desired. Moreover, if we modify the function ProveBase3 to only consider automorphisms in the inner automorphism group, then we determine that $\mathrm{Inn}(A_m)^2 \rtimes S_2$ does indeed have a base of size 3. This is done by replacing the loop for elements in Aut with the following code.

```
for a in Aut do
  if IsInnerAutomorphism( a ) then
    if x^a=Inverse(x) and y^a=Inverse(y) then
      U:=1;
      break;
    fi;
    if a = Identity( Aut ) then
      continue;
    fi;
    if x^a=x and y^a=y then
      U:=1;
      break;
    fi;
  else
    continue;
  fi;
od;
```

Note that the claim $b(\mathrm{Inn}(A_m)^2 \rtimes S_2) = 3$ can be proved without using GAP, as can the claim $b(W(2, A_5)) = 4$, but we do not provide these proofs here.

A.2 The twisted wreath case

In order to prove Proposition 5.3.4, which is a more general form of Theorem 5.0.1, we had to determine which non-abelian simple groups and which primitive permutation groups P of degree k for $2 \leqslant k \leqslant 32$ satisfy the equation $|T|^k \leqslant \sum_{\pi \in R(P)} |\pi^P||T|^{r_\pi}$ where $R(P)$ is a set of representatives for the conjugacy classes of elements of prime order in P and r_π is the number of cycles in the full cycle decomposition of π in S_k. In particular, we claimed that if T is one of A_5, A_6, $L_2(7)$, $L_2(8)$ or $L_2(11)$, then P must be S_k or A_k where $k \geqslant 10$, and if $|T| = 1092$, then no such P exists. Note that the orders of A_5, A_6, $L_2(7)$, $L_2(8)$ and $L_2(11)$ are 60, 168, 360, 504 and 660 respectively [20]. For each T whose order is one of 60, 168, 360, 504, 660, or 1092, the following GAP [30] commands output the primitive permutation groups of degree between 2 and 32 that satisfy the above equation, as well as the corresponding size for T. In the output, the group P is either S_k for $k \geqslant 10$ or A_k for $k \geqslant 14$, and the size 1092 never appears, as desired.

```
U:=[];; V:=[];;
for k in [2..32] do
  for P in AllPrimitiveGroups(NrMovedPoints,k) do
    for C in ConjugacyClasses(P) do
      if Order(Representative(C)) in Primes then
        Add(U,Size(C));
        Add(V,NrMovedPoints(Representative(C))/Order(Representative(C))
              +k-NrMovedPoints(Representative(C)));
      fi;
    od;
    for T in [60,168,360,504,660,1092] do
      if T^k-Sum([1..Length(U)], i -> U[i] * T^V[i]) <= 0 then
        Print([k,P,T],"\n");
      fi;
    od;
    U:=[];
    V:=[];
  od;
od;
```

Part II

The affine case

Chapter 6

The base size 2 problem for groups of affine type

As we learned in the Introduction, the base size 2 problem for groups of affine type is more of a representation theory problem than a permutation group problem. In particular, determining which groups of affine type possess a base of size 2 amounts to determining which groups G and which faithful irreducible $\mathbb{F}_pG$-modules admit regular orbits for all primes p. One way to approach this problem is to first bound the dimensions of faithful irreducible $\mathbb{F}_pG$-modules admitting no regular orbits of G, and then compare these bounds with known dimensions to rule out most candidates. The dimensions of any remaining modules are then hopefully small enough to be dealt with using computers or other methods. Fortunately, bounds of this nature can be constructed quite naturally for the class of almost quasisimple groups (defined in Section 6.3) by using bounds on the minimal number of conjugate generators of almost simple groups. Since the symmetric and alternating groups are almost simple and therefore almost quasisimple, this is the approach we will adopt in order to determine the regular orbits of these groups.

This chapter is organised as follows. In Section 6.1 we define the groups of affine type, and then in Section 6.2 we see how the base size 2 problem for these groups is equivalent to the regular orbit problem. Lastly, in Section 6.3 we determine some bounds on the dimensions of faithful irreducible representations of almost quasisimple groups admitting no regular orbits.

Note that all FG-modules are assumed to have finite dimension, where FG denotes the group algebra of a group G over a field F (see Section 7.1).

6.1 Groups of affine type

The following definitions for groups of affine type may be found in [49]. Let V be a vector space over $\mathbb{F}_p$ of dimension k where p is a prime. Since V is an additive group and the general linear group $\mathrm{GL}(V)$ acts naturally on the group V, we may define the *general affine group*, denoted by $\mathrm{Aff}(V)$, to be $V \rtimes \mathrm{GL}(V)$. Since V acts by translations on the set V and $\mathrm{GL}(V)$ acts naturally on the set V, the group $\mathrm{Aff}(V)$ also acts on the set V. Moreover, this action is faithful and transitive. Note that affine groups can be defined for arbitrary vector spaces of finite dimension, but this more general definition will not be needed.

We say that a group G has *affine type* if there exists a prime p and an $\mathbb{F}_p$-vector space V of dimension k for which $V \leqslant G \leqslant \mathrm{Aff}(V)$ and G acts primitively on V. Any such G has socle C_p^k and degree p^k. Note that the socle of G is abelian and acts regularly on V.

Let G be a subgroup of $\mathrm{Aff}(V)$ containing V. Then the stabiliser in $\mathrm{Aff}(V)$ of the point 0 is $\mathrm{GL}(V)$. Hence the stabiliser G_0 of the point 0 in G is $G \cap \mathrm{GL}(V)$, and V is naturally a faithful $\mathbb{F}_pG_0$-module. It turns out that the primitivity of G depends solely on the irreducibility of V as an $\mathbb{F}_pG_0$-module, as we now see.

Proposition 6.1.1. *Let p be a prime. If $V \leqslant G \leqslant \mathrm{Aff}(V)$, then G is a group of affine type if and only if V is an irreducible $\mathbb{F}_pG_0$-module.*

Proof. Note that the group V acts transitively on the set V, so G acts transitively on V. By Proposition 2.2.1, it therefore suffices to show that G_0 is a maximal subgroup of G if and only if V is an irreducible $\mathbb{F}_pG_0$-module. To make the proof easier to follow, we write the elements of G in the form (v, α) where $v \in V$ and $\alpha \in \mathrm{GL}(V)$.

Suppose that G_0 is a maximal subgroup of G. Let W be an $\mathbb{F}_pG_0$-submodule of V, and let $H := \{g \in G : Wg = W\}$. Then H is a subgroup of G containing G_0, so H is G or G_0. If $H = G$ and $v \in V$, then $v = 0(v, 1)$, so $v \in W$ since $0 \in W$ and $(v, 1) \in V \leqslant G = H$. Thus $V = W$, as desired. If $H = G_0$ and $w \in W$, then $x(w, 1) = x + w \in W$ for all $x \in W$, so $(w, 1) \in H = G_0$, forcing $w = 0$. Thus $W = \{0\}$.

Conversely, suppose that V is an irreducible $\mathbb{F}_pG_0$-module. Let $G_0 \leqslant H \leqslant G$, and let $W := \{w \in V : (w, 1) \in H\}$. Since every non-zero element of $\mathbb{F}_p$ is a sum of 1, it follows that W is a subspace of V. Moreover, if $w \in W$ and $(v, \alpha) \in G_0$, then $v = 0$, so $w(v, \alpha) = w\alpha$. But $(w\alpha, 1) = (0, \alpha)^{-1}(w, 1)(0, \alpha) \in H$, so $w\alpha \in W$. Thus W is an $\mathbb{F}_pG_0$-submodule of V and is therefore $\{0\}$ or V. Note that $G = G \cap (V \rtimes \mathrm{GL}(V)) = VG_0$ by Lemma 2.1.1. Since $H = H \cap G = H \cap (VG_0) = (H \cap V)G_0$ by Lemma 2.1.1, it follows that H is G_0 or G. □

Note that the proof above shows that if G is a subgroup of $\mathrm{Aff}(V)$ containing V, then $G = VG_0$. Thus every group of affine type is a semidirect product of its socle by its 0-stabiliser.

A primitive permutation group G with base size 1 must be of affine type, for such a group has an abelian socle by Lemma 2.3.3, and groups of affine type are the only primitive permutation groups with abelian socles (see Section 2.4). In addition, Lemma 2.3.3 implies that a group G of affine type with socle $V = C_p^k$ has base size 1 if and only if $G = V$ and $k = 1$. Thus the groups of affine type with base size 1 are classified, so we will only be interested in groups of affine type with base size at least 2. These are precisely the groups with non-trivial 0-stabilisers.

6.2 The regular orbit problem

Let G be a finite group and F a field. Let V be a faithful FG-module. Then G acts on V, so it is reasonable to consider whether G has a regular orbit on V (i.e. a vector $v \in V$ for which $vg \neq v$ for all $1 \neq g \in G$). We refer to this problem as the *regular orbit problem*. Note that the requirement that V be faithful is necessary, or else some non-trivial element of G will fix every element of V, making the existence of a regular orbit impossible.

To see the connection between the base size 2 problem for groups of affine type and the regular orbit problem, consider the following.

Let G be a group of affine type. Then there exists a prime p and a finite-dimensional $\mathbb{F}_p$-vector space V for which $V \leqslant G \leqslant \mathrm{Aff}(V)$ and $G = V \rtimes G_0$. Moreover, Proposition 6.1.1 implies that V is a faithful irreducible $\mathbb{F}_pG_0$-module. Then the transitivity of G and Lemma 2.3.1 imply that G has base size 2 if and only if G_0 is non-trivial and has a regular orbit on V.

Conversely, let H be a finite non-trivial group and V a faithful irreducible $\mathbb{F}_pH$-module for any prime p. Then V has finite dimension (see Lemma 7.2.2). Since we may view H as a subgroup of $\mathrm{GL}(V)$, it follows that $V \rtimes H$ is a subgroup of $\mathrm{Aff}(V)$ containing V for which $(V \rtimes H)_0 = H$ (by Lemma 2.1.1), so $V \rtimes H$ is a group of affine type by Proposition 6.1.1. Again, H has a regular orbit on V if and only if the group $V \rtimes H$ has base size 2.

Thus the base size 2 problem for groups of affine type is equivalent to the restriction of the regular orbit problem to irreducible representations of non-trivial groups over fields of prime order. In fact, it turns out that it is quite reasonable to approach the general regular orbit problem by starting with the field $\mathbb{F}_p$. Let G be a group, F a field and V a faithful FG-module. If F is infinite, then G always has a regular orbit on V (see Lemma

6.3.1), so we assume that F is finite with characteristic p. Then V can be regarded as a faithful $\mathbb{F}_pG$-module, and G has a regular orbit on V as an FG-module if and only if G has a regular orbit on V as an $\mathbb{F}_pG$-module. Note, however, that when V is an irreducible FG-module, V need not be an irreducible $\mathbb{F}_pG$-module, so it is not sufficient to only consider irreducible $\mathbb{F}_pG$-modules for the general regular orbit problem.

In any case, in order to solve the base size 2 problem for groups of affine type, we need to determine which groups G and which faithful irreducible $\mathbb{F}_pG$-modules V, where p is any prime, are such that G has a regular orbit on V. We focus on the case when the group G is a symmetric group or an alternating group.

6.3 Bounds for dimensions of irreducible representations

In this section, we determine some bounds for the dimensions of faithful irreducible representations of almost quasisimple groups that admit no regular orbits. These are obtained using the standard technique of counting fixed points, as in Lemma 3.2.1. Note that the material in this section was obtained in collaboration with O'Brien and Saxl [26].

We begin with some basic results that apply to all groups. Let G be a group, and let F be a field. For an FG-module V, we define $C_V(g) := \{v \in V : vg = v\}$ for all $g \in G$. Then $C_V(g)$ is a subspace of V. Note that $C_V(g)$ is precisely the set of fixed points of g in V, but we have assigned new notation to this set in order to emphasise that it is a vector space. Note also that $C_V(g)$ is a proper subspace of V when $1 \neq g \in G$ and V is faithful.

The following is a simple but crucial result.

Lemma 6.3.1. *Let G be a group and F a field. Let V be a faithful FG-module. If G has no regular orbits on V, then*

$$V = \bigcup_{g \in G \setminus \{1\}} C_V(g).$$

In particular, if F is infinite, then G has a regular orbit on V.

Proof. If there exists $v \in V$ that is not in $C_V(g)$ for any non-trivial $g \in G$, then clearly v is a regular orbit of G. Now suppose that F is infinite. Then V cannot be a union of finitely many proper subspaces, so G has a regular orbit on V. □

Thus the regular orbit problem is trivial over infinite fields. Moreover, Lemma 6.3.1 gives us a bound on the size of V that is easily computed using Magma [8]. To see this, we need the following useful observation about fixed points of central elements.

Lemma 6.3.2. *Let G be a group and F a field. Let V be a faithful irreducible FG-module. If $1 \neq g \in Z(G)$, then $C_V(g) = 0$.*

Proof. This follows from the fact that $C_V(g)$ is a proper FG-submodule of V. □

Now we provide the bound mentioned above. Note that for a group G, a field F and an FG-module V, we denote the stabiliser of a vector $v \in V$ in G by $C_G(v)$.

Lemma 6.3.3. *Let G be a group and F a finite field. Let V be a faithful irreducible FG-module. If G has no regular orbits on V, then*

$$|V| \leqslant \sum_{g \in X} |g^G||C_V(g)|,$$

where X is a set of representatives for the conjugacy classes of non-central elements of prime order in G.

Proof. Let $0 \neq v \in V$. Then $v \in C_V(g)$ for some $g \in G \setminus Z(G)$ by Lemmas 6.3.1 and 6.3.2, and this implies that $C_G(v)$ is a non-trivial group. Then there exists $h \in C_G(v)$ of prime order, and so $v \in C_V(h)$. In particular, $h \notin Z(G)$ by Lemma 6.3.2. Therefore, letting Y denote the set of non-central elements of prime order in G, it follows that $V = \bigcup_{g \in Y} C_V(g)$. Since the map $\varphi : C_V(g) \to C_V(h^{-1}gh)$ defined by $v \mapsto vh$ for all $v \in V$ is a bijection for all $g, h \in G$, the result follows. □

Next we focus on almost quasisimple groups. A group G is *quasisimple* if $G = G'$ and $G/Z(G)$ is simple. Note that $G/Z(G)$ must be non-abelian, or else G is soluble, in which case the condition $G = G'$ forces $G = 1$. More generally, as defined in [36], a group G is *almost quasisimple* if $G/Z(G)$ is almost simple. For example, the alternating group is quasisimple, and the symmetric group is almost quasisimple by Proposition 2.2.2.

We construct bounds for the dimensions of faithful irreducible representations of almost quasisimple groups using the following quantity. Let G be an almost quasisimple group where $G/Z(G)$ has socle $N/Z(G)$, and let $g \in G \setminus Z(G)$. Then $\langle N/Z(G), Z(G)g \rangle$ is generated by the $N/Z(G)$-conjugates of $Z(G)g$, so we define $r(g)$ to be the minimal number of $N/Z(G)$-conjugates of $Z(G)g$ generating $\langle N/Z(G), Z(G)g \rangle$.

In order to construct the aforementioned bounds, we need the definition of a structure closely related to $C_V(g)$. Let G be a group and F a field. If V is an FG-module and $X \subseteq G$, then define $[V, X] := \text{span}\{v - vg : v \in V, g \in X\}$; if $X = \{g\}$, then we simply write $[V, g]$. Now we see how $C_V(g)$ and $[V, g]$ relate.

Lemma 6.3.4. *Let G be a group and F a field. Let V be an FG-module. Then $\dim_F(V) = \dim_F(C_V(g)) + \dim_F([V, g])$ for all $g \in G$.*

Proof. Fix $g \in G$, and define $\varphi : V \to [V, g]$ by $v \mapsto v - vg$ for all $v \in V$. Then φ is a surjective linear transformation with kernel $C_V(g)$. □

The following result appears in various incarnations in the literature, and the version given here, which is essentially [36, Lemma 3.2], is the one most suited to our purposes; see also [48, Lemma 2] and the proof of [37, Theorem 6].

Lemma 6.3.5 ([36])**.** *Let G be an almost quasisimple group and F a field. Let V be a faithful irreducible FG-module. Then*

$$\dim_F(C_V(g)) \leqslant \dim_F(V)\left(1 - \frac{1}{r(g)}\right)$$

for all $g \in G \setminus Z(G)$.

Proof. Let $\overline{g}$ denote the coset $Z(G)g$ for $g \in G$, and let $\overline{N} := N/Z(G)$ where $N/Z(G)$ is the socle of $G/Z(G)$. Fix $g \in G \setminus Z(G)$. Suppose that $\overline{g}_1, \overline{g}_2, \ldots, \overline{g}_r$ are conjugates of $\overline{g} = \overline{g}_1$ that generate $\langle \overline{N}, \overline{g} \rangle$ where $r = r(g)$ and the representatives $g_2, \ldots, g_r$ are chosen so that they are conjugates of g in G. By this choice, it follows as in the proof of Lemma 6.3.3 that $|C_V(g)| = |C_V(g_i)|$ for all $i \in [r]$. Then Lemma 6.3.4 implies that the vector space $W := \operatorname{span}\{[V, g_i] : 1 \leqslant i \leqslant r\}$ is spanned by $r(g)\dim_F([V, g])$ elements. Note that if $g, h \in G$, then $v - vgh = (v - vg) + (vg - vgh) \in \operatorname{span}\{[V, g], [V, h]\}$. It follows that $W = [V, \langle g_1, \ldots, g_r \rangle]$, and so $r(g)\dim_F([V, g]) \geqslant \dim_F([V, \langle g_1, \ldots, g_r \rangle])$. Observe that $N \leqslant \langle g_1, \ldots, g_r \rangle Z(G)$, which then implies that $N' \leqslant \langle g_1, \ldots, g_r \rangle$. Thus $[V, N']$ is a subspace of $[V, \langle g_1, \ldots, g_r \rangle]$. But N' is a non-trivial normal subgroup of G and V is faithful, so $[V, N']$ is a non-zero FG-submodule of V. Thus $[V, N'] = [V, \langle g_1, \ldots, g_r \rangle] = V$, so $r(g)\dim_F([V, g]) \geqslant \dim_F(V)$. Then $\dim_F(V) - \dim_F(C_V(h)) \geqslant \dim_F(V)/r(g)$ by Lemma 6.3.4, as desired. □

The next result is a natural generalisation of part of the proof of [37, Theorem 6] and is largely a consequence of Lemma 6.3.5.

Lemma 6.3.6. *Let G be an almost quasisimple group, and let V be a faithful irreducible $\mathbb{F}_q G$-module. If G has no regular orbits on V, then*

$$\dim_{\mathbb{F}_q}(V) \leqslant r(G)\log_q |G|,$$

where $r(G) := \max\{r(g) : g \in G \setminus Z(G)\}$.

Proof. Lemma 6.3.1 and 6.3.2 imply that

$$V = \bigcup_{g \in G \setminus Z(G)} C_V(g).$$

Moreover, Lemma 6.3.5 implies that

$$\dim_{\mathbb{F}_q}(C_V(g)) \leqslant \dim_{\mathbb{F}_q}(V)\left(1-\frac{1}{r(G)}\right)$$

for all $g \in G \setminus Z(G)$. Putting these two observations together, we obtain that

$$q^{\dim_{\mathbb{F}_q}(V)} \leqslant |G| q^{\dim_{\mathbb{F}_q}(V)\left(1-\frac{1}{r(G)}\right)}.$$

Then $q^{\dim_{\mathbb{F}_q}(V)/r(G)} \leqslant |G|$, and so $\dim_{\mathbb{F}_q}(V) \leqslant r(G)\log_q|G|$. □

Now we give some more specific bounds for the case when the socle of $G/Z(G)$ is A_n.

Lemma 6.3.7. *Let G be an almost quasisimple group, and suppose that the socle of $G/Z(G)$ is A_n where $n \geqslant 5$. Let V be a faithful irreducible $\mathbb{F}_qG$-module. If G has no regular orbits on V, then*

$$\dim_{\mathbb{F}_q}(V) \leqslant (n-1)\log_q|G|, \tag{1}$$

and if $n \geqslant 7$, then

$$\dim_{\mathbb{F}_q}(V) \leqslant \max\{(n-1)\log_q(n(n-1)|Z(G)|), \tfrac{n}{2}\log_q(2n!|Z(G)|)\}. \tag{2}$$

In particular,

$$\dim_{\mathbb{F}_q}(V) \leqslant \tfrac{n}{2}\log_q(2n!|Z(G)|) \tag{3}$$

when $|Z(G)| \leqslant n$ and $n \geqslant 7$.

Proof. If $g \in G \setminus Z(G)$, then $r(g) \leqslant n-1$ for $n \geqslant 5$ by Guralnick and Saxl [35, Lemma 6.1], so equation (1) follows from Lemma 6.3.6.

Suppose that $n \geqslant 7$. Then $G/Z(G)$ is A_n or S_n by Proposition 2.2.2. Let $g \in G\setminus Z(G)$, and write $\overline{g}$ for the coset $Z(G)g$. If $\overline{g}$ is not a transposition, then by [35, Lemma 6.1], we have that $r(g) \leqslant n/2$. Let S_1 be the set of $g \in G$ for which $\overline{g}$ is a transposition, and let S_2 be the set of $g \in G \setminus Z(G)$ for which $\overline{g}$ is not a transposition. It then follows from Lemmas 6.3.1, 6.3.2 and 6.3.5 that

$$|V| \leqslant \sum_{g\in S_1}|C_V(g)| + \sum_{g\in S_2}|C_V(g)| \leqslant |S_1|q^{\dim_{\mathbb{F}_q}(V)\left(1-\frac{1}{n-1}\right)} + |S_2|q^{\dim_{\mathbb{F}_q}(V)\left(1-\frac{2}{n}\right)},$$

and since $q^{\dim_{\mathbb{F}_q}(V)} = |V|$, we obtain that

$$1 \leqslant 2\max\{|S_1|q^{-\frac{1}{n-1}\dim_{\mathbb{F}_q}(V)}, |S_2|q^{-\frac{2}{n}\dim_{\mathbb{F}_q}(V)}\}.$$

If $1 \leqslant 2|S_1|q^{-\dim_{\mathbb{F}_q}(V)/(n-1)}$, then $\dim_{\mathbb{F}_q}(V) \leqslant (n-1)\log_q(2|S_1|)$. Similarly, if $1 \leqslant 2|S_2|q^{-2\dim_{\mathbb{F}_q}(V)/n}$, then $\dim_{\mathbb{F}_q}(V) \leqslant (n/2)\log_q(2|S_2|)$. Thus

$$\dim_{\mathbb{F}_q}(V) \leqslant \max\{(n-1)\log_q(2|S_1|), \tfrac{n}{2}\log_q(2|S_2|)\}.$$

Since $2|S_1| = n(n-1)|Z(G)|$ and $|S_2| \leqslant |G| \leqslant n!|Z(G)|$, we have proved equation (2).

Suppose in addition that $|Z(G)| \leqslant n$. First we claim that $n^5 \leqslant 2n!$ for $n \geqslant 8$. Note that $(n+1)^4 \leqslant 5n^4 \leqslant n^5$, so if $n^5 \leqslant 2n!$, then $(n+1)^5 \leqslant n^5(n+1) \leqslant 2(n+1)!$. Thus the claim holds by induction, and so $(n(n-1)|Z(G)|)^2 \leqslant 2n!|Z(G)|$ for $n \geqslant 8$. Then

$$(n-1)\log_q(n(n-1)|Z(G)|) \leqslant \tfrac{n}{2}\log_q(2n!|Z(G)|),$$

and so $\dim_{\mathbb{F}_q}(V) \leqslant (n/2)\log_q(2n!|Z(G)|)$ when $n \geqslant 8$ by equation (2). Now suppose that $n = 7$. It suffices to show that $(42|Z(G)|)^{12/7} \leqslant 2 \cdot 7!|Z(G)|$ when $|Z(G)| \leqslant 7$, and this is true since $42^{12/7}|Z(G)|^{12/7-1} \leqslant 42^{12/7}7^{12/7-1} \leqslant 2 \cdot 7!$. □

Chapter 7

Representation theory

In this chapter, we collect some notation, definitions and results concerning the representation theory of finite groups that will be used to determine the regular orbits of the symmetric and alternating groups. These definitions and results are known and can be found in one of [6, 21, 39], though most proofs will be provided.

Given the nature of the regular orbit problem, we focus on the representation theory of groups over finite fields, though we work over arbitrary fields when it is natural to do so. Where necessary, we assume results that are specific to ordinary representation theory, and we also assume basic definitions and facts concerning Galois extensions, rings, representations, and modules over group algebras.

This chapter is organised as follows. In Section 7.1 we outline some standard notation, definitions and facts concerning tensor products, modules over group algebras and characters. In Section 7.2 we explore extensions of scalars and Galois conjugates, and in Section 7.3 we see how to use extensions of scalars to write representations over subfields. In Section 7.4 we define absolutely irreducible representations and splitting fields and prove some important properties of these concepts, and in Section 7.5 we look into the representation theory of index 2 subgroups. Lastly, in Section 7.6 we define Brauer characters and outline their most important properties.

7.1 Preliminaries

In this section, we briefly introduce some of the basic tools from algebra that will be needed throughout this chapter, and we then consider the character of an arbitrary representation. Further details may be found in [21].

For a ring R, every R-module is a right R-module unless otherwise stated, and we denote the multiplicative group of units of R by R^* and the ring of $n \times n$ matrices with entries in R by $M_n(R)$. For a field F, we denote the characteristic of F by $\mathrm{char}(F)$ and the algebraic closure of F by $\overline{F}$. An *F-algebra* A is a ring and an F-vector space for which $\lambda(ab) = (\lambda a)b = a(\lambda b)$ for all $\lambda \in F$ and $a, b \in A$.

We begin with some important properties of tensor products. Let R and S be rings with unity. Let V be a right R-module, and let W be a left R-module. Then the tensor product of V and W over R is denoted by $V \otimes_R W$. It is an abelian group with a universal property stating that if A is any abelian group and $\varphi : V \times W \to A$ is any R-balanced map, then there exists a unique group homomorphism $\varphi^* : V \otimes_R W \to A$ for which $(v \otimes w)\varphi^* = (v, w)\varphi$ for all $v \in V$ and $w \in W$.

We say that W is an (R, S)-*bimodule* if W is both a left R-module and a right S-module where $(rw)s = r(ws)$ for all $r \in R$, $s \in S$ and $w \in W$. The tensor product $V \otimes_R W$ is then a right S-module under the natural action. Furthermore, if F is a field and V has basis $v_1, \ldots, v_n$ and W has basis $w_1, \ldots, w_m$, then $V \otimes_F W$ is an F-vector space with basis $\{v_i \otimes w_j : i \in [n], j \in [m]\}$. Consequently, if $v \otimes w = 0$ for some $v \in V$ and $w \in W$, then $v = 0$ or $w = 0$.

It is easy to build homomorphisms of tensor products using homomorphisms of the modules they are composed of. Let V and V' be right R-modules and W and W' left R-modules. If $\varphi : V \to V'$ is a right R-homomorphism and $\theta : W \to W'$ is a left R-homomorphism, then there is a unique additive homomorphism $\varphi \otimes \theta : V \otimes_R W \to V' \otimes_R W'$ for which $v \otimes w \mapsto (v\varphi) \otimes (w\theta)$. If φ and θ are surjective, then clearly $\varphi \otimes \theta$ is as well, and if W and W' are (R, S)-bimodules and θ is an S-homomorphism, then $\varphi \otimes \theta$ is also an S-homomorphism.

Here are some important laws for tensor products. Firstly, they have an associative law. Let V be a right R-module, W an (R, S)-bimodule and U a left S-module. Then $(V \otimes_R W) \otimes_S U \simeq V \otimes_R (W \otimes_S U)$ via the homomorphism $(v \otimes w) \otimes u \mapsto v \otimes (w \otimes u)$.

Secondly, tensor products have a distributive law. Let V and V' be right R-modules and W and W' left R-modules. Then $(V \oplus V') \otimes_R W \simeq (V \otimes_R W) \oplus (V' \otimes_R W)$ via the homomorphism $(v, v') \otimes w \mapsto (v \otimes w, v' \otimes w)$. If W is an (R, S)-bimodule, then this is an S-isomorphism. Similarly, $V \otimes_R (W \oplus W') \simeq (V \otimes_R W) \oplus (V \otimes_R W')$, and this isomorphism is an S-isomorphism if W and W' are (R, S)-bimodules.

Thirdly, tensor products have an identity law. Let V be a right R-module. Then R is an (R, R)-bimodule, so $V \otimes_R R$ is a right R-module, and $V \otimes_R R \simeq V$ via the R-homomorphism $v \otimes r \mapsto vr$.

Let G be a group and F a field. The *group algebra* of G over F, denoted by FG, is the F-algebra with basis comprised of the elements of G. As in Chapter 6, we assume that every FG-module V has finite dimension. In particular, every FG-module has a composition series, and the Jordan-Hölder Theorem implies that any two composition series are equivalent. Thus every FG-module V has a corresponding set of composition factors, and these are uniquely determined. For an FG-module V and $g \in G$, the F-endomorphism of V defined by $v \mapsto vg$ for all $v \in V$ is denoted simply by g.

Let V and W be FG-modules. The F-vector space of FG-homomorphisms from V to W is denoted by $\mathrm{Hom}_{FG}(V, W)$. It has finite dimension over F. Note that if U is an FG-module, then $\mathrm{Hom}_{FG}(U \oplus V, W) \simeq \mathrm{Hom}_{FG}(U, W) \oplus \mathrm{Hom}_{FG}(V, W)$ and $\mathrm{Hom}_{FG}(U, V \oplus W) \simeq \mathrm{Hom}_{FG}(U, V) \oplus \mathrm{Hom}_{FG}(U, W)$.

Moreover, $\mathrm{End}_{FG}(V) := \mathrm{Hom}_{FG}(V, V)$ is an F-algebra whose multiplication is composition, called the *endomorphism algebra* of V. If V is irreducible and $0 \neq \varphi \in \mathrm{End}_{FG}(V)$, then $\ker(\varphi)$ is a proper FG-submodule of V, and so φ is invertible (this observation is often referred to as Schur's Lemma). Thus $\mathrm{End}_{FG}(V)$ is a division algebra, and if we also assume that F is finite, then $\mathrm{End}_{FG}(V)$ is a field by a well-known theorem of Wedderburn.

As in ordinary representation theory, the *character* of V is the function $\chi : G \to F$ that maps an element $g \in G$ to the trace of the matrix corresponding to the F-endomorphism g of V relative to any basis for V. If V and W are $\mathbb{C}G$-modules with characters χ and ψ respectively, then it is well known that V and W are isomorphic if and only if $\chi = \psi$. Unfortunately, this is not always the case in positive characteristic. However, we can say the following.

Theorem 7.1.1 ([6, 39])**.** *Let G be a group and F a field. Let V and W be irreducible FG-modules with characters χ and ψ respectively. Then $V \simeq W$ if and only if $\chi = \psi$.*

Proof. See [6, Theorem VII.1.11] or [39, Corollary 9.22]. □

As a consequence of Theorem 7.1.1, we write $\mathrm{Irr}_F(G)$ for the complete set of characters of all non-isomorphic irreducible FG-modules. Moreover, if E/F is a field extension and $\chi \in \mathrm{Irr}_E(G)$, then we denote by $F(\chi)$ the subfield of E generated by F and $\{\chi(g) : g \in G\}$.

7.2 Extensions of scalars

Let G be a group and E/F an extension of fields. Suppose that V is an FG-module. Then there is a representation of G in the general linear group $\mathrm{GL}(V)$, and hence in $\mathrm{GL}_n(F)$ where $n = \dim_F V$. Since the image of G also lies in $\mathrm{GL}_n(E)$, there is a representation

of G in $\mathrm{GL}_n(E)$ as well. Thus we would like to have some formalised method of turning V into an EG-module. This is done using the tensor product as follows.

Let V be an FG-module. Then E is an (F, E)-bimodule, so $V \otimes_F E$ is an E-vector space. It becomes an EG-module if we define $(v \otimes \lambda)g := vg \otimes \lambda$ for every $v \in V$, $\lambda \in E$ and $g \in G$. This EG-module is called the *extension of scalars* of V to E.

We make note of some basic properties of extensions of scalars. To begin, observe that $V \otimes 1 := \{v \otimes 1 : v \in V\}$ is an FG-submodule of $V \otimes_F E$ that is isomorphic to V. Moreover, if V has dimension n over F, then $V \simeq F^n$, so $V \otimes_F E \simeq (F \otimes_F E)^n \simeq E^n$ as E-vector spaces. Hence $\dim_F V = \dim_E (V \otimes_F E)$. It follows that if $\{v_1, \ldots, v_n\}$ is an F-basis of V, then $\{v_1 \otimes 1, \ldots, v_n \otimes 1\}$ is an E-basis of $V \otimes_F E$. Then for each $g \in G$, the matrix of the F-endomorphism g of V relative to an F-basis $\{v_1, \ldots, v_n\}$ of V is the same as the matrix of the E-endomorphism g of $V \otimes_F E$ relative to the E-basis $\{v_1 \otimes 1, \ldots, v_n \otimes 1\}$ of $V \otimes_F E$. In particular, V and $V \otimes_F E$ have the same character.

Note that if $V \otimes_F E$ is an irreducible EG-module, then it is certainly the case that V is an irreducible FG-module. However, there exist irreducible $\mathbb{F}_p A_n$-modules V for which $V \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}$ is not irreducible, so the converse is not true in general. We will return to this problem in Section 7.4.

Let W be an FG-module. If $\varphi : V \to W$ is an FG-homomorphism, then $\varphi \otimes 1 : V \otimes_F E \to W \otimes_F E$ is an EG-homomorphism, and $\varphi \otimes 1$ is surjective when φ is surjective. This has several consequences. Firstly, if W is an FG-submodule of V and ι is the corresponding inclusion map, then $\iota \otimes 1 : W \otimes_F E \to V \otimes_F E$ is an EG-homomorphism that must be injective, for if $w_1, \ldots, w_n$ is an F-basis of W, then $w_1 \otimes 1, \ldots, w_n \otimes 1$ is an E-basis of $W \otimes_F E$ as well as an E-linearly independent set in $V \otimes_F E$. Thus we may regard $W \otimes_F E$ as an EG-submodule of $V \otimes_F E$ (this is not true for general R-modules).

Secondly, if $V \simeq W$, then $V \otimes_F E \simeq W \otimes_F E$, for if φ is a witness to the isomorphism of V and W, then since $V \otimes_F E$ and $W \otimes_F E$ have the same E-dimension, it follows that $\varphi \otimes 1$ is an EG-isomorphism. The converse is also true but is a deeper result we will not need; Lemma 7.2.1(v) below provides a version that will suffice.

Thirdly, it can be checked that the distributive law $(V \oplus W) \otimes_F E \simeq (V \otimes_F E) \oplus (W \otimes_F E)$ is an EG-isomorphism, and if K/E is a field extension, then the associative and identity laws can be combined to obtain the group isomorphism $(V \otimes_F E) \otimes_E K \simeq V \otimes_F K$, which is easily checked to be a KG-isomorphism.

Note that if A is an F-algebra, then $A \otimes_F E$ is an E-algebra whose multiplication is defined by $(\sum_i a_i \otimes \lambda_i)(\sum_j b_j \otimes \mu_j) = \sum_{i,j} a_i b_j \otimes \lambda_i \mu_j$ for all $a_i, b_j \in A$ and $\lambda_i, \mu_j \in E$. In particular, $EG \simeq FG \otimes_F E$, so group algebras are preserved under extensions of scalars.

Here is a collection of useful well-known results about extensions of scalars.

Lemma 7.2.1 ([6, 21])**.** *Let G be a group and E/F an extension of fields. Let V and W be FG-modules. Then the following are true.*

(i) The EG-module $V \otimes_F E$ is completely reducible if and only if V is completely reducible. In particular, if V is irreducible then $V \otimes_F E$ is completely reducible.

(ii) As E-vector spaces, $\mathrm{Hom}_{EG}(V \otimes_F E, W \otimes_F E) \simeq \mathrm{Hom}_{FG}(V, W) \otimes_F E$. Moreover, if $V = W$, then this is an isomorphism of E-algebras.

(iii) If V and W have a common composition factor, then $V \otimes_F E$ and $W \otimes_F E$ also have a common composition factor.

(iv) If $V \otimes_F E$ and $W \otimes_F E$ are completely reducible and have a common composition factor, then V and W have a common composition factor.

(v) If V and W are irreducible FG-modules where $V \otimes_F E$ and $W \otimes_F E$ have a common composition factor, then $V \simeq W$.

Proof. (i) This follows from properties of the Jacobson radical. See [6, Theorem VII.1.8].

(ii) Let $\{e_i\}_{i \in I}$ be an F-basis for E. Then $E \simeq \oplus_{i \in I}(e_i F)$ as F-vector spaces, so $V \otimes_F E \simeq \oplus_{i \in I}(V \otimes e_i)$ and $W \otimes_F E \simeq \oplus_{i \in I}(W \otimes e_i)$ as F-vector spaces. Let $\alpha \in \mathrm{Hom}_{EG}(V \otimes_F E, W \otimes_F E)$. Then for every $v \in V$, $(v \otimes 1)\alpha = \sum_{i \in I} v_i \otimes e_i$ for some $v_i \in W$ where only finitely many of the v_i are non-zero. Fix $i \in I$. Define $\alpha_i : V \to W$ by $v \mapsto v_i$ for all $v \in V$. This is a well-defined F-linear map from V to W. Moreover, it is an FG-homomorphism since $(vg \otimes 1)\alpha = (v \otimes 1)\alpha g = \sum_{i \in I} v_i g \otimes e_i$. Also, only finitely many of the α_i are non-zero since V is a finite-dimensional E-vector space. Thus $\alpha = \sum_{i \in I} \alpha_i \otimes e_i \in \oplus_{i \in I}(\mathrm{Hom}_{FG}(V, W) \otimes e_i) = \mathrm{Hom}_{FG}(V, W) \otimes_F E$. This gives rise to an E-linear map from $\mathrm{Hom}_{EG}(V \otimes_F E, W \otimes_F E)$ to $\mathrm{Hom}_{FG}(V, W) \otimes_F E$ that is clearly bijective. If $V = W$, then it can be verified that it is an E-algebra homomorphism.

(iii) To begin, let U be any FG-submodule of V, and let $\varphi : V \to V/U$ be the natural quotient map. Then $\varphi \otimes 1 : V \otimes_F E \to (V/U) \otimes_F E$ is a surjective EG-homomorphism. Clearly $U \otimes_F E$ is contained in the kernel of $\varphi \otimes 1$, and these have the same E-dimension by rank-nullity. Hence $(V \otimes_F E)/(U \otimes_F E) \simeq V/U \otimes_F E$. We conclude that if V has composition factors $V_1, \ldots, V_r$, then the composition factors of $V \otimes_F E$ consist of the composition factors of $V_1 \otimes_F E, \ldots, V_r \otimes_F E$. The result follows.

(iv) Clearly $\mathrm{Hom}_{EG}(V \otimes_F E, W \otimes_F E)$ must be non-zero, and so $\mathrm{Hom}_{FG}(V, W)$ is also non-zero by (ii). Hence V and W have a common composition factor.

(v) Follows from (i) and (iv). □

The following result is well known.

Lemma 7.2.2. *Let G be a group and F a field. If V is an irreducible FG-module, then V is a composition factor of FG. In particular,* $\mathrm{Irr}_F(G)$ *is finite.*

Proof. Let $0 \neq v \in V$. The map $\varphi : FG \to V$ defined by $a \mapsto va$ for all $a \in FG$ is a non-zero FG-homomorphism, and V is irreducible, so $\mathrm{Im}(\varphi) = V$. □

Using Lemma 7.2.2, we obtain the following important consequence of Lemma 7.2.1.

Lemma 7.2.3 ([39])**.** *Let G be a group and E/F an extension of fields. Let V be an irreducible EG-module. Then there exists a unique irreducible FG-module U for which V is an EG-submodule of $U \otimes_F E$. Moreover, if V is faithful, then U is faithful.*

Proof. First we establish existence. We saw in the proof of Lemma 7.2.1(iii) that if $V_1, \ldots, V_r$ are the composition factors of FG, then the composition factors of $FG \otimes_F E$ are precisely the composition factors of $V_1 \otimes_F E, \ldots, V_r \otimes_F E$. Then V is a composition factor of $U \otimes_F E$ for some irreducible FG-module U, for Lemma 7.2.2 implies that V is a composition factor of EG, and $EG \simeq FG \otimes_F E$. Since $U \otimes_F E$ is completely reducible by Lemma 7.2.1(i), we may view V as an EG-submodule of $U \otimes_F E$, as desired.

Now we prove uniqueness. Suppose that V is an EG-submodule of $W \otimes_F E$ for some irreducible FG-module W. Then $W \otimes_F E$ and $U \otimes_F E$ have a common composition factor, so W and U are isomorphic by Lemma 7.2.1(v).

Lastly, suppose that V is faithful, and let $g \in G$ be such that $ug = u$ for all $u \in U$. Then $(u \otimes 1)g = u \otimes 1$ for all $u \in U$, so $vg = v$ for all $v \in V$. Hence $g = 1$ and U is faithful. □

Now we define the concept of a Galois conjugate of a representation. These special representations help elucidate the structure of $V \otimes_F E$ when E/F is a Galois extension. Indeed, the structure of $V \otimes_F E$ is particularly nice when E/F is an extension of finite fields. Note that if V is an EG-module where $[E : F]$ is finite, then V is naturally an FG-module with dimension $[E : F] \dim_E V$.

Let G be a group, and let E/F be a finite Galois extension with Galois group Γ. For $\gamma \in \Gamma$, we define the *Galois conjugate* V_γ as follows. View V as an abelian additive group and define a new scalar multiplication $*_\gamma$ on V by $\lambda *_\gamma v := (\lambda\gamma^{-1})v$ for all $\lambda \in E$ and $v \in V$. We denote this new vector space by V_γ. Then V_γ is an EG-module under the action $v \cdot g := vg$ for $v \in V_\gamma$ and $g \in G$. Note that any E-basis of V is an E-basis of V_γ, so V and V_γ have the same dimension over E. Moreover, V is an irreducible EG-module if and only if V_γ is irreducible, and V and V_γ are isomorphic as FG-modules.

We consider briefly the matrix representation of V_γ for any $\gamma \in \Gamma$. Let $\mathscr{B} = \{v_1, \ldots, v_r\}$ be an E-basis of V and V_γ. Let $g \in G$. For each $i \in [r]$, there exist $\lambda_{i,1}, \ldots, \lambda_{i,r} \in E$ for which $v_i g = \sum_{j=1}^r \lambda_{i,j} v_j$. Then

$$v_i \cdot g = v_i g = \sum_{j=1}^r \lambda_{i,j} v_j = \sum_{j=1}^r (\lambda_{i,j}\gamma) *_\gamma v_j.$$

Therefore, the matrix of the E-endomorphism g of V_γ relative to $\mathscr{B}$ is precisely that of the E-endomorphism g of V relative to $\mathscr{B}$ with γ applied to each entry. In particular, if V has character χ, then V_γ has character χ_γ where $\chi_\gamma(g) := \chi(g)\gamma$ for all $g \in G$.

The next result demonstrates the importance of Galois conjugates.

Lemma 7.2.4 ([6])**.** *Let G be a group and E/F a finite Galois extension with Galois group Γ. Let V be an EG-module. Then*

$$V \otimes_F E \simeq \bigoplus_{\gamma \in \Gamma} V_\gamma,$$

where V is viewed as an FG-module on the left-hand side.

Proof. Enumerate the elements of Γ as $\gamma_1, \ldots, \gamma_r$. Define

$$\begin{array}{rccc} \varphi: & V \otimes_F E & \to & V_{\gamma_1} \oplus \cdots \oplus V_{\gamma_r} \\ & v \otimes \lambda & \mapsto & (\lambda *_{\gamma_1} v, \ldots, \lambda *_{\gamma_r} v) \end{array}$$

for all $v \in V$ and $\lambda \in E$. This is a well-defined F-linear map by the universal property of tensor products, and it is routine to verify that it is also an EG-homomorphism. Moreover, $\dim_E(V \otimes_F E) = \dim_F V = [E:F] \dim_E V = \dim_E(V_{\gamma_1} \oplus \cdots \oplus V_{\gamma_r})$. It therefore remains to show that φ is injective.

Let $\{v_1, \ldots, v_s\}$ be an E-basis of V and $\{e_1, \ldots, e_t\}$ an F-basis of E. Then $\{e_i v_j : i \in [t], j \in [s]\}$ is an F-basis of V. Let $v \in V \otimes_F E$ and suppose that $v \in \ker(\varphi)$. We may write $v = \sum_{i,j}(e_i v_j \otimes \lambda_{i,j})$ for some $\lambda_{i,j} \in E$. Then $\sum_{i,j}(\lambda_{i,j}\gamma^{-1})(e_i v_j) = 0$ for every $\gamma \in \Gamma$. Fix $j \in [s]$. Then $\sum_i \lambda_{i,j}(e_i\gamma) = (\sum_i (\lambda_{i,j}\gamma^{-1})e_i)\gamma = 0$ for all $\gamma \in \Gamma$ since $\{v_1, \ldots, v_s\}$ is an E-basis. Hence if A is the $t \times [E:F]$ matrix whose (i,l)-th entry is $e_i\gamma_l$ and x is the vector $(\lambda_{1,j}, \ldots, \lambda_{t,j})$, then $xA = 0$. Since $\{e_1, \ldots, e_t\}$ is an F-basis of E, it is a known result of Galois theory that A is invertible. Thus $x = 0$. As j was arbitrary, φ is injective. □

Building on Lemma 7.2.4, we obtain much more information about extensions of scalars if we assume that E/F is an extension of finite fields.

Proposition 7.2.5 ([6]). *Let G be a group and E/F an extension of finite fields. Let U be an irreducible FG-module, and let V be an irreducible EG-submodule of $U \otimes_F E$ with character χ. Then*

$$U \otimes_F E \simeq \bigoplus_{\gamma \in \Sigma} V_\gamma,$$

where Σ is a transversal for $\mathrm{Gal}\,(E/F(\chi))$ in $\mathrm{Gal}(E/F)$. In addition, $U \otimes_F E$ is a direct sum of $|\Sigma| = [F(\chi) : F]$ irreducible non-isomorphic EG-modules, and V is FG-isomorphic to a direct sum of $[E : F(\chi)]$ copies of U.

Proof. Let $\Gamma := \mathrm{Gal}(E/F)$. To begin, we claim that the FG-module V is a direct sum of copies of U. Let W be an irreducible FG-submodule of V. Then $\mathrm{Hom}_{FG}(W, V)$ is non-zero, so $\mathrm{Hom}_{EG}(W \otimes_F E, V \otimes_F E)$ is non-zero by Lemma 7.2.1(ii). Since $V \otimes_F E \simeq \oplus_{\gamma \in \Gamma} V_\gamma$ by Lemma 7.2.4, it follows that $\mathrm{Hom}_{EG}(W \otimes_F E, V_{\gamma_0})$ is non-zero for some $\gamma_0 \in \Gamma$. But $W \otimes_F E$ is completely reducible by Lemma 7.2.1(i), so V_{γ_0} is isomorphic to a submodule of $W \otimes_F E$. Hence there exists $0 \neq \varphi \in \mathrm{Hom}_{EG}(V_{\gamma_0}, W \otimes_F E)$. If $\iota : V \to V_{\gamma_0}$ is the trivial additive group homomorphism, then it is easily verified that $0 \neq \iota \circ \varphi \circ (1 \otimes \gamma_0^{-1}) \in \mathrm{Hom}_{EG}(V, W \otimes_F E)$. Thus V is EG-isomorphic to a submodule of $W \otimes_F E$, and so Lemma 7.2.3 implies that $U \simeq W$. In particular, every irreducible FG-submodule of V is isomorphic to U. But we may use properties of the Jacobson radical to prove that V is completely reducible as an FG-module since it is completely reducible as an EG-module [6, Theorem VII.1.16], and the claim follows.

Thus the FG-module V is a direct sum of m copies of U for some m, in which case Lemma 7.2.4 implies that $\oplus_{\gamma \in \Gamma} V_\gamma = V \otimes_F E = (U \otimes_F E)^m$. The EG-modules V_γ and $V_{\gamma'}$ are isomorphic if and only if $\chi_\gamma = \chi_{\gamma'}$ by Theorem 7.1.1, which is true precisely when $\gamma' \gamma^{-1} \in \mathrm{Gal}(E/F(\chi))$. Hence, if Σ is a transversal for $\mathrm{Gal}\,(E/F(\chi))$ in Γ, then $\{V_\gamma : \gamma \in \Sigma\}$ is a set of non-isomorphic EG-modules, and in particular, $|\Sigma| = [F(\chi) : F]$ is the number of isomorphism types among the V_γ. Thus it suffices to show that $U \otimes_F E$ is a direct sum of non-isomorphic irreducible EG-modules, for then $U \otimes_F E \simeq \oplus_{\gamma \in \Sigma} V_\gamma$ and $m = [E : F(\chi)]$.

We may write $U \otimes_F E = W_1 \oplus \ldots \oplus W_r$ where W_i is a direct sum of n_i isomorphic copies of an irreducible EG-module U_i for each $i \in [r]$ such that $U_i \not\simeq U_j$ when $i \neq j$. Then $\mathrm{Hom}_{EG}(W_i, W_j) = 0$ for $i \neq j$, and so Lemma 7.2.1(ii) implies that

$$\mathrm{End}_{FG}(U) \otimes_F E \simeq \mathrm{End}_{EG}\,(U \otimes_F E) \simeq \bigoplus_{i=1}^{r} \mathrm{End}_{EG}(W_i) \simeq \bigoplus_{i=1}^{r} M_{n_i}(\mathrm{End}_{EG}(U_i)).$$

Fix $i \in [r]$. Since F is finite, $\mathrm{End}_{FG}(U)$ is a field. Then $\mathrm{End}_{FG}(U) \otimes_F E$ is a commutative ring, so $M_{n_i}(\mathrm{End}_{EG}(U_i))$ is a commutative ring. Thus $n_i = 1$. □

7.3 Realising representations over subfields

We have seen that if V is an irreducible EG-module, then there exists a unique irreducible FG-module U for which $V \leqslant U \otimes_F E$. In this section, we consider the situation where $V = U \otimes_F E$. In fact, we do this for reducible EG-modules as well.

Let G be a group and E/F an extension of fields. Let V be an EG-module, and let $\alpha : G \to \mathrm{GL}(V)$ be the representation of G corresponding to V. In other words, $\alpha : g \mapsto (v \mapsto vg)$ for all $g \in G$ and $v \in V$. We say that V (or α) can be *realised* (or *written*) over F if there exists an E-basis $\mathscr{B}$ of V such that the matrix of the E-endomorphism g of V relative to $\mathscr{B}$ has entries in F for every $g \in G$. The following elementary result shows how realisability can be interpreted for modules.

Lemma 7.3.1. *Let G be a group and E/F an extension of fields. Let V be an EG-module. Then the following are equivalent.*

(i) V can be realised over F.

(ii) $V \simeq U \otimes_F E$ for some FG-module U.

Furthermore, if V is an irreducible EG-module and (ii) holds, then U is irreducible.

Proof. (i) $\implies$ (ii): Suppose that V can be realised over F. Let $\{v_1, \ldots, v_r\}$ be an E-basis that is a witness to this. Then for each $i \in [r]$ and $g \in G$, there exist $\lambda_{i,1}, \ldots, \lambda_{i,r} \in F$ such that $v_i g = \sum_j \lambda_{i,j} v_j$. Hence if U is the F-subspace of V spanned by $\{v_1, \ldots, v_r\}$, then U is an FG-submodule of V and the map $\varphi : V \to U \otimes_F E$ defined by $v_i \mapsto v_i \otimes 1$ for all $i \in [r]$ extends to an EG-isomorphism.

(ii) $\implies$ (i): Suppose that $V \simeq U \otimes_F E$ for some FG-module U. Let $\{v_1, \ldots, v_r\}$ be an F-basis of U. Then $\{v_1 \otimes 1, \ldots, v_r \otimes 1\}$ is an E-basis of $U \otimes_F E$ that clearly has the desired property. Thus V can be realised over F.

Furthermore, if V is an irreducible EG-module and (ii) holds, then any FG-submodule W of U can be extended to an EG-submodule $W \otimes_F E$ of V, and so U is irreducible. □

Note that when V is irreducible, Lemma 7.2.3 implies that the FG-module U is unique. Lemma 7.2.3 also motivates the following useful observation.

Lemma 7.3.2. *Let G be a group and E/F an extension of fields. Let V be an irreducible EG-module, and suppose that $V \leqslant U \otimes_F E$ for some irreducible FG-module U. Then V can be realised over F if and only if $U \otimes_F E$ is an irreducible EG-module.*

Proof. Certainly V can be realised over F if $U \otimes_F E$ is irreducible. Conversely, suppose that V can be realised over F. Then $V = W \otimes_F E$ for some irreducible FG-module

W, and we conclude that $U \simeq W$ by Lemma 7.2.3. Thus $U \otimes_F E \simeq W \otimes_F E$, and so $V = U \otimes_F E$. Since V is irreducible, so is $U \otimes_F E$. □

In fact, if we have an irreducible representation defined over a finite field, then Proposition 7.2.5 and Lemma 7.3.2 give us a very useful extension of Lemma 7.3.1.

Lemma 7.3.3 ([6]). *Let G be a group and E/F an extension of finite fields. Let V be an irreducible EG-module with character χ. Then V can be realised over F if and only if F contains $\chi(g)$ for all $g \in G$.*

Proof. By Lemma 7.2.3, there exists an irreducible FG-module U for which $V \leqslant U \otimes_F E$. Then Lemma 7.3.2 implies that V can be realised over F precisely when $U \otimes_F E$ is an irreducible EG-module. Since $U \otimes_F E$ is a direct sum of $[F(\chi) : F]$ irreducible EG-modules by Proposition 7.2.5, the EG-module $U \otimes_F E$ is irreducible if and only if $F(\chi) = F$. □

7.4 Absolutely irreducible representations and splitting fields

Now we return to the problem of determining when extensions of scalars are irreducible. To do this, we must look more closely at the structure of the endomorphism algebra.

Let G be a group and F a field. Let V be an irreducible FG-module. For any $\lambda \in F$, the map defined by $v \mapsto \lambda v$ for all $v \in V$ is an FG-endomorphism of V. These endomorphisms form a field that is isomorphic to F, so F can be embedded into $\mathrm{End}_{FG}(V)$ as an F-subalgebra. Normally, we do not distinguish between the field F and its image in $\mathrm{End}_{FG}(V)$.

First we see that $\mathrm{End}_{FG}(V) = F$ when F is an algebraically closed field.

Lemma 7.4.1 (Schur's Lemma, [21]). *Let G be a group and F an algebraically closed field. Let V be an irreducible FG-module. Then $\mathrm{End}_{FG}(V) = F$.*

Proof. Let $\varphi \in \mathrm{End}_{FG}(V)$. Since $\mathrm{End}_{FG}(V)$ has finite dimension over F, the elements $1, \varphi, \varphi^2, \ldots$ are not linearly independent. Thus φ is a root of some non-zero monic polynomial $f(x)$ in $F[x]$. Since F is algebraically closed, there exist $\lambda_1, \ldots, \lambda_r \in F$ such that $f(x) = (x - \lambda_1) \cdots (x - \lambda_r)$. Moreover, φ commutes with all of the elements of F, so we obtain $0 = (\varphi - \lambda_1) \cdots (\varphi - \lambda_r)$. But every non-zero element of $\mathrm{End}_{FG}(V)$ has an inverse, so we must have $\varphi - \lambda_i = 0$ for some i. Thus $\varphi \in F$. □

Now we see that the condition $\mathrm{End}_{FG}(V) = F$ is fundamental to the irreducibility of extensions of scalars of V.

Proposition 7.4.2 ([6]). *Let G be a group and F a field. Let V be an irreducible FG-module. Then the following are equivalent.*

(i) $V \otimes_F E$ is an irreducible EG-module for every extension E/F.

(ii) $V \otimes_F E$ is an irreducible EG-module for some algebraically closed extension E/F.

(iii) $\mathrm{End}_{FG}(V) = F$.

Proof. (i) $\Longrightarrow$ (ii): Take E to be $\overline{F}$.

(ii) $\Longrightarrow$ (iii): Since $V \otimes_F E$ is irreducible for the algebraically closed field E, Lemma 7.4.1 implies that $E = \mathrm{End}_{EG}(V \otimes_F E)$. This is isomorphic to $\mathrm{End}_{FG}(V) \otimes_F E$ by Lemma 7.2.1(ii), so $\mathrm{End}_{FG}(V)$ has dimension 1 over F.

(iii) $\Longrightarrow$ (i): Let E be any extension of F. By Lemma 7.2.1(ii), $\mathrm{End}_{EG}(V \otimes_F E) \simeq \mathrm{End}_{FG}(V) \otimes_F E$, which equals $F \otimes_F E$ by assumption. Since the map $\varphi : F \otimes_F E \to E$ defined by $f \otimes e \mapsto fe$ is an E-isomorphism, it follows that $\mathrm{End}_{EG}(V \otimes_F E)$ has dimension 1 over E. Thus $\mathrm{End}_{EG}(V \otimes_F E)$ is a field. But $V \otimes_F E$ is completely reducible by Lemma 7.2.1(i), so if W is a proper EG-submodule of $V \otimes_F E$, then we have an EG-endomorphism of $V \otimes_F E$ that is not surjective, a contradiction. Thus $V \otimes_F E$ is irreducible. □

When any of the conditions of Proposition 7.4.2 hold, we say that V is an *absolutely irreducible* FG-module.

Proposition 7.4.2 demonstrates that the endomorphism algebra plays an important role in the study of absolutely irreducible representations. In fact, when the endomorphism algebra is a field, it can be used to turn an irreducible representation into an absolutely irreducible one. Let G be a group, F a finite field and V an irreducible FG-module. Then $k := \mathrm{End}_{FG}(V)$ is a finite field, and V is naturally a kG-module, where scalar multiplication is evaluation and the action of G on V is unchanged. Since $F \subseteq k$, we see that $\mathrm{End}_{kG}(V) \subseteq \mathrm{End}_{FG}(V) = k$, so V is an absolutely irreducible kG-module by Proposition 7.4.2. Note that if V is faithful as an FG-module, then V is faithful as a kG-module. Also, observe that G has a regular orbit on the FG-module V if and only if G has a regular orbit on the kG-module V.

We say that a field F is a *splitting field* for a group G if every irreducible FG-module is absolutely irreducible. Let us now consider some basic properties of splitting fields.

Lemma 7.4.3 ([6, 21]). *Let G be a group and E/F an extension of fields.*

(i) If F is a splitting field for G, then E is a splitting field for G. In fact, if $V_1, \ldots, V_r$ form a complete set of non-isomorphic irreducible FG-modules, then $V_1 \otimes_F E, \ldots, V_r \otimes_F E$ form a complete set of non-isomorphic irreducible EG-modules.

(ii) Let E be a splitting field for G. Then F is a splitting field for G if and only if every irreducible EG-module can be realised over F.

(iii) Every algebraically closed field is a splitting field for G.

(iv) If E is algebraically closed, then there is a finite extension of F contained in E that is a splitting field for G.

(v) If E is a splitting field for G and V is an FG-module for which $V \otimes_F E$ is an irreducible EG-module, then V is an absolutely irreducible FG-module.

Proof. (i) Let V be an irreducible EG-module. By Lemma 7.2.3, there exists a unique irreducible FG-module U for which V is an EG-submodule of $U \otimes_F E$. Certainly $U \simeq V_i$ for some i, so V is an EG-submodule of $V_i \otimes_F E$, and $V_i \otimes_F E$ must be irreducible, so $V = V_i \otimes_F E$. In particular, if K is any extension of E, then $V \otimes_E K \simeq V_i \otimes_F K$, and so $V \otimes_E K$ is irreducible. Since V and K were arbitrary, we conclude that E is a splitting field for G. Now suppose that $V_i \otimes_F E \simeq V_j \otimes_F E$ for some i and j. Then V_i and V_j are isomorphic FG-modules by Lemma 7.2.1(v), so $i = j$.

(ii) By (i), it suffices to show that F is a splitting field for G when every irreducible EG-module can be realised over F. Let U be an irreducible FG-module, and let V be an irreducible EG-submodule of $U \otimes_F E$. Since V can be realised over F by assumption, Lemma 7.3.2 implies that $U \otimes_F E$ is an irreducible EG-module. Since E is a splitting field for G, it follows that $E = \mathrm{End}_{EG}(U \otimes_F E)$, and this is isomorphic to $\mathrm{End}_{FG}(U) \otimes_F E$ by Lemma 7.2.1(ii), so $\mathrm{End}_{FG}(U)$ has dimension 1 over F. Thus U is an absolutely irreducible FG-module and F is a splitting field for G.

(iii) Immediate from Lemma 7.4.1.

(iv) Let $\overline{F}$ be the algebraic closure of F in E. Let $V_1, \ldots, V_r$ be a complete set of non-isomorphic irreducible $\overline{F}G$-modules. For each $i \in [r]$, choose a basis $\mathscr{B}_i$ for V_i, and for each $g \in G$, let $M_{i,g}$ denote the set of entries of the matrix of the $\overline{F}$-endomorphism g of V_i relative to $\mathscr{B}_i$. Let M be the union of the sets $M_{i,g}$ for $i \in [r]$ and $g \in G$. Let K be the subfield of $\overline{F}$ generated by F and the elements of M. Then V_i can be realised over K for all $i \in [r]$, so K is a splitting field for G by (ii) and (iii). Lastly, the extension K/F is finite since M is finite and every element of M is algebraic over F.

(v) The EG-module $V \otimes_F E$ is irreducible, so the FG-module V is irreducible, and since E is a splitting field, $V \otimes_F \overline{E} \simeq (V \otimes_F E) \otimes_E \overline{E}$ is also irreducible. Hence V is absolutely irreducible by Proposition 7.4.2(ii). □

Using Lemmas 7.3.3 and 7.4.3, we can construct a smallest splitting field for G.

Proposition 7.4.4 ([6]). *Let G be a group and E an algebraically closed field of positive characteristic p. Then the finite field*

$$\mathbb{F}_p(G) := \mathbb{F}_p(\chi(g) : \chi \in \mathrm{Irr}_E(G), g \in G)$$

is the unique smallest splitting field of characteristic p for G in E.

Proof. By Lemma 7.4.3(iv), there exists a finite extension F of $\mathbb{F}_p$ contained in E that is a splitting field for G. Let $V_1, \ldots, V_r$ be a complete set of non-isomorphic irreducible FG-modules. Then $V_1 \otimes_F E, \ldots, V_r \otimes_F E$ form a complete set of non-isomorphic irreducible EG-modules by Lemma 7.4.3(i). For each i, let χ_i be the character of V_i. Then χ_i is also the character of $V_i \otimes_F E$. Thus $K := \mathbb{F}_p(G)$ is a subfield of F. Since K contains $\chi_i(g)$ for all i and $g \in G$, and since F is finite, Lemma 7.3.3 implies that V_i can be realised over K for each i, so by Lemma 7.4.3(ii), K is a splitting field for G. If k is any other splitting field for G contained in E, then repeating the argument which showed that $K \subseteq F$ yields that K is also a subfield of k. □

As a consequence of Proposition 7.4.4, we make the following definition. For a group G and an algebraically closed field E of positive characteristic p, we define the *smallest splitting field for G in E* to be $\mathbb{F}_p(G) = \mathbb{F}_p(\chi(g) : \chi \in \mathrm{Irr}_E(G), g \in G)$.

7.5 Representations of index 2 subgroups

In this section, we focus on the representation theory of index 2 subgroups, which is especially well behaved. We do this in order to understand the representation theory of the alternating group.

To begin, we briefly introduce the concepts of restriction and induction. Let G be a group and F a field. Let H be a subgroup of G, and let V be an FG-module. Then we may view V as an FH-module by forgetting how elements in $G \setminus H$ act on V. The FH-module V is denoted by $V \downarrow H$ and referred to as the *restricted module* of V from G to H. We say that $V \downarrow H$ *splits* if it is not irreducible. On the other hand, if W is an FH-module, then since FG is naturally an (FH, FG)-bimodule, we may define the *induced module* $W \uparrow G$ of W from H to G to be the FG-module $W \otimes_{FH} FG$.

Using the concept of induction, we see that every irreducible FH-module arises as a submodule of the restriction of some irreducible FG-module.

Lemma 7.5.1. *Let G be a group with subgroup H, and let F be a field. If W is an irreducible FH-module, then there is an irreducible FG-module V for which $W \leqslant V \downarrow H$.*

Proof. Since $W \uparrow G$ has a composition series, there exists an irreducible FG-module V for which $\mathrm{Hom}_{FG}(W \uparrow G, V)$ is non-zero. Then there exists $0 \neq \varphi \in \mathrm{Hom}_{FH}(W, V \downarrow H)$ by Frobenius-Nakayama reciprocity [6, Theorem VII.4.5]. Since W is an irreducible FH-module, it follows that φ is injective, and so W is an FH-submodule of $V \downarrow H$. □

Now suppose that N is a normal subgroup of a group G and F is a field. Let V be an FG-module, and let W be an irreducible FN-submodule of V. Then for any $g \in G$, the normality of N implies that Wg is an irreducible FN-submodule of V. Using this observation, the structure of $V \downarrow N$ is easily determined when N has index 2.

Lemma 7.5.2. *Let G be a group with an index 2 subgroup N, and let F be a field. Let V be an irreducible FG-module, and let W be an irreducible FN-submodule of V. Then either $V \downarrow N = W$, or $V \downarrow N = W \oplus Wg$ for any $g \in G \setminus N$.*

Proof. Since Wg is an irreducible FN-submodule of V for every $g \in G$, it follows that $\sum_{g \in G} Wg$ is an FG-submodule of V and is therefore equal to V. Fix $g \in G \setminus N$. Then $V \downarrow N = W + Wg$ since N has index 2 in G. But W and Wg are irreducible, so either $W = Wg$ or $W \cap Wg = \emptyset$. Thus either $V \downarrow N = W$ or $V \downarrow N = W \oplus Wg$. □

Note that a similar result can be proved for arbitrary normal subgroups, but this more general result will not be needed.

Closely related to the irreducibility of $V \downarrow N$ are the concepts of the sign representation and the associate of V, which we now define. Let G be a group with an index 2 subgroup N, and let F be any field. Then F becomes an FG-module if we define $\lambda g := \lambda$ when $g \in N$ and $\lambda g := -\lambda$ when $g \in G \setminus N$ for every $\lambda \in F$. This one-dimensional FG-module is called the *sign module* or *sign representation* and is denoted by sgn. For an FG-module V, the F-vector space $V \otimes_F \mathrm{sgn}$, called the *associate* of V, becomes an FG-module by defining $(v \otimes \lambda)g := (vg) \otimes (\lambda g)$ for all $v \in V$, $\lambda \in \mathrm{sgn}$ and $g \in G$. Then $V \otimes_F \mathrm{sgn} = \{v \otimes 1 : v \in V\}$, and so $V \otimes_F \mathrm{sgn}$ is irreducible when V is irreducible, and if $\{v_i : 1 \leqslant i \leqslant n\}$ is an F-basis for V, then $\{v_i \otimes 1 : 1 \leqslant i \leqslant n\}$ is an F-basis for $V \otimes_F \mathrm{sgn}$.

This last observation has several consequences. Certainly V and $V \otimes_F \mathrm{sgn}$ have the same dimension. In addition, if $g \in G$ and $[g]$ is the matrix of the F-endomorphism g of V with respect to the basis $\{v_i : 1 \leqslant i \leqslant n\}$, then the matrix of the F-endomorphism g of $V \otimes_F \mathrm{sgn}$ with respect to the basis $\{v_i \otimes 1 : 1 \leqslant i \leqslant n\}$ is $[g]$ when $g \in N$ and $-[g]$ when $g \in G \setminus N$. In particular, if χ is the character of V and ψ is the character of $V \otimes_F \mathrm{sgn}$, then $\psi(g) = \chi(g)$ when $g \in N$ and $\psi(g) = -\chi(g)$ when $g \in G \setminus N$.

Our next result describes the relationship between the associate of an FG-module V, the character of V, and the irreducibility of $V \downarrow N$.

Lemma 7.5.3. *Let G be a group with an index 2 subgroup N, and let F be a field whose characteristic is not 2. Let V be an irreducible FG-module with character χ. Then the following statements hold.*

(i) $V \simeq V \otimes_F \mathrm{sgn}$ if and only if $\chi(g) = 0$ for all $g \in G \setminus N$.

(ii) If $\chi(g) \neq 0$ for some $g \in G \setminus N$, then $V \downarrow N$ is irreducible.

(iii) If $V \downarrow N$ is absolutely irreducible, then $\chi(g) \neq 0$ for some $g \in G \setminus N$.

Proof. (i) By Theorem 7.1.1, $V \simeq V \otimes_F \mathrm{sgn}$ if and only if $\chi(g) = -\chi(g)$ for all $g \in G \setminus N$. Since the characteristic of F is not 2, the result follows.

(ii) Suppose that $V \downarrow N$ is not irreducible, and let W be an irreducible FN-submodule of $V \downarrow N$. Then Lemma 7.5.2 implies that $V \downarrow N = W \oplus Wg_0$ for any $g_0 \in G \setminus N$. The map $\varphi : W \oplus Wg_0 \to W \uparrow G$ defined by $w_1 + w_2 g_0 \mapsto w_1 \otimes 1 + w_2 \otimes g_0$ for all $w_1, w_2 \in W$ is easily checked to be an FG-isomorphism. Since $V \otimes_F \mathrm{sgn} \downarrow N \simeq V \downarrow N$, it follows that $V \simeq W \uparrow G \simeq V \otimes_F \mathrm{sgn}$. Thus $\chi(g) = 0$ for all $g \in G \setminus N$ by (i).

(iii) Suppose that $V \downarrow N$ is absolutely irreducible but $\chi(g) = 0$ for all $g \in G \setminus N$. Then by (i) there exists an FG-isomorphism $\varphi : V \to V \otimes_F \mathrm{sgn}$. Let $\psi : V \to V \otimes_F \mathrm{sgn}$ be defined by $v \mapsto v \otimes 1$. Then ψ is an FN-isomorphism and $\varphi\psi^{-1} \in \mathrm{End}_{FN}(V \downarrow N) = F$, so there exists $\lambda \in F^*$ for which $v\varphi = \lambda(v \otimes 1)$ for all $v \in V$. But if $g \in G \setminus N$, then $\lambda(v \otimes 1)g = v\varphi g = (vg)\varphi = \lambda(vg \otimes 1) = -\lambda(v \otimes 1)g$ for all $v \in V$, so $2\lambda = 0$. Thus either $\mathrm{char}(F) = 2$ or $\lambda = 0$, both of which are contradictions. □

Note that if the characteristic of F is 2, then for any group G with an index 2 subgroup N and any FG-module V, the associate $V \otimes_F \mathrm{sgn}$ is always isomorphic to V.

7.6 Brauer characters

The irreducible representations of S_n and A_n over $\mathbb{F}_p$ for $n \leqslant 12$ and $p \leqslant n$ are described in the Brauer Atlas [44] using Brauer characters, which are character-like functions that are built using positive characteristic representations but are only defined over the complex numbers. Every finite group has a Brauer character table for any prime p, and this table contains a wealth of information about the irreducible representations of G in characteristic p. We wish to have some understanding of these functions and tables in order to use them to determine the regular orbits of the symmetric and alternating groups.

Normally, Brauer characters are defined using p-modular systems or algebraically closed fields [22, 39], but this requires concepts from algebraic number theory that will not be needed elsewhere. In fact, we only need to work with Brauer characters as they

are defined in [44], so we adopt their approach and construct Brauer characters over finite fields with the following property.

Let G be a group. A field F has the *splitting property for* G if, for any FG-module V and $g \in G$, the characteristic polynomial of the F-endomorphism g of V splits into linear factors over F. Of course, any algebraically closed field has the splitting property, but it turns out that there is always a finite field with the splitting property for G. This is a consequence of the following observation about the eigenvalues of g.

Lemma 7.6.1. *Let G be a group and F a field of positive characteristic p. Write $|G| = p^a m$ where $p \nmid m$ and a is a non-negative integer. Let V be an FG-module and $g \in G$. Then every eigenvalue of the F-endomorphism g of V is an m-th root of unity.*

Proof. Fix $g \in G$. Then the polynomial $x^{|G|} - 1 \in F[x]$ annihilates the F-endomorphism g, and so the minimal polynomial of g over F divides $x^{|G|} - 1 = (x^m - 1)^{p^a}$. Thus any eigenvalue of g is an m-th root of unity. □

Therefore, if $|G| = p^a m$ where $p \nmid m$ and F is a field of characteristic p that contains all m-th roots of unity, then F has the splitting property for G. In particular, if n is the order of p in the multiplicative group of integers modulo m, then the finite field $\mathbb{F}_{p^n}$ contains all m-th roots of unity and hence has the splitting property for G.

An important aspect of fields with the splitting property is that they are splitting fields, which we now prove.

Lemma 7.6.2. *Let G be a group, and let F be a field of positive characteristic with the splitting property for G. Then F is a splitting field for every subgroup of G.*

Proof. Let $E := \overline{F}$. Let $H \leqslant G$, and let V be an irreducible EH-module of dimension k with character χ. Let $g \in H$, and let $\lambda_1, \ldots, \lambda_k \in E$ be the eigenvalues of the E-endomorphism g of V. By Lemma 7.2.3, there exists an irreducible FH-module W for which $V \leqslant W \otimes_F E$. Moreover, Lemma 7.5.1 implies that there exists an irreducible FG-module U of dimension l, say, for which $W \leqslant U \downarrow H$. Then $V \leqslant W \otimes_F E \leqslant (U \downarrow H) \otimes_F E = (U \otimes_F E) \downarrow H$. Since F has the splitting property for G, the characteristic polynomial of the F-endomorphism g of U splits into linear factors over F. Let $\mu_1, \ldots, \mu_l \in F$ be the eigenvalues of this endomorphism. Then they are also the eigenvalues of the E-endomorphism g of $U \otimes_F E$. But an eigenvalue of the E-endomorphism g of V is also an eigenvalue of the E-endomorphism g of $U \otimes_F E$, so $\{\lambda_1, \ldots, \lambda_k\} \subseteq \{\mu_1, \ldots, \mu_l\}$. In particular, $\lambda_i \in F$ for every $i \in [k]$, and so $\chi(g) = \sum_{i=1}^{k} \lambda_i \in F$. Since V was arbitrary, we conclude that the smallest splitting field $\mathbb{F}_p(H)$ for H in E is a subfield of F. Thus F is a splitting field for H by Proposition 7.4.4 and Lemma 7.4.3(i). □

Let G be a group. If p is a prime, then an element $g \in G$ is said to be *p-regular* if its order is not divisible by p. We write $G_{p'}$ for the set of p-regular elements of G. It turns out that the image of a character only depends on $G_{p'}$, as we now see.

Lemma 7.6.3 ([39])**.** *Let G be a group and $g \in G$. Let p be a prime. Then there exists $g_{p'} \in G_{p'}$ such that for any field F of characteristic p and any FG-module with character χ we have $\chi(g) = \chi(g_{p'})$.*

Proof. Let g have order $p^b n$ where $p \nmid n$ and b is a non-negative integer. Since p^b and n are relatively prime, there exist integers k and l for which $kp^b + ln = 1$, and so $g = g^{kp^b} g^{ln}$. Let $g_{p'} := g^{kp^b}$, and note that $g_{p'}$ is indeed p-regular.

Suppose that F is a field of characteristic p with the splitting property for G, and let V be an FG-module with character χ and dimension k. Then F contains all of the eigenvalues of g, so g has a Jordan canonical form. Let $\mathscr{B}$ be a basis of V for which the matrix $[g]$ of g with respect to this basis is in Jordan canonical form. Then the matrix of $g_{p'}$ with respect to $\mathscr{B}$ is a power of $[g]$, as is the matrix of $x := g^{ln}$. Consequently, these matrices are all upper triangular. Let $\lambda_1, \ldots, \lambda_k$ be the eigenvalues of g and $\mu_1, \ldots, \mu_k$ the eigenvalues of $g_{p'}$. Then since $g = x g_{p'}$, it follows that $\lambda_1 \mu_1^{-1}, \ldots, \lambda_k \mu_k^{-1}$ are the eigenvalues of x. We can write $|G| = p^a m$ where $p \nmid m$ and a is a non-negative integer. Then the eigenvalues of x are m-th roots of unity by Lemma 7.6.1. However, the order of x is a power of p, and so the order of $\lambda_i \mu_i^{-1}$ is also a power of p for all $i \in [k]$. This forces $\lambda_i = \mu_i$ for all $i \in [k]$, and so $\chi(g) = \sum_{i=1}^k \lambda_i = \sum_{i=1}^k \mu_i = \chi(g_{p'})$.

Now suppose that F is an arbitrary field of characteristic p, and let V be an FG-module with character χ. Then there exists an extension E of F that has the splitting property for G, and $V \otimes_F E$ is an EG-module with character χ, so $\chi(g) = \chi(g_{p'})$. □

Note that the p-regular element $g_{p'}$ defined in the proof of Lemma 7.6.3 is normally called the *p'-part* of g.

For an integer r, let $U_r(\mathbb{C})$ denote the set of r-th roots of unity in $\mathbb{C}$. Let G be a group, and let $\mathbb{F}_q$ be a field with the splitting property for G. Observe that $\mathbb{F}_q^*$ and $U_{q-1}(\mathbb{C})$ are both isomorphic to the cyclic group C_{q-1}. This motivates the following definition, which is not standard but is useful for our purposes. We say that $(\mathbb{F}_q, \theta)$ is a *p-system for G* if p is a prime, $\mathbb{F}_q$ is a field of characteristic p that has the splitting property for G, and $\theta : \mathbb{F}_q^* \to U_{q-1}(\mathbb{C})$ is a group isomorphism.

At last we are able to define Brauer characters. Let G be a group, and let $(\mathbb{F}_q, \theta)$ be a p-system for G. Let V be an $\mathbb{F}_q G$-module of dimension k. We construct a function $\beta : G_{p'} \to \mathbb{C}^*$ as follows. Let $g \in G_{p'}$, and let $\lambda_1, \ldots, \lambda_k \in \mathbb{F}_q^*$ be the eigenvalues of the

$\mathbb{F}_q$-endomorphism g of V. Note that this list necessarily includes multiplicities. Then we define $\beta(g) := \sum_{i=1}^{k}(\lambda_i)\theta$. The function β is called the *Brauer character of V with respect to $(\mathbb{F}_q, \theta)$*. When the p-system is specified, we refer to β as the Brauer character of V.

Brauer characters behave like characters in many ways. For example, since similar matrices have the same eigenvalues, it follows that $\beta(h^{-1}gh) = \beta(g)$ for all $h \in G$ and $g \in G_{p'}$. Thus Brauer characters are constant on conjugacy classes. Moreover, again because similar matrices have the same eigenvalues, it follows that isomorphic $\mathbb{F}_qG$-modules have the same Brauer character (though the converse is not true). In fact, Brauer characters often behave better than characters. For example, if V has character χ, then $\chi(1)$ is equivalent to $\dim_{\mathbb{F}_q}(V)$ modulo the prime p, whereas $\beta(1) = \dim_{\mathbb{F}_q}(V)$.

We wish to have some method for recovering the character of an $\mathbb{F}_qG$-module V if we are given the Brauer character of V. We expect this to be possible, for if V has character χ and the $\mathbb{F}_q$-endomorphism g of V has eigenvalues $\lambda_1, \ldots, \lambda_k$ where $g \in G$, then $\chi(g) = \sum_{i=1}^{k} \lambda_i$. It turns out that this can be done by extending the inverse of θ to a ring homomorphism. Let G be a group, and let $(\mathbb{F}_q, \theta)$ be a p-system for G. Let ξ be a primitive $(q-1)$-th root of unity in $U_{q-1}(\mathbb{C})$. Then the map

$$\begin{array}{rccc} {}^{-}: & \mathbb{Z}[\xi] & \to & \mathbb{F}_q \\ & \xi & \mapsto & \xi\theta^{-1} \end{array}$$

is a well-defined ring homomorphism that extends θ^{-1}. In particular, since the image of the Brauer character of an $\mathbb{F}_qG$-module V lies in $\mathbb{Z}[\xi]$, we obtain the following.

Lemma 7.6.4 ([39])**.** *Let G be a group with p-system $(\mathbb{F}_q, \theta)$. Let V be an $\mathbb{F}_qG$-module with character χ and Brauer character β. Then $\overline{\beta(g)} = \chi(g)$ for all $g \in G_{p'}$.*

Proof. Let $g \in G_{p'}$, and let $\lambda_1, \ldots, \lambda_k$ be the eigenvalues of the $\mathbb{F}_q$-endomorphism g of V. Then $\overline{\beta(g)} = \sum_{i=1}^{k} \overline{\lambda_i\theta} = \sum_{i=1}^{k} \lambda_i = \chi(g)$. □

Consequently, Lemmas 7.6.3 and 7.6.4 imply that we can reconstruct the character of an $\mathbb{F}_qG$-module V from the Brauer character of V. In fact, we can say even more.

Theorem 7.6.5 ([6, 39])**.** *Let G be a group with p-system $(\mathbb{F}_q, \theta)$. Let V and W be irreducible $\mathbb{F}_qG$-modules. Then the following are equivalent.*

(i) V and W are isomorphic $\mathbb{F}_qG$-modules.

(ii) V and W have the same character.

(iii) V and W have the same Brauer character.

Proof. The equivalence (i) $\iff$ (ii) is Theorem 7.1.1. Moreover, (i) $\implies$ (iii) is clear, and (iii) $\implies$ (ii) follows from Lemmas 7.6.3 and 7.6.4. □

As a result of Theorem 7.6.5, we can now define the Brauer character table of a group. Let G be a group, and let $(\mathbb{F}_q, \theta)$ be a p-system for G. We write $\mathrm{IBr}_p(G)$ for the complete set of Brauer characters of non-isomorphic irreducible $\mathbb{F}_qG$-modules, and we define the *p-Brauer character table of G* to be the table whose rows correspond to elements in $\mathrm{IBr}_p(G)$, whose columns correspond to the conjugacy classes of p-regular elements of G, and whose entries are $\beta_i(g_j)$ where $\beta_i \in \mathrm{IBr}_p(G)$ and g_j is in the j-th conjugacy class of p-regular elements. We omit the prefix p- when the context permits.

Although the definition of a p-Brauer character table appears to depend on the choice of p-system, it turns out that this is not the case. It can be shown that if B_i is the p-Brauer character table of G with respect to the p-system $(\mathbb{F}_q, \theta_i)$ for $i = 1, 2$, then the columns of B_2 are a permutation of the columns of B_1. Moreover, the Brauer Atlas [44] describes a way of lifting the eigenvalues in $\overline{\mathbb{F}_p}$ to $\mathbb{C}$ that is independent of any finite fields the eigenvalues are considered to belong to (we give more details of this lifting below), and so it does not matter which field with the splitting property we choose.

Brauer character tables have some nice properties. First of all, the Brauer character table of G is closely related to the ordinary character table of G, for it turns out that if χ is an ordinary character of G, then the restriction of χ to the p-regular elements of G is a Brauer character of G [39, Theorem 15.6]. In fact, $|\mathrm{IBr}_p(G)|$ is precisely the number of conjugacy classes of p-regular elements of G [39, Corollary 15.11].

The case where the characteristic of the field does not divide the order of the group is particularly nice, for if G is a group and p is a prime for which $p \nmid |G|$, then every element of G is p-regular. In particular, the p-Brauer character of G is defined on every element of G, and so every ordinary character is a Brauer character. But $|\mathrm{IBr}_p(G)|$ is the number of conjugacy classes of G, and this is equal to $|\mathrm{Irr}_{\mathbb{C}}(G)|$. Thus the p-Brauer table of G is the same as the ordinary character table of G up to a permutation of the rows and columns [39, Theorem 15.13].

In order to use the Brauer character table of a group, we wish to extend the definition of a Brauer character to all absolutely irreducible representations. Let G be a group, and let B be the p-Brauer character table of G with respect to the p-system $(\mathbb{F}_q, \theta)$. Let F be a field of characteristic p, and let V be an absolutely irreducible FG-module with character χ. Note that $\mathbb{F}_q$ can be viewed as a subfield of $\overline{F}$ since every element of $\mathbb{F}_q$ is algebraic over $\mathbb{F}_p$. Then since $\mathbb{F}_q$ is a splitting field for G by Lemma 7.6.2, Lemma 7.4.3(i) implies that there exists a unique irreducible $\mathbb{F}_qG$-module U for which $V \otimes_F \overline{F} \simeq U \otimes_{\mathbb{F}_q} \overline{F}$. If β is the Brauer character of U, then we say that β is the *Brauer character* of V. Note that U has character χ. Note also that $\dim_F(V) = \beta(1)$, so the dimension of V can often be

used to identify the Brauer character of V.

This next result shows how to use [44] to determine whether absolutely irreducible representations can be written over subfields.

Lemma 7.6.6. *Let G be a group with p-Brauer character table B. Let V be an absolutely irreducible $\mathbb{F}_{p^n}G$-module with Brauer character β. If $m \mid n$, then V can be realised over $\mathbb{F}_{p^m}$ if and only if $\overline{\beta(g)} \in \mathbb{F}_{p^m}$ for all $g \in G_{p'}$.*

Proof. Suppose that V has character χ. Then V can be realised over $\mathbb{F}_{p^m}$ if and only if $\chi(g) \in \mathbb{F}_{p^m}$ for all $g \in G_{p'}$ by Lemmas 7.3.3 and 7.6.3. Since $\overline{\beta(g)} = \chi(g)$ for all $g \in G_{p'}$ by Lemma 7.6.4, the result follows. □

Of course, if $\beta(g)$ is an integer, then $\overline{\beta(g)} \in \mathbb{F}_p$, so we only need to worry about the irrational entries in the Brauer character table to use Lemma 7.6.6. Appendix 1 of [44] contains lists of the most common irrationalities and their images under the map $^-$ for small primes. To see how the appendix can be used, we need to know how the map $^-$ is defined.

First we describe how [44] constructs finite fields. Fix a prime p. For each positive integer n, let $f_n(x)$ be a polynomial of degree n in $\mathbb{F}_p[x]$ for which the following hold:

(i) The polynomial $f_n(x)$ is monic and primitive (and therefore irreducible).

(ii) If $d \mid n$, then $x^{(p^n-1)/(p^d-1)} + (f_n)$ is a root of $f_d(x)$ in $\mathbb{F}_p[x]/(f_n)$.

The *n-th Conway polynomial* C_n is then defined to be the smallest polynomial of degree n satisfying conditions (i) and (ii) with respect to an ordering whose definition can be found in [44]. Note that these polynomials always exist (see [44] for a reference). Then for any prime p and integer n, [44] constructs the finite field of order p^n as $\mathbb{F}_p[x]/(C_n)$.

Since $x + (C_n)$ is a primitive $(p^n - 1)$-th root of unity that generates the cyclic group $(\mathbb{F}_p[x]/(C_n))^*$ by (i), we can define the map

$$\begin{aligned} \theta_n : \ (\mathbb{F}_p[x]/(C_n))^* &\to U_{p^n-1}(\mathbb{C}) \\ x + (C_n) &\mapsto \exp(\tfrac{2\pi i}{p^n-1}). \end{aligned}$$

Then θ_n is a group isomorphism, so we can extend θ_n^{-1} to the ring homomorphism $^-$ in the usual way. Moreover, $\mathbb{F}_p[x]/(C_d)$ embeds into $\mathbb{F}_p[x]/(C_n)$ by mapping $f(x) + (C_d) \mapsto f(x^{(p^n-1)/(p^d-1)}) + (C_n)$ for all $f(x) \in \mathbb{F}_p[x]$ by (ii), so $^-$ is consistent with subfields and field extensions.

Now suppose that ζ is listed in [44, Appendix 1] for the prime p. Next to ζ in the table are two entries. One is a Conway polynomial C_n, and the other is a polynomial $f(x) \in \mathbb{F}_p[x]$ of degree at most $n - 1$. Then [44] implies that $\zeta \in \mathbb{Z}[\exp(\frac{2\pi i}{p^n-1})]$ and

$\overline{\zeta} = f(x) + (C_n)$. Furthermore, when an irrational is not listed in [44, Appendix 1], its image under $^-$ can often be computed using GAP [30]. Thus we can usually determine whether a given finite field contains $\overline{\beta(g)}$ when $\beta(g)$ is irrational.

Let us now return to groups with index 2 subgroups to see how Brauer character tables can be used to understand representations of these groups over different fields. Let G be a group with an index 2 subgroup N, and let E/F be a field extension where F is a splitting field for G. Recall that if U is an irreducible EG-module, then Lemma 7.4.3(i) implies that there exists a unique irreducible FG-module V for which $U = V \otimes_F E$. Combined with Lemma 7.6.6 (when E is finite and a splitting field for N), our next and final result of this section enables us to determine the structure of $V \downarrow N$ from the structure of $U \downarrow N$ and the Brauer character tables of G and N.

Lemma 7.6.7. *Let G be a group with an index 2 subgroup N, and let E/F be a field extension of characteristic p where F and E are splitting fields for G and N respectively. Let U be an irreducible EG-module, and let V be the unique irreducible FG-module for which $U = V \otimes_F E$. Let W be an irreducible EN-submodule of U and $g_0 \in G \setminus N$. Then we have the following possibilities.*

(i) If $U \downarrow N = W$, then $V \downarrow N$ is absolutely irreducible.

(ii) If $U \downarrow N = W \oplus Wg_0$ and W can be realised over F, then $V \downarrow N$ splits, and if not, then $V \downarrow N$ is irreducible but not absolutely irreducible.

Moreover, suppose that $p \geqslant 3$ and let B be the p-Brauer character table of G. If U has Brauer character β, then $U \downarrow N$ is irreducible if and only if $\beta(g) \neq 0$ for some $g \in G_{p'} \setminus N$.

Proof. Note that $U \downarrow N = (V \downarrow N) \otimes_F E$. Hence if $U \downarrow N$ is irreducible, then $V \downarrow N$ is absolutely irreducible by Lemma 7.4.3(v) since E is a splitting field for N. By Lemma 7.5.2, we may therefore assume that $U \downarrow N = W \oplus Wg_0$. Let X be an irreducible FN-submodule of V. Again by Lemma 7.5.2, either $V \downarrow N = X$ or $V \downarrow N = X \oplus Xg_0$. In the former case, $X \otimes_F E = U \downarrow N = W \oplus Wg_0$, and so $V \downarrow N$ is not absolutely irreducible and $X \otimes_F E$ is not irreducible. In the latter case, $U \downarrow N \simeq (X \otimes_F E) \oplus (Xg_0 \otimes_F E)$, so $X \otimes_F E$ is irreducible by Lemma 7.5.2, and without loss of generality, we may assume that $W \simeq X \otimes_F E$. Since $W \leqslant X \otimes_F E$ in both cases, Lemma 7.3.2 implies that W can be realised over F precisely when $V \downarrow N$ is not irreducible.

Now suppose that U has character χ and B is the p-Brauer character table of G with respect to some p-system $(\mathbb{F}_q, \theta)$. View $\mathbb{F}_q$ as a subfield of $\overline{E}$, and let X be the unique irreducible $\mathbb{F}_qG$-module for which $U \otimes_E \overline{E} \simeq X \otimes_{\mathbb{F}_q} \overline{E}$. Then X has character χ and Brauer character β. Let γ be the Brauer character of $X \otimes_{\mathbb{F}_q} \mathrm{sgn}$. Lemma 7.5.3 implies

that $U \downarrow N$ is irreducible if and only if $\chi(g) \neq 0$ for some $g \in G \setminus N$, and also that this occurs if and only if $X \not\cong X \otimes_{\mathbb{F}_q} \mathrm{sgn}$. Since $X \not\cong X \otimes_{\mathbb{F}_q} \mathrm{sgn}$ if and only if $\beta \neq \gamma$ by Theorem 7.6.5, it suffices to show that $\beta \neq \gamma$ if and only if $\beta(g) \neq 0$ for some $g \in G_{p'} \setminus N$.

Let $g \in G_{p'} \setminus N$, and let $\lambda_1, \ldots, \lambda_k$ be the eigenvalues of the $\mathbb{F}_q$-endomorphism g of X. Fix $i \in [k]$. If v is an eigenvector of λ_i, then $(v \otimes 1)g = (vg) \otimes (-1) = -\lambda_i(v \otimes 1)$, and so the eigenvalues of the $\mathbb{F}_q$-endomorphism g of $X \otimes_{\mathbb{F}_q} \mathrm{sgn}$ are $-\lambda_1, \ldots, -\lambda_k$. Thus $\gamma(g) = \sum_{i=1}^{k}(-\lambda_i)\theta = (-1)\theta\beta(g)$. Similarly, if $g \in N_{p'}$ and $\lambda_1, \ldots, \lambda_k$ are the eigenvalues of the $\mathbb{F}_q$-endomorphism g of X, then they are also the eigenvalues of the $\mathbb{F}_q$-endomorphism g of $X \otimes_{\mathbb{F}_q} \mathrm{sgn}$, so $\gamma(g) = \beta(g)$. Thus $\beta \neq \gamma$ if and only if there exists $g \in G_{p'} \setminus N$ for which $(-1)\theta\beta(g) \neq \beta(g)$. But $1 = 1\theta \neq (-1)\theta$ since $p \neq 2$, so the desired result follows. □

Note that if G is a group with an index 2 subgroup N, then there are no 2-regular elements in $G \setminus N$, for if $g \in G_{2'}$ then the order of g is odd, and so $g \in N$.

Chapter 8

Regular orbits of S_n and A_n

This chapter is devoted to the proof of Theorem 8.0.1, stated below, which describes which faithful irreducible representations of the symmetric and alternating groups admit regular orbits. Much of the material in this chapter was obtained in collaboration with O'Brien and Saxl [26], namely Theorem 8.0.1 and the material in Sections 8.2 and 8.4. In particular, computations using the computer package Magma [8] were carried out by O'Brien. Note that Section 8.3 will also be included in [26], but its material is entirely the author's.

It is well known that the irreducible $\mathbb{F}_pS_n$-modules are characterised in terms of the p-regular partitions of n, and following convention, we write D^μ for the irreducible $\mathbb{F}_pS_n$-module corresponding to the p-regular partition μ. These concepts will be considered in greater detail in Section 8.1. Note that there exists a unique p-regular partition λ for which $D^\lambda \simeq D^\mu \otimes_{\mathbb{F}_p} \mathrm{sgn}$, and we denote this partition by $m(\mu)$. Moreover, recall that if V is an irreducible $\mathbb{F}_pA_n$-module, then there exists a p-regular partition μ for which $V \leqslant D^\mu \downarrow A_n$ by Lemma 7.5.1.

Theorem 8.0.1. *Let G be S_n or A_n where $n \geqslant 5$, and let p be a prime. Let V be a faithful irreducible $\mathbb{F}_pG$-module, and let μ be a p-regular partition of n for which $V \leqslant D^\mu \downarrow G$.*

(i) Suppose that μ or $m(\mu)$ is $(n-1,1)$. Then G has a regular orbit on V if and only if either $p > n$, or $p = n-1$ and $G = A_n$.

(ii) Suppose that neither μ nor $m(\mu)$ is $(n-1,1)$. Then G has a regular orbit on V if and only if n, p, μ and G are not listed in Table 8.1.

Note that for any 2-regular partition μ, the partition $m(\mu)$ is the same as μ, and so $m(\mu)$ is omitted from Table 8.1.

n	p	μ	G	$\dim_{\mathbb{F}_p}(V)$	$m(\mu)$
5	2	(3,2)	S_5, A_5	4	-
6	2	(4,2)	S_6, A_6	4	-
	3	(4,1,1)	S_6, A_6	6	(4,1,1)
	5	(3,3)	S_6	5	(2,2,2)
		(2,2,2)	S_6	5	(3,3)
7	2	(5,2)	S_7	14	-
		(4,3)	S_7	8	-
			A_7	4	-
8	2	(6,2)	S_8, A_8	14	-
		(5,3)	S_8	8	-
			A_8	4	-
9	2	(5,4)	S_9	16	-
			A_9	8	-
		(5,3,1)	A_9	20	-
10	2	(6,4)	S_{10}, A_{10}	16	-
12	2	(7,5)	S_{12}	32	-

Table 8.1: $\mathbb{F}_pG$-modules V on which G has no regular orbits.

Köhler and Pahlings [46] have recently extended work by Goodwin [34] to prove a more general version of Theorem 8.0.1 in coprime characteristic, which for the group S_n requires the additional assumption that $D^\mu \downarrow A_n$ is irreducible. However, their methods do not always determine whether S_n has a regular orbit on D^μ, so we have included the case where $p > n$ and $D^\mu \downarrow A_n$ is irreducible.

This chapter is organised as follows. In Section 8.1 we outline the representation theory of S_n. In Section 8.2 the bounds of Section 6.3 are applied to modules with large dimension, and in Section 8.3 regular orbits are explicitly constructed for modules with small dimension. Lastly, in Section 8.4 we combine these results and consider small n.

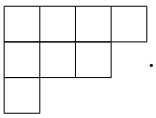
8.1 Irreducible FS_n-modules

In this section, we outline the characterisation of irreducible FS_n-modules in terms of partitions of n, as well as some important properties of these modules. Note that most of the material in this section is drawn from James [40].

Let F be an arbitrary field with characteristic p, where for this chapter we adopt the convention that the characteristic of F is the size of its prime subfield. A *partition* μ of n is a tuple $\mu = (\mu_1, \mu_2, \dots)$ such that $n = \sum_i \mu_i$ where the μ_i are non-negative integers

and $\mu_i \geqslant \mu_{i+1}$ for all $i \geqslant 1$. If $\mu_i > 0$, then we say that μ_i is a *part* of μ. Usually, we write partitions in the form $(\mu_1^{a_1}, \ldots, \mu_l^{a_l})$ where $\mu_i > \mu_{i+1} > 0$ for all $i \in [l-1]$ and the a_i are positive integers for which $\sum_{i=1}^{l} a_i \mu_i = n$. When p is a prime or ∞, we say that the partition μ is *p-regular* if no part of the partition μ is repeated p times.

Let μ be a partition of n. The *Young diagram* $[\mu]$ is $\{(i,j) : i,j \in \mathbb{Z}, 1 \leqslant i, 1 \leqslant j \leqslant \mu_i\}$, and the *nodes* of $[\mu]$ are the $(i,j) \in [\mu]$. The i-th *row* of $[\mu]$ consists of those nodes with i in their first coordinate, and the j-th *column* of $[\mu]$ consists of those nodes with j in their second coordinate. Often we omit the brackets and write $[\mu_1, \mu_2, \ldots]$ for $[\mu]$. We visualise Young diagrams by giving each node a box in the plane. For example, here is the Young diagram of $(4,3,1)$:



A *μ-tableau* is the Young diagram $[\mu]$ with an integer between 1 and n placed in each box at a node with no repeats. For example,

1	7	2	4
5	8	6	
3			

is a $(4,3,1)$-tableau. There are $n!$ different μ-tableaux, and S_n acts on them naturally by replacing the number in the box at a node with its image under the permutation. Let t be a μ-tableau. We define the *row stabiliser* of t to be the subgroup of S_n that fixes the rows of t setwise. Then we define an equivalence relation on the set of μ-tableaux by $t_1 \sim t_2$ if and only if $t_1 = t_2\pi$ for some π in the row stabiliser of t_1, and we call the equivalence class $\{t\}$ a *μ-tabloid*. Note that tabloids can be thought of as tableaux with unordered rows. Note also that the natural action of S_n on the set of tabloids is well defined.

For a partition μ of n, we define M_F^μ to be the vector space over F whose basis elements are the μ-tabloids, and the action of S_n on these basis elements is extended linearly to make M_F^μ into an FS_n-module. For a μ-tableau t, the *column stabiliser* C_t is defined to be the subgroup of S_n that fixes the columns of t setwise, and the *polytabloid* $e_t := \{t\} \sum_{\pi \in C_t} (\pi \operatorname{sgn}) \pi$, where $(\pi \operatorname{sgn})$ is the sign of $\pi \in S_n$. The *Specht module* S_F^μ is then defined to be the FS_n-submodule of M_F^μ spanned by the set of polytabloids. If F has infinite characteristic, then the S_F^μ afford a complete list of non-isomorphic irreducible FS_n-modules as μ ranges over the set of partitions of n. However, if F has finite characteristic, then S_F^μ is not necessarily irreducible.

Let $<,>$ denote the unique bilinear form on M_F^μ for which $< \{t_1\}, \{t_2\} >$ is 1 if $\{t_1\} = \{t_2\}$ and 0 otherwise. Then $<,>$ is a symmetric, S_n-invariant, non-singular

bilinear form. In particular, the orthogonal complement $S_F^{\mu\perp}$ is an FS_n-submodule of M^μ. Then we denote the quotient $S_F^\mu / S_F^\mu \cap S_F^{\mu\perp}$ by D_F^μ. Note that we omit the subscript F and write M^μ, S^μ, or D^μ if the context permits.

It turns out that the FS_n-module D_F^μ is either zero or irreducible [40, Theorem 4.8], and also that D_F^μ is non-zero precisely when μ is p-regular [40, Theorem 11.1]. In fact, for a field extension E of F, the ES_n-modules $D_F^\mu \otimes_F E$ and D_E^μ are isomorphic, and so the FS_n-module D_F^μ is absolutely irreducible when μ is p-regular [40, Theorem 4.9]. Consequently, we have the following result, which is [40, Theorem 11.5].

Theorem 8.1.1 ([40])**.** *Let F be a field. The D_F^μ afford a complete list of non-isomorphic irreducible FS_n-modules as μ ranges over the* $\mathrm{char}(F)$*-regular partitions of n.*

An important case of this theorem is when $\mathrm{char}(F) > n$. Certainly every partition of n is then $\mathrm{char}(F)$-regular. In addition, the Specht module S_F^μ is irreducible for every partition μ of n [40, Theorem 23.5]. Hence $\dim_F(D_F^\mu) = \dim_F(S_F^\mu)$ for every partition μ, and the S_F^μ afford a complete list of non-isomorphic irreducible FS_n-modules as μ ranges over the partitions of n. We will make much use of these two observations.

The proof of Theorem 8.1.1 in [40, Theorem 11.5] shows that every field is a splitting field for S_n. However, this is not the case for A_n. Indeed, there exist primes p for which the finite field $\mathbb{F}_p$ is not a splitting field for A_n. Fortunately, we can say the following.

Lemma 8.1.2 ([40, 60])**.** *Let F be a field of prime characteristic p. Then F is a splitting field for S_n. If F contains $\mathbb{F}_{p^2}$, then F is a splitting field for A_n.*

Proof. Any field is a splitting field for S_n by [40, Theorem 11.5]. In particular, $\mathbb{F}_p$ is a splitting field for S_n, and A_n has index 2 in S_n, so $\mathbb{F}_{p^2}$ is a splitting field for A_n by [60]. The general statement about F then follows from Lemma 7.4.3(i). □

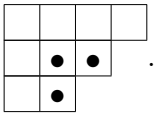
Lemma 8.1.2 has several important consequences. First, it implies that every irreducible $\mathbb{F}_pS_n$-module is absolutely irreducible. In particular, the dimensions of the irreducible $\mathbb{F}_pS_n$-modules are listed in the p-Brauer character table of S_n. In addition, every irreducible FS_n-module can be realised over $\mathbb{F}_p$ by Lemma 7.4.3(i). Similar statements hold for A_n over the splitting field $\mathbb{F}_{p^2}$.

Recall that for a p-regular partition μ of n, we denote by $m(\mu)$ the partition of n for which $D^{m(\mu)} \simeq D^\mu \otimes_F \mathrm{sgn}$. If $p = 2$, then it is always the case that $m(\mu) = \mu$, and if p is odd, then there is a combinatorial description for $m(\mu)$. This description is well known when $p = \infty$ or $p > n$ [40, Theorems 4.9 and 8.15], and the proof of the conjectured description for arbitrary fields was recently completed [27]. However, it happens to be

the case that whenever we need to compute $m(\mu)$, the corresponding n is small enough that we can use decomposition tables or Brauer character tables and GAP [30, 56] to do this, and so we do not give any further description of $m(\mu)$ here.

We wish to use the bounds of Section 6.3 to prove that S_n has regular orbits on most irreducible $\mathbb{F}_p S_n$-modules. Thus we need to know something about the dimension of D^μ. Certainly this dimension is bounded above by that of the Specht module S^μ, so we start by considering the dimension of S^μ. It turns out that this dimension is not only independent of the field but also easily computed.

Let μ be a partition of n. The *(i,j)-hook* of $[\mu]$ consists of the node (i, j), the nodes to the right of (i, j) in $[\mu]$, and the nodes below (i, j) in $[\mu]$. For example, the nodes of the $(2, 2)$-hook of $[4, 3, 2]$ are those containing bullets in the following diagram:



The *hook length* of the (i, j)-hook is defined to be the number of nodes in the hook, and the *hook graph* of μ is the Young diagram $[\mu]$ with each node $(i, j) \in [\mu]$ replaced with its hook length. For example, the hook graph of $(4, 3, 2)$ is

6	5	3	1
4	3	1	
2	1		

.

Then we have the following remarkable formula [40, Theorem 20.1], which is originally due to Frame, Robinson and Thrall:

$$\dim_F(S^\mu) = \frac{n!}{\prod(\text{hook lengths in } [\mu])}.$$

This formula is called the *hook formula*. For example, $\dim_F(S^{(4,3,2)}) = 9!/(3 \cdot 6!) = 168$.

Thus we can easily compute the dimension of S^μ using the hook formula. More generally, the dimension of D^μ can be computed by determining the rank of the Gram matrix with respect to a basis of S^μ, where the *Gram matrix* of S^μ with respect to the basis $s_1, \ldots, s_k$ of S^μ is the matrix whose (i, j)-th entry is $< s_i, s_j >$. However, there is no known simple formula that computes this rank, and although the hook formula provides an upper bound, this upper bound is normally too large to be of any use. Moreover, we are more in need of lower bounds on the dimension of D^μ for the regular orbit problem. Fortunately, James [41] provides some useful methods for determining such bounds.

For each non-negative integer m, as in James [41], we write $R_n(m)$ for the class of irreducible FS_n-modules V for which there exists some p-regular partition μ of n such

that $\mu_1 \geqslant n-m$, and $V \simeq D^\mu$ or $V \simeq D^\mu \otimes_F \mathrm{sgn}$. Then James [41] proves various results with conclusions stating that either $V \in R_n(m)$ or $\dim_F(V)$ is bounded below by some function of n. In fact, [41, Lemma 4] and [41, Appendix Table 1] allow us to construct our own functions, which we do in Lemma 8.2.1 with $m = 2$. Accordingly, the proof of Theorem 8.0.1 divides into two cases. In Section 8.2 we will be primarily concerned with modules that are not in $R_n(2)$, and in Section 8.3 we will be concerned with modules that are in $R_n(2)$, where most of the bounds of Section 6.3 are not applicable.

We will often make use of the known Brauer character tables of the symmetric and alternating groups. The Brauer Atlas [44] contains the p-Brauer character tables of S_n and A_n for $n \leqslant 12$ and $p \leqslant n$, while GAP [30] contains the p-Brauer character tables of S_n and A_n for $n \leqslant 17$ and $p \leqslant n$, as well as $n = 19$ when $p = 2$. Moreover, the GAP package SpinSym [56] also contains the tables of S_n and A_n for $n = 18$ and $p = 2, 3, 5$. If $p > n$, then the p-Brauer character tables of S_n and A_n are the same as the ordinary character tables [39, Theorem 15.13], so they can be found in the Atlas [20] for $n \leqslant 13$ and in GAP [30] for larger n.

8.2 Modules not in $R_n(2)$

The following lemma is the key tool for modules not in $R_n(2)$. It relies significantly on James [41].

Lemma 8.2.1. *Let F be a field of prime characteristic p. Let $f(n) := (n^3 - 9n^2 + 14n - 6)/6$. Let $f_2(n)$ be defined by $f_2(15) = f_2(16) = 127$, $f_2(17) = f_2(18) = 253$, $f_2(19) = f_2(20) = 505$, $f_2(21) = f_2(22) = 930$, and $f_2(n) = f(n)$ for $n \geqslant 23$. If p is odd, let $f_p(n)$ be defined by $f_p(11) = 54$, $f_p(12) = 88$, $f_p(13) = 107$, $f_p(14) = 175$, $f_p(15) = 213$ and $f_p(n) = f(n)$ for $n \geqslant 16$. Let V be an irreducible FS_n-module where $n \geqslant 15$ when $p = 2$ and $n \geqslant 11$ when p is odd. Then $V \in R_n(2)$ or $\dim_F(V) > f_p(n)$.*

Proof. Suppose that there is a function $g : \mathbb{N} \to \mathbb{R}$ and a positive integer N for which

(i) $2g(n) > g(n+2)$ for all $n \geqslant N$,

(ii) If n is N or $N+1$, every irreducible FS_n-module U is in $R_n(2)$ or $\dim_F(U) > g(n)$,

(iii) For all $n \geqslant N$, if $U \in R_n(4) \setminus R_n(2)$, then $\dim_F(U) > g(n)$.

Then James [41, Lemma 4] implies that for all $n \geqslant N$, either $V \in R_n(2)$ or $\dim_F(V) > g(n)$. Thus it suffices to show that $f_p(n)$ satisfies conditions (i)-(iii) with $N = 15$ when $p = 2$ and $N = 11$ otherwise. Note that $2f_2(n) > f_2(n+2)$ for all $n \geqslant 15$, and if p is odd, then $2f_p(n) > f_p(n+2)$ for all $n \geqslant 11$. Moreover, using the lower bounds in James [41, Appendix Table 1], it is routine to verify that if $U \in R_n(4) \setminus R_n(2)$ and $n \geqslant 11$, then

$\dim_F(U) > f(n)$ unless U is $D^{(7,4)}$ or its associate, in which case $\dim_F(U) \geqslant 55 > f_p(11)$ for all odd p. Since $f(n) \geqslant f_p(n)$ for all p and $n \geqslant 11$, it remains to check condition (ii).

Let U be an irreducible FS_n-module, and suppose that U is not in $R_n(2)$. To begin, suppose that $p = 2$. If $n = 15$ or $n = 16$, then $\dim_F(U) > (n-1)(n-2)/2$ by [41, Theorem 7] since $U \notin R_n(2)$. Using the 2-Brauer character table of S_n [30], we can check that $\dim_F(U) \geqslant 128 > f_2(n)$. Thus condition (ii) holds with $N = 15$. Now suppose that p is an odd prime and $n = 11$ or $n = 12$. First assume that $p \leqslant n$. Since $\dim_F(U) > (n-1)(n-2)/2$ by [41, Theorem 7], the Brauer Atlas [44] implies that $\dim_F(U) \geqslant 55$ when $n = 11$ and $\dim_F(U) \geqslant 89$ when $n = 12$. Thus $\dim_F(U) > f_p(n)$, as desired. Assume instead that $p > n$. Then $U \simeq S^\mu$ for some partition μ of n. The dimensions of the Specht modules are listed in the decomposition matrices in James [40, Appendix], and we see that it is still the case that $\dim_F(U) \geqslant 55$ when $n = 11$ and $\dim_F(U) \geqslant 89$ when $n = 12$. Thus condition (ii) is indeed true with $N = 11$. □

Note that the dimension of $D^{(n-3,3)}$ over any field of prime characteristic is precisely $f(n)+1$ for infinitely many n by James [41, Appendix Table 1], so Lemma 8.2.1 provides a tight lower bound on $\dim_F(V)$ for $V \notin R_n(2)$.

Now we are in a position to determine the regular orbits of S_n on modules not in $R_n(2)$. We also prove some results for modules in $R_n(2) \setminus R_n(1)$ when n is small, as the inclusion of these cases simplifies the proof.

Proposition 8.2.2. *Let V be a faithful irreducible $\mathbb{F}_pS_n$-module where $n \geqslant 7$ and p is prime. Let μ be the p-regular partition for which $V \simeq D^\mu$.*

(i) Suppose that $D^\mu \notin R_n(2)$. Then S_n has no regular orbits on V if and only if $p = 2$ and $\mu = (\lfloor n/2 \rfloor + 1, \lfloor (n-1)/2 \rfloor)$ for $7 \leqslant n \leqslant 10$ or $n = 12$.

(ii) Suppose that $D^\mu \in R_n(2) \setminus R_n(1)$ where either $n \leqslant 11$, or $12 \leqslant n \leqslant 14$ and $p = 2$. Then S_n has no regular orbits on V if and only if $p = 2$ and $\mu = (n-2, 2)$ for $7 \leqslant n \leqslant 8$.

Proof. We will prove (i) and (ii) simultaneously. Therefore, we will assume throughout this proof that either $V \notin R_n(2)$, or $V \in R_n(2) \setminus R_n(1)$ where either $n \leqslant 11$, or $12 \leqslant n \leqslant 14$ and $p = 2$. In particular, it is always the case that $V \notin R_n(1)$.

We remark that for small n, Magma [8] will often be used to construct irreducible representations of S_n over $\mathbb{F}_p$ in order to determine whether they admit regular orbits. When p is odd, this can be done for all irreducible representations using the command `IrreducibleModules`, and when $p = 2$, this can be done for particular representations by finding the composition factors of permutation modules of S_n acting on subgroups of the form $S_{n_1} \times S_{n_2} \times \cdots \times S_{n_r}$ where $\sum_{i=1}^r n_i = n$.

Suppose that S_n does not have a regular orbit on V. Then equation (3) of Lemma 6.3.7 implies that $\dim_{\mathbb{F}_p}(V) \leqslant (n/2)\log_p(2n!)$. In particular, $\dim_{\mathbb{F}_p}(V) \leqslant n^3$, so there are only finitely many n for which $V \notin R_n(3)$ by James [41, Theorem 5]. Motivated by classifying these exceptional modules, Müller [62] has completely determined the dimensions of the irreducible $\mathbb{F}_pS_n$-modules of dimension at most n^3 for $p \in \{2,3,5\}$ and $n \leqslant 37$, including the corresponding partitions; we will use this information when character tables are not available. For this proof, define $g(p,n) := (n/2)\log_p(2n!)$. Note that if n is fixed, then $g(p,n)$ is a decreasing function in p.

First of all, suppose that $V \notin R_n(2)$. Recalling the function $f_p(n)$ that was defined in Lemma 8.2.1, it follows from this lemma that $f_p(n) < \dim_{\mathbb{F}_p}(V)$ if either $n \geqslant 15$ when $p = 2$, or $n \geqslant 11$ when p is odd. If $p = 2$ and $n \geqslant 21$, then it is easily checked that $g(2,n) \leqslant f_2(n)$, a contradiction. Similarly, if p is odd and $n \geqslant 14$, then $g(p,n) \leqslant g(3,n) \leqslant f_p(n)$, and if $p \geqslant 5$ and $12 \leqslant n \leqslant 13$, then $g(p,n) \leqslant g(5,n) \leqslant f_p(n)$, both contradictions. Moreover, if $p = 3$ and $n = 12$ or $n = 13$, then $\dim_{\mathbb{F}_3}(V)$ is at least 120 or 143 respectively by the decomposition matrices in [40, Appendix], but $\dim_{\mathbb{F}_3}(V) \leqslant \lfloor g(3,n) \rfloor$, which is 112 or 137, a contradiction. Thus $n \leqslant 20$ when $p = 2$, and $n \leqslant 11$ when p is odd.

Now we analyse the various possibilities for p and n when $V \notin R_n(1)$. To begin, suppose that $p > n$. Then $p \geqslant 11$, so $n \leqslant 11$. Recall that $\dim_{\mathbb{F}_p}(V) = \dim_{\mathbb{F}_p}(S^\mu)$. The dimensions of all Specht modules are listed in the decomposition matrices in James [40, Appendix], so we determine that if n is 7, 9, 10 or 11, then $\dim_{\mathbb{F}_p}(V)$ is at least 14, 27, 35 or 44 respectively. But $\dim_{\mathbb{F}_p}(V) \leqslant \lfloor g(11,n) \rfloor$, and this is 13, 25, 32 or 41 respectively, a contradiction. Thus $n = 8$. Then $\dim_{\mathbb{F}_p}(V) \leqslant \lfloor g(11,n) \rfloor = 18$, so $\dim_{\mathbb{F}_p}(V) = 14$ and there are two such modules. If $p \geqslant 29$, then $\dim_{\mathbb{F}_p}(V) \leqslant \lfloor g(29,n) \rfloor = 13$, a contradiction, so p is 11, 13, 17, 19, or 23. Then we use Magma [8] to verify that V fails the bound of Lemma 6.3.3, and so S_n has a regular orbit on V, a contradiction.

Hence $p \leqslant n$. Suppose that $p = 2$ and $15 \leqslant n \leqslant 20$. Then $V \notin R_n(2)$ by assumption, so $f_2(n) < \dim_{\mathbb{F}_2}(V)$ by Lemma 8.2.1, while $\dim_{\mathbb{F}_2}(V) \leqslant \lfloor g(2,n) \rfloor$. Using Müller [62] when $n = 20$ and GAP [30, 56] otherwise, we determine that the dimension of V must be as listed in Table 8.2 and also that there is a unique irreducible representation for each listed dimension. Now suppose that $n \leqslant 14$ when $p = 2$, and recall that $n \leqslant 11$ when p is odd. Note that if U is an irreducible $\mathbb{F}_pS_n$-module and $U \in R_n(1)$, then $\dim_{\mathbb{F}_p}(U)$ is either 1, $n-2$ when $p \mid n$, or $n-1$ when $p \nmid n$ by [41, Appendix Table 1]. Using this information and [30, 44], we can determine the possible dimensions for V such that $V \notin R_n(1)$ and $\dim_{\mathbb{F}_p}(V) \leqslant \lfloor g(p,n) \rfloor$. We list these in Tables 8.2 and 8.3 when p is even and odd respectively. Also, if d is a dimension listed in Table 8.2 or 8.3 with a subscript

c, then we mean that there are c irreducible representations of dimension d, and if d has no subscript, then we mean that there is only one irreducible representation of dimension d. The meaning of the other symbols in these tables will shortly be made clear.

n	$\lfloor g(2,n) \rfloor$	$\dim_{\mathbb{F}_2}(D^\mu)$
7	46	$8^\times$, $14^\times$, 20
8	65	$8^\times$, $14^\times$, 40, 64
9	87	$16^\times$, 26^{**}, 40, 48†, 78
10	113	$16^\times$, 26^{**}, 48
11	144	32^*, 44†, 100†, 144
12	179	$32^\times$, 44^{***}, 100, 164
13	217	${}_2 64$, 208†
14	261	${}_2 64$, 208
15	309	128†
16	362	128, 336
17	419	256†
18	481	256
19	548	512†
20	620	512

Table 8.2: Possible dimensions for D^μ when $p = 2$.

n	p	$\lfloor g(p,n) \rfloor$	$\dim_{\mathbb{F}_p}(D^\mu)$
7	3	29	13^{**}, 13, ${}_2 15$, 20
	5	20	${}_2 8^{**}$, ${}_2 13$, ${}_2 15$, 20
	7	16	${}_2 10$, ${}_4 14$
8	3	41	${}_2 13^{**}$, ${}_2 21$, ${}_2 28$, ${}_2 35$
	5	28	13^*, 13, ${}_2 20$, ${}_4 21$
	7	23	${}_2 14$, ${}_2 19$, ${}_2 21$
9	3	55	${}_2 21$, ${}_2 27$, ${}_2 35$, ${}_2 41$
	5	37	${}_2 21$, ${}_2 27$, ${}_2 28$, ${}_2 34$
	7	31	${}_2 19$, ${}_2 28$
10	3	71	${}_2 34$, ${}_2 36$, ${}_2 41$
	5	49	${}_2 28$, ${}_2 34$, ${}_2 35$
	7	40	${}_2 35$, ${}_2 36$
11	3	91	${}_2 34$, ${}_2 45$
	5	62	${}_2 43$, ${}_2 45$, ${}_2 55$
	7	51	${}_2 44$, ${}_2 45$
	11	41	${}_2 36$

Table 8.3: Possible dimensions for D^μ when p is odd and $p \leqslant n$.

Hence $\dim_{\mathbb{F}_p}(V)$ is listed in Table 8.2 or 8.3. If $\dim_{\mathbb{F}_p}(V)$ has no *, **, ***, † or $^\times$ next to it, then we use Magma [8] to verify that V fails the bound of Lemma 6.3.3, and so S_n has a regular orbit on V, a contradiction. If $\dim_{\mathbb{F}_p}(V)$ has * next to it, then we can find a regular orbit of S_n on V by randomly selecting vectors using Magma, and if $\dim_{\mathbb{F}_p}(V)$ has ** next to it, then we can find a regular orbit of S_n on V by exhaustively searching the vectors in V using Magma. Thus $p = 2$. If $\dim_{\mathbb{F}_p}(V)$ has *** next to it, then $n = 12$ and $\dim_{\mathbb{F}_2}(V) = 44$. For this case, we use Magma to find an orbit of S_n on V containing more than 249,995,355 points, and since this is greater than $n!/2$, this orbit must be regular.

Next, suppose that $\dim_{\mathbb{F}_p}(V)$ has † next to it. Let D^λ be the $\mathbb{F}_2 S_{n+1}$-module whose dimension is $\dim_{\mathbb{F}_2}(V)$, which exists by Table 8.2. We claim that $D^\mu \simeq D^\lambda \downarrow S_n$, in which case S_n has a regular orbit on V. Using [62] for λ when $n = 19$ and [30, 56] otherwise, we determine that the partitions μ and λ are either $(\lfloor n/2 \rfloor + 1, \lfloor (n-1)/2 \rfloor)$ and $(\lfloor n/2 \rfloor + 2, \lfloor (n-1)/2 \rfloor)$ respectively for $n \in \{15, 17, 19\}$, or $(n-3, 3)$ and $(n-2, 3)$ respectively for $n \in \{9, 11, 13\}$ unless $n = 11$ and $\dim_{\mathbb{F}_2}(D^\mu) = 44$, in which case they are $(9, 2)$ and $(10, 2)$ respectively. Thus μ and λ have the form $(n-m, m)$ and $(n-m+1, m)$ respectively for some integer m. Then S^μ is a bottom factor in a series of $S^\lambda \downarrow S_n$ by [40, Theorem 9.3], so there exists an $\mathbb{F}_2 S_n$-homomorphism $\varphi : S^\mu \to D^\lambda$ for which $\ker(\varphi) = S^\mu \cap S^\lambda \cap S^{\lambda\perp} \subseteq S^\mu \cap S^{\mu\perp}$. Thus D^μ is a composition factor of $S^\mu / \ker(\varphi)$, but D^μ and D^λ have the same dimension, so $D^\mu \simeq D^\lambda \downarrow S_n$, as desired.

Finally, suppose that $\dim_{\mathbb{F}_p}(V)$ has $^\times$ next to it. Using the decomposition matrices in [40], we determine that μ is either $(\lfloor n/2 \rfloor + 1, \lfloor (n-1)/2 \rfloor)$ when $\dim_{\mathbb{F}_2}(D^\mu) = 2^{\lfloor (n-1)/2 \rfloor}$ for $7 \leqslant n \leqslant 10$ or $n = 12$, or $(n-2, 2)$ when $\dim_{\mathbb{F}_2}(D^\mu) = 14$ for $7 \leqslant n \leqslant 8$, as desired.

Conversely, suppose that $p = 2$ and μ is either the partition $(n-2, 2)$ for $7 \leqslant n \leqslant 8$, or the partition $(\lfloor n/2 \rfloor + 1, \lfloor (n-1)/2 \rfloor)$ for $7 \leqslant n \leqslant 10$ or $n = 12$. Recall that V has dimension 14 if $\mu = (n-2, 2)$ and dimension $2^{\lfloor (n-1)/2 \rfloor}$ if $\mu = (\lfloor n/2 \rfloor + 1, \lfloor (n-1)/2 \rfloor)$. Note that if S_n does have a regular orbit on V, then V contains an orbit of length $n!$. Thus S_n has no regular orbits on V when $|V| < n!$. In this way, we see that S_n has no regular orbits on V when either $\mu = (6, 2)$, or $\mu = (\lfloor n/2 \rfloor + 1, \lfloor (n-1)/2 \rfloor)$ for $7 \leqslant n \leqslant 10$. Moreover, if $\mu = (5, 2)$, then we use Magma [8] to check that every orbit is too small to be regular. Lastly, if $\mu = (7, 5)$, then we use Magma to prove that S_n has no regular orbits on V by enumerating enough points in non-regular orbits so that fewer than $n!$ points remain. This required finding 45 orbits consisting of a total of 3,854,632,320 points. □

Now we use Lemma 8.2.1 and Proposition 8.2.2 to determine the regular orbits of the alternating group.

Proposition 8.2.3. *Let V be a faithful irreducible $\mathbb{F}_pA_n$-module where $n \geqslant 7$ and p is prime. Let μ be a p-regular partition of n for which $V \leqslant D^\mu \downarrow A_n$, and suppose that $D^\mu \notin R_n(2)$.*

(i) If $V \not\simeq D^\mu \downarrow A_n$, then A_n has no regular orbits on V if and only if $p = 2$ and μ is $(5,3,1)$ or $(\lfloor n/2 \rfloor + 1, \lfloor (n-1)/2 \rfloor)$ for $7 \leqslant n \leqslant 9$.

(ii) If $V \simeq D^\mu \downarrow A_n$, then A_n has no regular orbits on V if and only if $p = 2$ and $\mu = (6,4)$.

Proof. (i) Since $V \not\simeq D^\mu \downarrow A_n$, Lemma 7.5.2 implies that $D^\mu \downarrow A_n \simeq V \oplus Vg$ for any $g \in S_n \setminus A_n$. Note that A_n has a regular orbit on V if and only if A_n has a regular orbit on Vg. Also, since $D^\mu \downarrow A_n$ splits and $D^\mu_{\mathbb{F}_{p^2}} \simeq D^\mu_{\mathbb{F}_p} \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}$, it follows that $D^\mu_{\mathbb{F}_{p^2}} \downarrow A_n$ splits. Recall that $\mathbb{F}_{p^2}$ is a splitting field for A_n by Lemma 8.1.2, and let λ be any p-regular partition of n. Then for p odd, Lemma 7.6.7 implies that $D^\lambda_{\mathbb{F}_{p^2}} \downarrow A_n$ splits if and only if the Brauer character of $D^\lambda_{\mathbb{F}_{p^2}}$ vanishes for every p-regular element in $S_n \setminus A_n$. Moreover, Lemma 7.5.3 implies that $D^\lambda_{\mathbb{F}_{p^2}} \downarrow A_n$ splits if and only if $m(\lambda) = \lambda$. For the case where $p = 2$, we can determine whether $D^\lambda_{\mathbb{F}_4} \downarrow A_n$ splits by comparing dimensions in the 2-Brauer character tables of S_n and A_n. We will use these facts and observations throughout the proof.

As in the symmetric case, Magma [8] will often be used to construct irreducible representations of A_n over $\mathbb{F}_p$. In fact, these representations normally already exist in the database of Atlas groups and can be accessed by the command `MatRepKeys`; otherwise, we can use the methods described in the proof of Proposition 8.2.2.

Suppose that A_n does not have a regular orbit on V. Then Lemma 6.3.6 implies that $\dim_{\mathbb{F}_p}(V) \leqslant r(A_n)\log_p(n!/2)$. Since $r(A_n) \leqslant n/2$ by Guralnick and Saxl [35, Lemma 6.1], and since $\dim_{\mathbb{F}_p}(V) = \dim_{\mathbb{F}_p}(D^\mu)/2$, we obtain that $\dim_{\mathbb{F}_p}(D^\mu) \leqslant n\log_p(n!/2)$. For this proof, let $g(p,n) := n\log_p(n!/2)$. Note that if n is fixed, then $g(p,n)$ is a decreasing function in p. Note also that $g(p,n) \leqslant n^3$, and so Müller [62] applies for $p \in \{2,3,5\}$ and $n \leqslant 37$ as in the proof of Proposition 8.2.2. Recall the function $f_p(n)$ that was defined in Lemma 8.2.1. Then since $D^\mu \notin R_n(2)$ by assumption, Lemma 8.2.1 implies that $f_p(n) < \dim_{\mathbb{F}_p}(D^\mu)$ if either $n \geqslant 15$ when $p = 2$, or $n \geqslant 11$ when p is odd.

First we claim that either $p = 2$ and $n \leqslant 19$, or $3 \leqslant p \leqslant 13$ and $n \leqslant 10$, or $p \geqslant 17$ and $n \leqslant 11$. If either $p = 2$ and $n \geqslant 30$, or $p = 3$ and $n \geqslant 20$, or $p = 5$ and $n \geqslant 16$, or $p = 7$ and $n \geqslant 15$, or $p = 11$ or 13 and $n \geqslant 14$, or $p = 17$ and $n \geqslant 12$, then $g(p,n) \leqslant f_p(n)$, a contradiction. Thus we also have a contradiction if $p \geqslant 19$ and $n \geqslant 12$, and we conclude that the claim is proved for $p \geqslant 17$. Moreover, if $p = 2$ and $20 \leqslant n \leqslant 29$, then since $D^\mu_{\mathbb{F}_{p^2}} \downarrow A_n$ splits and $\dim_{\mathbb{F}_2}(D^\mu)$ is bounded below by $f_2(n)$ and above by $g(2,n)$, we

obtain from Müller [62] that μ is $(\lfloor n/2 \rfloor + 1, \lfloor (n-1)/2 \rfloor)$ where $n = 20$ or $n = 21$. But then n is congruent to 4 or 5 mod 8, so [5, Theorem 6.1] implies that $D^\mu \downarrow A_n$ splits only after an extension to $\mathbb{F}_4$, a contradiction. Thus the claim holds for $p = 2$. Lastly, if either $p = 3$ and $11 \leqslant n \leqslant 19$, or $p = 5$ and $11 \leqslant n \leqslant 15$, or $p = 7$ and $11 \leqslant n \leqslant 14$, or $p = 11$ or 13 and $11 \leqslant n \leqslant 13$, then using Müller [62] when $p = 3$ and $n = 19$ and GAP [30] otherwise, we ascertain there is no μ for which $D^\mu_{\mathbb{F}_{p^2}} \downarrow A_n$ splits and $\dim_{\mathbb{F}_p}(D^\mu)$ is bounded below by $f_p(n)$ and above by $g(p, n)$. This establishes the claim.

Therefore, either $p = 2$ and $n \leqslant 19$, or $3 \leqslant p \leqslant 13$ and $n \leqslant 10$, or $p \geqslant 17$ and $n \leqslant 11$. Using [20, 30, 44, 56], we can determine the possible dimensions for D^μ over $\mathbb{F}_p$ such that $D^\mu_{\mathbb{F}_{p^2}} \downarrow A_n$ splits and $\dim_{\mathbb{F}_p}(D^\mu) \leqslant \lfloor g(p, n) \rfloor$. We list these in Table 8.4, omitting those n and p for which no μ is found. Moreover, for those $\dim_{\mathbb{F}_p}(D^\mu)$ listed in Table 8.4, we determine that $D^\mu \downarrow A_n$ is irreducible if and only if $\dim_{\mathbb{F}_p}(D^\mu)$ is listed with the superscript $^+$. This follows from [20, 30, 44] and Lemma 7.6.6 by applying Lemma 7.6.7 to $D^\mu_{\mathbb{F}_{p^2}} \simeq D^\mu_{\mathbb{F}_p} \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}$.

n	p	$g(p,n)$	$\dim_{\mathbb{F}_p}(D^\mu)$
7	2	79	$8^\times$
	3	49	20^+
	5	34	20^+
	11	22	20
	13	21	20^+
8	2	114	$8^\times$, 40**
9	2	157	$16^\times$, $40^\times$
	7	56	42^+
	11	45	42^+
	13	42	42^+
10	2	207	128
	5	89	70
11	2	266	32^+
12	2	334	32^+, 288^+
13	2	409	64^+, 288^+
15	2	588	128†
16	2	692	128
17	2	804	256
19	2	1059	512^+

Table 8.4: Possible dimensions for D^μ when $V \not\simeq D^\mu \downarrow A_n$.

Hence $\dim_{\mathbb{F}_p}(D^\mu)$ is listed in Table 8.4 with no superscript $^+$. Recall that $\dim_{\mathbb{F}_p}(V) = \dim_{\mathbb{F}_p}(D^\mu)/2$. In addition, there are precisely two irreducible $\mathbb{F}_pA_n$-modules of dimension $\dim_{\mathbb{F}_p}(V)$ for each listed dimension of D^μ except when either $n = 9$ and $\dim_{\mathbb{F}_p}(D^\mu) = 16$, or $n = 10$ and $p = 5$, in which case there are three. When $\dim_{\mathbb{F}_p}(D^\mu)$ has no adjacent **, † or $^\times$ in Table 8.4, we use Magma [8] to verify that V fails the bound of Lemma 6.3.3, a contradiction, and if $\dim_{\mathbb{F}_p}(D^\mu)$ has an adjacent **, then we can find a regular orbit of A_n on V by exhaustively searching the vectors in V using Magma, a contradiction.

Next suppose that $\dim_{\mathbb{F}_p}(D^\mu)$ has † next to it. Then $p = 2$ and $n = 15$. Let D^λ be the $\mathbb{F}_2S_{16}$-module whose dimension is $\dim_{\mathbb{F}_2}(D^\mu)$, which exists by Table 8.4. Using [30, 56], we obtain that $\mu = (8, 7)$, $\lambda = (9, 7)$ and $D^\mu \simeq D^\lambda \downarrow S_{15}$. Let W be an irreducible $\mathbb{F}_2A_{16}$-submodule of D^λ. Then $W \downarrow A_{15}$ is a proper $\mathbb{F}_2A_{15}$-submodule of D^μ, so $W \downarrow A_{15}$ is irreducible by Lemma 7.5.2 and thus isomorphic to V or Vg. We have already determined that A_{16} has a regular orbit on W, so A_{15} has a regular orbit on V.

Thus $\dim_{\mathbb{F}_2}(V)$ has $^\times$ next to it. Using the decomposition matrices in [40], we determine that μ is $(5, 3, 1)$ when $\dim_{\mathbb{F}_2}(D^\mu) = 40$ and $(\lfloor n/2\rfloor + 1, \lfloor (n-1)/2\rfloor)$ when $\dim_{\mathbb{F}_2}(D^\mu) = 2^{\lfloor (n-1)/2\rfloor}$ for $7 \leqslant n \leqslant 9$, as desired.

Conversely, suppose that $p = 2$ and μ is $(5, 3, 1)$ or $(\lfloor n/2\rfloor + 1, \lfloor (n-1)/2\rfloor)$ for $7 \leqslant n \leqslant 9$. Recall that D^μ has dimension 40 if μ is $(5, 3, 1)$ and dimension $2^{\lfloor (n-1)/2\rfloor}$ if μ is $(\lfloor n/2\rfloor + 1, \lfloor (n-1)/2\rfloor)$. Then $D^\mu \downarrow A_n$ genuinely splits as it has no superscript $^+$ in Table 8.4. If $\mu = (\lfloor n/2\rfloor + 1, \lfloor (n-1)/2\rfloor)$ for $7 \leqslant n \leqslant 9$, then $|V| \leqslant 2^8 < |A_n|$, so A_n does not have a regular orbit on V. If $\mu = (5, 3, 1)$, then V has dimension 20, and we use Magma [8] to check that every orbit of A_n on one of the irreducible $\mathbb{F}_2A_n$-modules of dimension 20 is too small to be regular.

(ii) Suppose that A_n has no regular orbits on V. Then S_n has no regular orbits on D^μ, so Proposition 8.2.2 implies that $p = 2$ and $\mu = (\lfloor n/2\rfloor + 1, \lfloor (n-1)/2\rfloor)$ for $7 \leqslant n \leqslant 10$ or $n = 12$. But $D^\mu \downarrow A_n$ is irreducible, and so μ is $(6, 4)$ or $(7, 5)$ by [44] and Lemmas 7.6.6 and 7.6.7. Moreover, if $\mu = (7, 5)$, then $D^\mu \downarrow A_n$ is not absolutely irreducible, so $k := \mathrm{End}_{\mathbb{F}_2A_n}(V) \supsetneq \mathbb{F}_2$. Recall from Section 7.4 that V is an irreducible kN-module. Then Lemma 7.2.4 implies that $V \otimes_{\mathbb{F}_2} k \simeq \oplus_{\gamma\in\Gamma} V_\gamma$ where $\Gamma = \mathrm{Gal}(k/\mathbb{F}_2)$. Since $V \otimes_{\mathbb{F}_2} k = (D^\mu \otimes_{\mathbb{F}_2} k) \downarrow A_n$ and $D^\mu \otimes_{\mathbb{F}_2} k$ is an irreducible kS_n-module, Lemma 7.5.2 forces $|\Gamma| \leqslant 2$. Thus $\mathrm{End}_{\mathbb{F}_2A_n}(V) = \mathbb{F}_4$, and we may view V as an irreducible $\mathbb{F}_4A_n$-module of dimension 16. Since we can find a regular orbit of A_n on both irreducible $\mathbb{F}_4A_n$-modules of dimension 16 by using Magma [8] to do a random search, it follows that A_n has a regular orbit on V as an $\mathbb{F}_2A_n$-module. Thus $\mu = (6, 4)$, in which case A_n does not have a regular orbit on V since $|V| = 2^{16} < |A_{10}|$. □

8.3 Modules in $R_n(2)$

Now we focus on modules in $R_n(2)$. We begin with modules in $R_n(2) \setminus R_n(1)$, and then we deal with modules in $R_n(1)$ at the end of this section. Note that the bounds of Lemma 6.3.7 are not useful in this case since the dimension of a module in $R_n(2)$ is at most n^2. Thus our proofs will instead be constructive.

In the case of modules in $R_n(2) \setminus R_n(1)$, we actually prove a stronger result concerning groups of the form $S_n \times A$ where A is an abelian group. Let F be any field, and let A be a finite subgroup of F^*. If V is an irreducible FS_n-module, then V naturally becomes an irreducible $F(S_n \times A)$-module where A acts by scalar multiplication on V. We will prove the following result about the regular orbits of $S_n \times A$.

Proposition 8.3.1. *Let F be a field, and let V be an FS_n-module in $R_n(2) \setminus R_n(1)$ where $n \geqslant 13$, or $n = 12$ and $|F| \neq 2$. Let A be a finite subgroup of F^*. Then $S_n \times A$ has a regular orbit on V. Moreover, $V \downarrow A_n$ is irreducible and $A_n \times A$ has a regular orbit on V.*

Proposition 8.3.1 extends the work of Hall, Liebeck and Seitz [37, Theorem 6], who found a regular orbit of A_n on modules in $R_n(2) \setminus R_n(1)$ for $n > 30$. Our methods of proof are similar. Note that the claims of Proposition 8.3.1 also hold when $n = 12$ and $|F| = 2$ by Proposition 8.2.2(ii) and Lemma 8.3.2 below; this case will be handled in Section 8.4.

For modules in $R_n(2) \setminus R_n(1)$, we are primarily concerned with the partitions $(n-2, 2)$ and $(n-2, 1^2)$. For these partitions, the modules M^μ and S^μ can be understood using graphs, making them much easier to work with. We assume a familiarity with basic terminology from graph theory throughout this section.

Suppose that $\mu = (n-2, 2)$. Each μ-tabloid is determined by the unordered pair of integers in its second row, so the set of simple undirected graphs on n vertices with edges weighted by field elements is isomorphic to M^μ if we identify each unordered pair $\{i, j\}$ with the edge whose ends are i and j. The Specht module S^μ is spanned by the polytabloids, so with this viewpoint, S^μ is spanned by the alternating 4-cycles, which are graphs of the form $\{i, j\} - \{j, k\} + \{k, l\} - \{l, i\}$ for distinct $i, j, k, l \in \{1, \ldots, n\}$. Now observe that the sum of $\{1, 2\} - \{2, 3\} + \{3, 4\} - \{4, 1\}$ and $\{1, 4\} - \{4, 5\} + \{5, 6\} - \{6, 1\}$ is the alternating 6-cycle $\{1, 2\} - \{2, 3\} + \{3, 4\} - \{4, 5\} + \{5, 6\} - \{6, 1\}$. Continuing in this way, we conclude that S^μ contains every alternating $2m$-cycle for $m \geqslant 2$.

Similarly, if $\mu = (n-2, 1^2)$, then each μ-tabloid is determined by the ordered pair of integers in its second and third rows, so the set of simple directed graphs on n vertices with edges weighted by field elements is isomorphic to M^μ if we identify each ordered pair (i, j) with the edge whose tail is i and head is j. With this viewpoint, the Specht

module S^μ is spanned by the directed 3-cycles, which are graphs of the form $(i,j)-(j,i)+(j,k)-(k,j)+(k,i)-(i,k)$ for distinct $i,j,k \in \{1,\dots,n\}$. Now observe that the sum of $(1,2)-(2,1)+(2,3)-(3,2)+(3,1)-(1,3)$ and $(1,3)-(3,1)+(3,4)-(4,3)+(4,1)-(1,4)$ is the directed 4-cycle $(1,2)-(2,1)+(2,3)-(3,2)+(3,4)-(4,3)+(4,1)-(1,4)$. Continuing in this way, we conclude that S^μ contains every directed m-cycle for $m \geqslant 3$.

We begin by proving that the restriction of a module in $R_n(2) \setminus R_n(1)$ to A_n is indeed irreducible, as claimed in Proposition 8.3.1.

Lemma 8.3.2. *Let F be a field, and suppose that $n \geqslant 7$. If V is an FS_n-module in $R_n(2) \setminus R_n(1)$, then $V \downarrow A_n$ is irreducible.*

Proof. For $n > 30$, this is proved in Step 5 of the proof of [37, Theorem 6]. We reproduce this proof here in order to deal with smaller n. Since the modules in $R_n(2) \setminus R_n(1)$ have the form D^μ or $D^\mu \otimes_F \mathrm{sgn}$ where μ is $(n-2,2)$ or $(n-2,1^2)$, and since $D^\mu \downarrow A_n \simeq D^\mu \otimes_F \mathrm{sgn} \downarrow A_n$, it suffices to assume that $V = D^\mu$ where μ is $(n-2,2)$ or $(n-2,1^2)$.

Suppose for a contradiction that $D^\mu \downarrow A_n$ is not irreducible, and let W be an irreducible FA_n-submodule of D^μ. Then Lemma 7.5.2 implies that $D^\mu = W \oplus Wg$ where $g = (12) \in S_n$. Note that $\dim_F([W,g]) = \dim_F(W) - \dim_F(C_W(g))$ by Lemma 6.3.4. But $C_W(g) = 0$ since $W \cap Wg = 0$, and $(n^2-5n+2)/2 \leqslant \dim_F(D^\mu)$ by [41, Appendix Table 1], so $(n^2-5n+2)/4 \leqslant \dim_F(D^\mu)/2 = \dim_F([W,g])$. Moreover, $\dim_F([W,g]) \leqslant \dim_F([M^\mu,g]) = \dim_F(M^\mu) - \dim_F(C^\mu)$ where $C^\mu := C_{M^\mu}(g)$, and $\dim_F(M^\mu)$ is either $n(n-1)/2$ or $n(n-1)$ when μ is $(n-2,2)$ or $(n-2,1^2)$ respectively. Hence we conclude that $\dim_F(C^{(n-2,2)}) \leqslant (n^2+3n-2)/4$ and $\dim_F(C^{(n-2,1^2)}) \leqslant (3n^2+n-2)/4$.

Now we consider the dimension of C^μ and compare it to the upper bounds above to obtain a contradiction for all but the smallest n. Suppose that $\mu = (n-2,2)$. Then the graphs $\{1,2\}$, $\{i,j\}$ and $\{1,i\}+\{2,i\}$ are fixed by g for all $i,j \notin \{1,2\}$, and these form a linearly independent set in M^μ, so $\dim_F(C^\mu) \geqslant 1 + (n-2)(n-3)/2 + (n-2) = (n^2-3n+4)/2$. But this is impossible unless $n = 7$. Next suppose that $\mu = (n-2,1^2)$. Then the graphs (i,j), $(1,2)+(2,1)$, $(1,i)+(2,i)$, and $(i,1)+(i,2)$ are fixed by g for all $i,j \notin \{1,2\}$, and again these form a linearly independent set, so $\dim_F(C^\mu) \geqslant (n-2)(n-3)+1+(n-2)+(n-2) = n^2-3n+3$. But this is impossible unless $n \leqslant 11$.

Suppose then that either $n = 7$ when $\mu = (n-2,2)$, or $n \leqslant 11$ when $\mu = (n-2,1^2)$. Recall from Lemma 7.5.3 that if $\mathrm{char}(F) \neq 2$ and $m(\mu) \neq \mu$, then $D^\mu \downarrow A_n$ is irreducible. If $2 < \mathrm{char}(F) \leqslant n$, then it is easily checked using [30, 56] that $m(\mu) \neq \mu$ unless $\mathrm{char}(F) = 11$ and $n = 11$, in which case $\mu = (9,1^2)$. Then D^μ has dimension 36 by [41, Appendix Table 1], and so [44] implies that $D^{m(\mu)} \not\simeq D^\mu$. Similarly, if $\mathrm{char}(F) > n$ (including the case where $\mathrm{char}(F) = \infty$), then the dimension of $D^\mu = S^\mu$ can be computed using the

hook formula, and we determine using [20] that $D^{m(\mu)} \not\cong D^\mu$. Lastly, if $\mathrm{char}(F) = 2$, then $\mu = (5,2)$, and so D^μ has dimension 14 by the decomposition matrix of S_7 in [40]. Then it is easily checked using [44] that $D^\mu \downarrow A_n$ is irreducible. □

We will need the following technical result about graphs. Note that K_l denotes the complete graph on l vertices and $K_{l,l'}$ denotes the complete bipartite graph whose vertices are partitioned into sets of size l and l'.

Lemma 8.3.3. *Let $\Gamma = (V, E)$ be a finite simple undirected graph with vertex set V and edge set E. Suppose that $|V| \geqslant 12$ and $1 \leqslant |E| \leqslant 2|V| + 8$, and suppose that the maximal degree of Γ is at most 8. Then either there exist distinct vertices $v_1, v_2, v_3, v_4 \in V$ such that the edge $\{v_1, v_2\} \in E$ but the edges $\{v_2, v_3\}, \{v_3, v_4\}, \{v_4, v_1\} \notin E$, or $|V| = 12$ and Γ is one of the following exceptions: $K_{4,8}$, $K_6 \cup K_6$ or $K_5 \cup K_7$.*

Proof. Let a be a vertex in V with minimal non-zero degree in Γ. Note that if Γ contains a vertex c of degree 0, then since $|V| \geqslant 12$ and $\deg a \leqslant 8$, there exists a vertex $d \neq a, c$ that is not adjacent to a, and so taking v_2 to be a vertex adjacent to a and letting $v_1 = a$, $v_3 = c$ and $v_4 = d$, we are done. Thus we may assume that every vertex has non-zero degree. In particular, since $2|E| = \sum_{v \in V} \deg v$ by the handshake lemma, it follows that $2|E| \geqslant |V| \deg a$. Thus $\deg a \leqslant 5$, or else $6|V| \leqslant 2|E| \leqslant 2(2|V| + 8)$, and so $|V| \leqslant 8$, a contradiction.

Let b be a vertex that is not adjacent to the vertex a of maximal degree. Let A be the set of vertices adjacent to a, B the set of vertices adjacent to b, A' the subset of A whose vertices are not adjacent to b, B' the subset of B whose vertices are not adjacent to a, and C the set of vertices in V that are not in A, B or $\{a, b\}$.

Suppose first of all that C is non-empty. If A' is non-empty, then let $v_1 = a$, $v_3 = b$ and choose $v_2 \in A'$ and $v_4 \in C$. By the symmetry of this argument, we may assume that $A = B$. Then $\deg a = \deg b$, but a has minimal degree and b has maximal degree among the vertices not adjacent to a, so every vertex of C has the same degree as a and b. Note that if there is an edge whose ends are both in C, then we may take $v_3 = b$, $v_4 = a$, and v_1 and v_2 to be the ends of this edge. Otherwise, every vertex of C is adjacent to every vertex of A. Then any vertex of A has degree at least $|C| + 2$, so $|C| \leqslant 6$, but $\deg a \leqslant 5$, so $|V| = 2 + \deg a + |C| \leqslant 13$. If $|V| = 13$, then it follows that Γ must contain a subgraph isomorphic to $K_{5,8}$, but $K_{5,8}$ has 40 edges, so Γ has at least 40 edges, contradicting our assumption that $|E| \leqslant 34$. Similarly, if $|V| = 12$, then Γ must contain a subgraph isomorphic to $K_{5,7}$ or $K_{4,8}$, but $K_{5,7}$ has 35 edges, $K_{4,8}$ has 32 edges, and $|E| \leqslant 32$, so Γ must in fact be $K_{4,8}$.

Thus we may assume that C is empty. Note that $|B'| = |V| - \deg a - 2 \geqslant 12 - 5 - 2 = 5$. Then $|A \cap B| \leqslant 3$, so $|A'| + |B'| = |V| - |A \cap B| - 2 \geqslant 12 - 3 - 2 = 7$. Then the set A' is non-empty since a has non-zero degree, b has degree at most 8 and $|V| \geqslant 12$. If there is an edge that has one end in A' and the other in B', then we may take these ends to be v_1 and v_2 respectively along with $v_3 = a$ and $v_4 = b$, so we assume that there is no such edge. Suppose further that there exists $d \in A \cap B$. Then d cannot be adjacent to every vertex of A' and B' or else it will have degree at least 9. If d is not adjacent to some vertex of A', then we take $v_1 = a$, $v_2 = d$, v_3 to be a vertex of A' not adjacent to d, and $v_4 \in B'$. Thus by symmetry we may assume that $A \cap B$ is empty, so that Γ consists of exactly two connected components. If the component containing the vertices of A' is not a complete graph, then we may choose distinct vertices v_1 and v_4 from A' that do not have an edge between them and take $v_2 = a$ and $v_3 = b$. By symmetry, we may therefore assume that one component of Γ is a complete graph on $|A'| + 1$ vertices, while the other is a complete graph on $|B'| + 1$ vertices. Note that a complete graph on n vertices has $n(n-1)/2$ edges. Recall that $|A'| \leqslant 5$ and $|B'| \leqslant 8$. Then $|V| = |A'| + |B'| + 2 \leqslant 15$, and so the initial assumptions on $|V|$ and $|E|$ force $|V| = 12$, which in turn forces Γ to be the graph whose components are either K_6 and K_6, or K_5 and K_7. □

For $s \in S^\mu$, the *underlying graph* of s is defined to be either the graph s with weights removed when $\mu = (n-2, 2)$, or the graph s with weights, direction and multiple edges removed when $\mu = (n-2, 1^2)$. Thus the underlying graph of $s \in S^\mu$ is always a finite simple undirected graph.

Lemma 8.3.4. *Let μ be $(n-2, 2)$ or $(n-2, 1^2)$, and suppose that $n \geqslant 12$. Let F be a field for which μ is* $\mathrm{char}(F)$*-regular, and let A be a finite subgroup of F^*. If there exists $s \in S^\mu$ whose underlying graph has maximal degree at most 4, a trivial automorphism group, and at most $n+4$ edges when $n \geqslant 13$ or 14 edges when $n = 12$, then $S_n \times A$ has a regular orbit on D^μ and $D^\mu \otimes_F \mathrm{sgn}$.*

Proof. We claim it suffices to prove that $s - \lambda sg \notin S^{\mu\perp}$ for all $1 \neq g \in S_n$ and $\lambda \in F^*$. Suppose that this occurs. Then $s \notin S^{\mu\perp}$ since $S^{\mu\perp}$ is an FS_n-submodule of M^μ. If $(s + S^\mu \cap S^{\mu\perp})g\lambda = s + S^\mu \cap S^{\mu\perp}$ for some $g \in S_n$ and $\lambda \in A$, then $s - \lambda sg \in S^{\mu\perp}$, so $g = 1$ by assumption. But $s \notin S^{\mu\perp}$, so $\lambda = 1$. Hence $S_n \times A$ has a regular orbit on D^μ. Moreover, if $(s + S^\mu \cap S^{\mu\perp} \otimes 1)g\lambda = s + S^\mu \cap S^{\mu\perp} \otimes 1$ for some $g \in S_n$ and $\lambda \in A$, then either $g \in A_n$ and $s - \lambda sg \in S^{\mu\perp}$, or $g \in S_n \setminus A_n$ and $s + \lambda sg \in S^{\mu\perp}$. If the latter holds, then $g = 1$, but this is ridiculous since $g \notin A_n$, so the former holds. Then again $g = 1$,

and as before this implies that $\lambda = 1$. Hence $S_n \times A$ has a regular orbit on $D^\mu \otimes_F \mathrm{sgn}$, and the claim is proved.

Fix $1 \neq g \in S_n$ and $\lambda \in F^*$. Then $s - \lambda sg \neq 0$, or else g is a non-trivial automorphism of the underlying graph of s. Moreover, the underlying graph Γ of $s - \lambda sg$ has at most $2n + 8$ edges when $n \geqslant 13$ or 28 edges when $n = 12$, and its vertices have degree at most 8. Note that if $n = 12$, then Γ cannot be $K_{4,8}$, $K_6 \cup K_6$ or $K_5 \cup K_8$, as these graphs have too many edges. Hence Lemma 8.3.3 implies that there exist distinct vertices i, j, k, l such that $\{i, j\}$ is an edge of Γ but $\{j, k\}$, $\{k, l\}$ and $\{l, i\}$ are not edges of Γ. Let

$$s' := \begin{cases} \{i,j\} - \{j,k\} + \{k,l\} - \{l,i\} & \text{if } \mu = (n-2,2), \\ (i,j) - (j,i) + (j,k) - (k,j) & \\ \quad +(k,l) - (l,k) + (l,i) - (i,l) & \text{if } \mu = (n-2,1^2). \end{cases}$$

Then $s' \in S^\mu$. We claim that $< s - \lambda sg, s' > \neq 0$, in which case $s - \lambda sg \notin S^{\mu\perp}$, as desired. Certainly this is the case if $\mu = (n-2, 2)$ since $< s - \lambda sg, s' >$ is the weight of the edge $\{i, j\}$ in $s - \lambda sg$, so we suppose that $\mu = (n-2, 1^2)$. Observe that (u, v) is an edge of $t \in S^\mu$ if and only if (v, u) is an edge of t. Also, if (u, v) has weight δ in t, then (v, u) has weight $-\delta$ in t. Let δ be the weight of (i, j) in $s - \lambda sg$. Then $< s - \lambda sg, s' > = < \delta(i,j) - \delta(j,i), (i,j) - (j,i) > = 2\delta \neq 0$, or else μ is not $\mathrm{char}(F)$-regular. □

We now prove Proposition 8.3.1.

Proof of Proposition 8.3.1. By Lemma 8.3.2, $V \downarrow A_n$ is irreducible, so V is irreducible as an $F(A_n \times A)$-module as well. It therefore suffices to show that $S_n \times A$ has a regular orbit on V, where V is D^μ or $D^\mu \otimes_F \mathrm{sgn}$ and μ is $(n-2, 2)$ or $(n-2, 1^2)$.

Suppose first of all that $n \geqslant 13$. Let $m := 2\lfloor n/2 \rfloor$. If $\mu = (n-2, 2)$, then define

$$\begin{aligned} s_1 &:= \{1,2\} - \{2,4\} + \{4,5\} - \{5,1\}, \\ s_2 &:= \{2,3\} - \{3,4\} + \{4,6\} - \{6,2\}, \\ s_3 &:= \{5,6\} - \{6,7\} + \cdots + \{m-1,m\} - \{m,5\}, \end{aligned}$$

and if $\mu = (n-2, 1^2)$, then define s_1, s_2 and s_3 by replacing each weighted edge $\pm\{i, j\}$ above with $(i, j) - (j, i)$. Note that s_1, s_2 and s_3 are in S^μ in either case. Let $s := s_1 + s_2 + s_3$. Then the underlying graph of s has $m + 4$ edges and maximal degree 4. Moreover, it is routine to verify that the underlying graph of s has a trivial automorphism group. Thus $S_n \times A$ has a regular orbit on D^μ and $D^\mu \otimes_F \mathrm{sgn}$ for $n \geqslant 13$ by Lemma 8.3.4.

Now suppose that $n = 12$ and $|F| \neq 2$. Then we may choose non-zero elements λ_1 and λ_2 of F such that $\lambda_1 + \lambda_2 \neq 0$. If $\mu = (n-2, 2)$, then define

$$\begin{aligned} s_1 &:= \lambda_1(\{1,2\} - \{2,3\} + \{3,4\} - \{4,1\}), \\ s_2 &:= \lambda_2(\{3,4\} - \{4,5\} + \{5,6\} - \{6,7\} + \{7,8\} - \{8,3\}), \\ s_3 &:= \lambda_1(\{7,8\} - \{8,9\} + \{9,10\} - \{10,11\} + \{11,12\} - \{12,7\}), \end{aligned}$$

and if $\mu = (n-2, 1^2)$, then define s_1, s_2 and s_3 by replacing each weighted edge $\pm\lambda_k\{i,j\}$ above with $\lambda_k(i,j) - \lambda_k(j,i)$. Then for either partition μ, the element $s := s_1 + s_2 + s_3$ is an element of S^μ whose underlying graph has 14 edges, maximal degree 3 and a trivial automorphism group, so we are done by Lemma 8.3.4. Note that by extending s_3 so that s has $m+2$ edges, this construction would also work for $n \geqslant 12$ provided $|F| \neq 2$. □

To finish this section, we consider modules in $R_n(1)$, where we find the only infinite class of irreducible modules on which S_n has no regular orbits. Neither module in $R_n(0)$ is faithful for $n \geqslant 5$, so we are only concerned with modules in $R_n(1) \setminus R_n(0)$. In particular, we are primarily concerned with the partition $\mu = (n-1, 1)$. Let F be a field. Note that M^μ is isomorphic to the permutation module F^n where S_n acts on $(a_1, \ldots, a_n) \in F^n$ by permuting the coordinates; that is, $(a_1, \ldots, a_n)g^{-1} := (a_{1g}, \ldots, a_{ng})$ for all $g \in S_n$. Then S^μ is isomorphic to $S := \{(a_1, \ldots, a_n) \in F^n : \sum_{i=1}^n a_i = 0\}$. The FS_n-module S has dimension $n-1$ and is called the *deleted permutation module*. Moreover, $S^{\mu\perp}$ is isomorphic to $S^\perp = \{(a, \ldots, a) \in F^n\}$, and clearly $S \cap S^\perp$ is either 0 when $p \nmid n$, or $S^\perp$ when $p \mid n$. Then D^μ is isomorphic to the *fully deleted permutation module* $D := S/S \cap S^\perp$. Note that D has dimension $n-1$ if $p \nmid n$ and dimension $n-2$ if $p \mid n$.

We now determine the regular orbits of $D^{(n-1,1)}$. The proof of this result is a straightforward computation, and we include it here for the sake of completeness. Note that for a finite field F of characteristic p, the regular orbits of $S_n \times F^*$ on $S^{(n-1,1)}$ have been determined by Gluck [31] and also Schmid [66] (for $p > n$) using different methods.

Proposition 8.3.5. *Suppose that $n \geqslant 5$, and let p be a prime.*

(i) The group S_n has a regular orbit on the $\mathbb{F}_pS_n$-module $D^{(n-1,1)}$ if and only if S_n has a regular orbit on $D^{(n-1,1)} \otimes_{\mathbb{F}_p} \mathrm{sgn}$ if and only if $p > n$.

(ii) The group A_n has a regular orbit on the irreducible $\mathbb{F}_pA_n$-module $D^{(n-1,1)} \downarrow A_n$ if and only if $p > n$ or $p = n-1$.

Proof. Let S and D be as defined above where $F = \mathbb{F}_p$, and let $V := D$ and $W := S \cap S^\perp$. Note that the $\mathbb{F}_pA_n$-module $V \downarrow A_n$ is irreducible for all $n \geqslant 5$, for if not, then a similar argument to that in the proof of Lemma 8.3.2 implies $\dim_{\mathbb{F}_p}(V)/2 \leqslant \dim_{\mathbb{F}_p}([\mathbb{F}_p^n, (12)])$,

but $[\mathbb{F}_p^n, (12)]$ is one-dimensional, a contradiction. We prove (i) and (ii) simultaneously by considering the various possibilities for p in relation to n.

If $p \leqslant n-2$, then clearly any n-tuple of elements from $\mathbb{F}_p$ must contain either three repeated elements or two pairs of repeated elements, so every element of V is fixed by some non-trivial element of A_n. But if A_n has no regular orbits on V, then S_n has no regular orbits on V or $V \otimes_{\mathbb{F}_p} \mathrm{sgn}$, so this case is complete.

If $p = n$, then we claim that A_n has no regular orbits on V, from which it follows once again that S_n has no regular orbits on V or $V \otimes_{\mathbb{F}_p} \mathrm{sgn}$. Let $v + W \in V$. Note that if v has exactly two repeated elements, then there is exactly one element $b \in \mathbb{F}_p$ that does not appear in v, but the sum of the elements of $\mathbb{F}_p$ vanishes, as does the sum of the coordinates of v, so b must be the repeated element, a contradiction. Moreover, if v has at least two pairs of repeated elements or a triple of repeated elements, then $v + W$ is certainly fixed by a non-trivial element of A_n. Hence we may assume that v is of the form $(a_1, \ldots, a_p)$ where $a_i \neq a_j$ for all i and j. Let $g \in S_n$ be the permutation for which $vg = (a_1 + 1, \ldots, a_p + 1)$. Then g fixes $v + W$. Moreover, g must be a p-cycle, for if $(i_1 \cdots i_k)$ is a cycle of g for some $k \in [p]$, then $a_{i_k} = a_{i_1} + 1$ and $a_{i_j} = a_{i_{j+1}} + 1$ for all $j \in [k-1]$, and it follows that $a_{i_1} = a_{i_1} + k$. Thus $k = p$ and $g \in A_n$, as desired.

If $p = n - 1$, then $V = S$, and every element of V must contain at least two repeated elements. Thus S_n has no regular orbits on V. Moreover, $v := (1, 2, \ldots, p-1, 0, 0) \in V$, and if $vg = v$ for some $g \in A_n$, then $g = 1$. Thus A_n has a regular orbit on V. It remains to show that S_n has no regular orbits on $V \otimes_{\mathbb{F}_p} \mathrm{sgn}$. Let $0 \neq v \in V$. If v has at least three repeated elements or two pairs of repeated elements, then v is fixed by some non-trivial element g of A_n, and so $v \otimes 1$ will also be fixed by g. The only other possibility is for v to have exactly two repeated elements, say in positions i and j. Then every element of $\mathbb{F}_p$ appears in v, and since the sum of the elements of $\mathbb{F}_p$ vanishes, this repeated element must be 0. Then there exists a permutation $g \in S_n$ fixing i and j for which $vg = -v$. If g is odd, then $(v \otimes 1)g = v \otimes 1$, and if g is even, then $(v \otimes 1)g(ij) = v \otimes 1$. Thus S_n has no regular orbits on $V \otimes_{\mathbb{F}_p} \mathrm{sgn}$.

Lastly, suppose that $p > n$. Then $V = S$, and no non-trivial element of S_n fixes

$$\begin{cases} (1, -1, 2, -2, n/2, -n/2) & \text{if } n \text{ is even,} \\ (1, -1, 2, -2, \ldots, \lfloor n/2 \rfloor, -\lfloor n/2 \rfloor, 0) & \text{if } n \text{ is odd,} \end{cases}$$

as all of its entries are distinct. Thus S_n has a regular orbit on V, and so A_n does as well. For $V \otimes_{\mathbb{F}_p} \mathrm{sgn}$, let $a \in \mathbb{F}_p$ be such that the vector $v := (0, 1, 2, \ldots, n-2, a) \in V$. Then v cannot be fixed by any non-trivial element of A_n since it contains at most two repeats, and there can be no element of S_n taking v to $-v$ since the subset $\{0, 1, 2, \ldots, n-2, a\}$

of $\mathbb{F}_p$ cannot contain both -1 and -2. Hence S_n has a regular orbit on $V \otimes_{\mathbb{F}_p} \mathrm{sgn}$. □

8.4 Proof of the main theorem

In this section, we prove Theorem 8.0.1 by putting together the results of Sections 8.2 and 8.3 and then considering the remaining case of $5 \leqslant n \leqslant 7$.

Proof of Theorem 8.0.1. Lemma 7.5.1 and Theorem 8.1.1 imply that if V is a faithful irreducible $\mathbb{F}_pG$-module, then there exists a p-regular partition μ for which $V \leqslant D^\mu \downarrow G$. Moreover, $D^\mu \in R_n(m)$ for some non-negative integer m. Since V is faithful as an $\mathbb{F}_pG$-module, D^μ is faithful as an $\mathbb{F}_pS_n$-module, and so $D^\mu \notin R_n(0)$. If $D^\mu \in R_n(1) \setminus R_n(0)$, then μ or $m(\mu)$ is $(n-1,1)$, so the condition of (i) holds. Then (i) is precisely Proposition 8.3.5, so we assume that $D^\mu \notin R_n(1)$. Then neither μ nor $m(\mu)$ is $(n-1,1)$, so the condition of (ii) holds. We prove (ii) by first considering the case where $n \geqslant 7$, and then the case where $5 \leqslant n \leqslant 6$.

Suppose that $n \geqslant 7$. We are done by Propositions 8.2.2(i) and 8.2.3 if $D^\mu \notin R_n(2)$, so we assume that $D^\mu \in R_n(2) \setminus R_n(1)$. Moreover, if $G = S_n$, then we are done by Proposition 8.2.2(ii) and Proposition 8.3.1, so we assume that $G = A_n$. Then $V = D^\mu \downarrow G$ by Lemma 8.3.2. Suppose that G does not have a regular orbit on V. Then S_n does not have a regular orbit on D^μ, so Proposition 8.2.2(ii) and Proposition 8.3.1 imply that $p = 2$ and $\mu = (n-2,2)$ for $7 \leqslant n \leqslant 8$. If $\mu = (5,2)$, then we can find a regular orbit of G on V by using Magma [8] to do an exhaustive search, so $\mu = (6,2)$, in which case G does not have a regular orbit on V since $|V| = 2^{14} < |A_8|$.

Thus $5 \leqslant n \leqslant 6$. Recall that the dimensions of the irreducible $\mathbb{F}_pS_n$- and $\mathbb{F}_{p^2}A_n$-modules are given in [20, 44]. Moreover, using [20, 44] and Lemmas 7.6.6 and 7.6.7, we can ascertain whether $D^\mu \downarrow A_n$ splits, and if not, whether it is absolutely irreducible. In particular, we can compute the dimension of V. Note that the partition μ can be determined for a given dimension using [30, 56] or [40].

Suppose that $p \leqslant n$. If n, p, μ and G are not listed in Table 8.1, then we use Magma [8] to prove that G has a regular orbit on V either by showing that V fails the bound of Lemma 6.3.3, or by finding one through an exhaustive search. Thus we assume that n, p, μ and G are listed in Table 8.1. If μ is $(3,2)$ or $(4,1^2)$, then $D^\mu \downarrow A_n$ is irreducible but not absolutely irreducible, and A_n does not have a regular orbit on D^μ since either $2^4 = |V| < |A_n|$ when $\mu = (3,2)$, or a search of the orbits using Magma shows they are too small when $\mu = (4,1^2)$. Thus S_n does not have a regular orbit on D^μ. Moreover, if μ is $(4,2)$, then $D^\mu \downarrow A_n$ is absolutely irreducible, and A_n does not have a regular orbit on

D^μ since $2^4 = |V| < |A_n|$, so S_n does not either. Lastly, if μ is (3^2) or (2^3), then $D^\mu \downarrow A_n$ is absolutely irreducible, and we determine that S_n does not have a regular orbit on D^μ by using Magma to check that all of the orbits are too small. Note that $m(3^2) = (2^3)$.

Suppose instead that $p > n$. Assume for a contradiction that $G = S_n$ and G has no regular orbits on V. Then equation (1) of Lemma 6.3.7 implies that $\dim_{\mathbb{F}_p}(V) \leqslant (n-1)\log_p(n!)$. Note that $(n-1)\log_p(n!)$ is a decreasing function in p when n is fixed. If $n = 5$, then $\dim_{\mathbb{F}_p}(V)$ is 5 or 6, and so $p \leqslant 47$ or $p \leqslant 23$ respectively. There are two modules of dimension 5 and one of dimension 6. Using Magma [8], we check that G has a regular orbit on V in every case. If $n = 6$, then $\dim_{\mathbb{F}_p}(V)$ is 5, 9, 10 or 16, and so p is at most 719, 37, 23 or 7 respectively. There are four modules of dimension 5, two of dimension 9, two of dimension 10, and one of dimension 16. However, two of the modules of dimension 5 are associates in $R_n(1)$, and we already know that G has a regular orbit on these. Again, we use Magma to check that G has a regular orbit on V in every case. For the case where $\dim_{\mathbb{F}_p}(V) = 5$, this required an exhaustive search of the orbits for $p \leqslant 61$, but for $67 \leqslant p \leqslant 91$, random selection was enough to find a regular orbit, and for $101 \leqslant p \leqslant 719$, either random selection found a regular orbit or the bound of Lemma 6.3.3 failed.

Now suppose for a contradiction that $G = A_n$ and G has no regular orbits on V. Then $D^\mu \downarrow A_n$ cannot be irreducible, so $D^\mu_{\mathbb{F}_{p^2}} \downarrow A_n$ splits. Thus either $n = 5$ and $\dim_{\mathbb{F}_p}(V) = 3$, or $n = 6$ and $\dim_{\mathbb{F}_p}(V) = 8$. It follows from the proof of [35, Lemma 6.1] that $r(A_n) \leqslant 3$ when $n = 5$ or $n = 6$, so $\dim_{\mathbb{F}_p G}(V) \leqslant 3\log_p(n!/2)$ by Lemma 6.3.6. Then $p \leqslant 59$ when $n = 5$, and $p \leqslant 7$ when $n = 6$, but we determine that $D^\mu \downarrow A_n$ splits only when $n = 5$ and $p \in \{11, 19, 29, 31, 41, 59\}$ using either the usual methods or Magma [8]. Then we use Magma to prove that A_n has a regular orbit on V for these remaining primes. □

8.5 Concluding remarks

Thus we have determined the regular orbits of the symmetric and alternating groups. The next step in the base size 2 problem for groups of affine type is to expand these results to include almost quasisimple groups G for which the socle of $G/Z(G)$ is A_n. In fact, a step towards this goal has already been achieved, as the regular orbits of the double covers of the symmetric and alternating groups have been determined in collaboration with O'Brien and Saxl [26]. In addition, many of the methods we have used will apply to almost quasisimple groups G for which the socle of $G/Z(G)$ is a sporadic simple group, as the outer automorphism group of a sporadic group has size at most 2.

Furthermore, Theorem 8.0.1 shows that S_n has a regular orbit on D^μ if and only if S_n has a regular orbit on $D^\mu \otimes_{\mathbb{F}_p} \mathrm{sgn}$. It would be interesting, therefore, to determine whether this occurs in general. In other words, if G is any group with an index 2 subgroup, F is any (finite) field of characteristic p, and V is any faithful irreducible FG-module, is it true that G has a regular orbit on V if and only if G has a regular orbit on $V \otimes_F \mathrm{sgn}$?

Another problem is to classify the regular orbits of S_n on faithful irreducible FG-modules for arbitrary finite fields F. Since $D^\mu_F = D^\mu_{\mathbb{F}_p} \otimes_{\mathbb{F}_p} F$ when F is a field of characteristic p, it follows that S_n has a regular orbit on D^μ_F if S_n has a regular orbit on $D^\mu_{\mathbb{F}_p}$. However, the converse is not necessarily true, so Theorem 8.0.1 implies that we must consider extensions of scalars of $D^\mu_{\mathbb{F}_p}$ where either μ or $m(\mu)$ is $(n-1,1)$ and $p \leqslant n$, or n, p, and μ are listed in Table 8.1. In fact, it is reasonable to consider whether for each n and p, there is a finite field F of characteristic p for which S_n has a regular orbit on every faithful irreducible FS_n-module.

More generally, we could consider this problem for A_n, or indeed for any group G whose regular orbits over $\mathbb{F}_p$ are determined. For if F is a finite field of characteristic p and V is a faithful irreducible FG-module, then there exists a unique faithful irreducible $\mathbb{F}_pG$-module U for which $V \leqslant U \otimes_{\mathbb{F}_p} F$ by Lemma 7.2.3, and we may view U as an $\mathbb{F}_pG$-submodule of V by Proposition 7.2.5, so G has a regular orbit on the FG-module V if G has a regular orbit on the $\mathbb{F}_pG$-module U. Thus, as with the symmetric group, it suffices to consider those faithful irreducible FG-modules V with the property that G has no regular orbits on the unique faithful irreducible $\mathbb{F}_pG$-module U for which $V \leqslant U \otimes_{\mathbb{F}_p} F$.

References

[1] Aschbacher, M., and Guralnick, R. M. Some applications of the first cohomology group. *J. Algebra 90* (1984), 446–460.

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

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

[4] Baddeley, R. W. Primitive permutation groups with a regular non-abelian normal subgroup. *Proc. London Math. Soc. 67* (1993), 547–595.

[5] Benson, D. Spin modules for symmetric groups. *J. London Math. Soc. 38* (1988), 250–262.

[6] Blackburn, N., and Huppert, B. *Finite groups II.* Springer-Verlag, Berlin, 1981.

[7] Bochert, A. Ueber die Zahl der verschiedenen Werthe, die eine Function gegebener Buchstaben durch Vertauschung derselben erlangen kann. *Math. Ann. 33* (1889), 584–590.

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

[9] Brauer, R. Number theoretical investigations on groups of finite order. In *Proc. Intern. Sympos. on Algebraic Number Theory, Tokyo and Nikko* (1956), pp. 55–62.

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

[11] Burness, T. C., Guralnick, R. M., and Saxl, J. Base sizes for geometric actions of finite classical groups. *In preparation*.

[12] Burness, T. C., Guralnick, R. M., and Saxl, J. Base sizes for S-actions of finite classical groups. *Israel J. Math. To appear*.

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

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

[15] Burness, T. C., O'Brien, E. A., and Wilson, R. A. Base sizes for sporadic simple groups. *Israel J. Math. 177* (2010), 307–333.

[16] Burness, T. C., and Seress, Á. On Pyber's base size conjecture. *Trans. Amer. Math. Soc. To appear*.

[17] Cameron, P. J. *Permutation groups*. Cambridge University Press, Cambridge, 1999.

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

[19] Cameron, P. J., Neumann, P. M., and Saxl, J. On groups with no regular orbits on the set of subsets. *Arch. Math. 43* (1984), 295–296.

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

[21] Curtis, C. W., and Reiner, I. *Representation theory of finite groups and associative algebras*. Amer. Math. Soc., Providence, 1962.

[22] Curtis, C. W., and Reiner, I. *Methods of representation theory*, vol. I. John Wiley and Sons Inc., New York, 1981.

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

[24] Dolfi, S. Orbits of permutation groups on the power set. *Arch. Math. 75* (2000), 321–327.

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

[26] Fawcett, J. B., O'Brien, E. A., and Saxl, J. Regular orbits of symmetric and alternating groups. *In preparation*.

[27] Ford, B., and Kleshchev, A. S. A proof of the Mullineux conjecture. *Math. Z. 226* (1997), 267–308.

[28] Fulman, J., and Guralnick, R. M. 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.

[29] Gallagher, P. X. The number of conjugacy classes in a finite group. *Math. Z. 118* (1970), 175–179.

[30] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.5.6*, 2012. `http://www.gap-system.org`.

[31] Gluck, D. Regular orbits on the deleted permutation module. *Arch. Math. 89* (2007), 481–484.

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

[33] Gluck, D., Seress, Á., and Shalev, A. Bases for primitive permutation groups and a conjecture of Babai. *J. Algebra 199* (1998), 367–378.

[34] Goodwin, D. P. M. Regular orbits of linear groups with an application to the $k(GV)$-problem, 1. *J. Algebra 227* (2000), 395–432.

[35] Guralnick, R. M., and Saxl, J. Generation of finite almost simple groups by conjugates. *J. Algebra 268* (2003), 519–571.

[36] Guralnick, R. M., and Tiep, P. H. The non-coprime $k(GV)$ problem. *J. Algebra 293* (2005), 185–242.

[37] Hall, J. I., Liebeck, M. W., and Seitz, G. M. Generators for finite simple groups, with applications to linear groups. *Quart. J. Math. Oxford 43* (1992), 441–458.

[38] Hölder, O. Bildung zusammengesetzter Gruppen. *Math. Ann. 46* (1895), 321–422.

[39] Isaacs, I. M. *Character theory of finite groups.* Dover publications, 1994.

[40] James, G. D. *The representation theory of the symmetric group.* Springer-Verlag, Berlin, 1978.

[41] James, G. D. On the minimal dimensions of irreducible representations of symmetric groups. *Math. Proc. Camb. Phil. Soc. 94* (1983), 417–424.

[42] James, G. D., and Liebeck, M. W. *Representations and characters of groups.* Cambridge University Press, Cambridge, 2001.

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

[44] Jansen, C., Lux, K., Parker, R., and Wilson, R. *An atlas of Brauer characters.* Clarendon Press, Oxford, 1995.

[45] Kleidman, P., and Liebeck, M. W. *The subgroup structure of the finite classical groups.* Cambridge University Press, Cambridge, 1990.

[46] Köhler, C., and Pahlings, H. Regular orbits and the $k(GV)$-problem. In *Groups and Computation III: Proceedings of the International Conference at the Ohio State University, June 15-19, 1999* (2001), pp. 209–228.

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

[48] Liebeck, M. W. Regular orbits of linear groups. *J. Algebra 184* (1996), 1136–1142.

[49] Liebeck, M. W., Praeger, C. E., and Saxl, J. On the O'Nan-Scott theorem for finite primitive permutation groups. *J. Austral. Math. Soc. 44* (1988), 389–396.

[50] Liebeck, M. W., and Pyber, L. Upper bounds for the number of conjugacy classes of a finite group. *J. Algebra 198* (1997), 538–562.

[51] Liebeck, M. W., and Saxl, J. Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces. *Proc. London Math. Soc. 3* (1991), 266–314.

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

[53] Liebeck, M. W., and Shalev, A. Bases of primitive permutation groups. *Groups, combinatorics and geometry: Durham* (2001), 147–154.

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

[55] Liebeck, M. W., and Shalev, A. Character degrees and random walks in finite groups of Lie type. *Proc. London Math. Soc. 90* (2005), 61–86.

[56] Maas, L. A. *SpinSym – a GAP package, Version 1.0*, 2013. `http://www.uni-due.de/~s400304/spinsym/`.

[57] Malle, G., Saxl, J., and Weigel, T. Generation of classical groups. *Geom. Dedicata 49* (1994), 85–116.

[58] Maslen, D. K., and Rockmore, D. N. Separation of variables and the computation of Fourier transforms on finite groups. *J. Amer. Math. Soc. 10* (1997), 169–214.

[59] Mazurov, V. D. Minimal permutation representations of finite simple classical groups. Special linear, symplectic, and unitary groups. *Algebra Logika 32* (1993), 142–153.

[60] Meyer, H. Finite splitting fields of normal subgroups. *Arch. Math. 83* (2004), 97–101.

[61] Miller, M. D. On the lattice of normal subgroups of a direct product. *Pac. J. Math. 60* (1975), 153–158.

[62] Müller, J. Private communication, 2011.

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

[64] Pyber, L. Asymptotic results for permutation groups. *DIMACS Ser. Discrete Math. Theoret. Comp. Sci. 11* (1993), 197–219.

[65] Rotman, J. J. *An introduction to the theory of groups.* Springer-Verlag, New York, 1995.

[66] Schmid, P. *The solution of the k(GV) problem.* Imperial College Press, London, 2007.

[67] Scott, L. L. Representations in characteristic p. In *The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979)* (1980), vol. 37, pp. 319–331.

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

[69] Seress, Á. Primitive groups with no regular orbits on the set of subsets. *Bull. London Math. Soc. 29* (1997), 697–704.

[70] Seress, Á. *Permutation group algorithms.* Cambridge University Press, Cambridge, 2003.

[71] Stroppel, M. Locally compact groups with many automorphisms. *J. Group Theory 4* (2001), 427–455.

[72] Suzuki, M. *Group theory I.* Springer-Verlag, Berlin, 1982.

[73] Vasilyev, A. V. Minimal permutation representations of finite simple exceptional groups of types G_2 and F_4. *Algebra Logika 35* (1996), 371–383.

[74] Vasilyev, A. V. Minimal permutation representations of finite simple exceptional groups of types E_6, E_7, and E_8. *Algebra Logika 36* (1997), 518–530.

[75] Vasilyev, A. V. Minimal permutation representations of finite simple exceptional twisted groups. *Algebra Logika 37* (1998), 17–35.

[76] Vasilyev, V. A., and Mazurov, V. D. Minimal permutation representations of finite simple orthogonal groups. *Algebra Logika 33* (1995), 337–350.