Bases for permutation groups and related problems

By

Hong Yi Huang

School of Mathematics
University of Bristol

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

May 2025

Supervised by Professor Tim Burness

Abstract

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group on a finite set Ω. A *base* for G is a subset of Ω with trivial pointwise stabiliser, and the minimal size of a base is called the *base size* of G, denoted $b(G)$. This classical invariant has found a wide range of applications and connections, attracting significant attention since the early years of group theory in the 19th century. Historically, there has been a particular focus on studying base sizes for primitive groups, which can be viewed as the basic building blocks of all finite permutation groups, and this still remains a very active area of research.

In the 1990s, Jan Saxl initiated a project with the ultimate goal of classifying the primitive groups G with $b(G) = 2$. In order to study the bases for these groups, Burness and Giudici defined the *Saxl graph* of G, where the vertex set is Ω, and two vertices are adjacent if they form a base. This opened up a new direction of studying the graph-theoretical properties of the Saxl graphs of primitive groups.

In this thesis, we focus on the study of base sizes and Saxl graphs of primitive groups. We determine the exact base size of every primitive group of diagonal type, and this is the first family of primitive groups arising in the O'Nan-Scott theorem for which the precise base size is known. We also initiate the study of base sizes for product type primitive groups, focussing on the groups with soluble point stabilisers. In addition, we extend the definition of the Saxl graph to groups G with $b(G) \geqslant 3$ and we study various connectivity properties of this graph for primitive groups, including its diameter, arc-transitivity and completeness. We adopt probabilistic and computational methods in order to establish the main theorems, which rely on a detailed analysis of the conjugacy classes and subgroup structure of the finite almost simple groups.

Dedication and acknowledgements

First of all, my deep thanks go to my supervisor, Tim Burness, for his exceptional supervision and patient guidance over the past four years. Thank you for your incredibly detailed comments on my work and invaluable advice regarding my career.

My examiners, Jeremy Rickard and Gareth Tracey, deserve much thanks for their thorough review of this lengthy thesis and for their valuable suggestions.

I sincerely appreciate all my collaborators for their brilliant ideas and dedication. I am especially indebted to my undergraduate supervisor, Cai Heng Li, for his ongoing insightful advice and encouragement, as well as his generous hospitality during my research visits in 2021 and 2023. I would also like to express my gratitude to the mathematicians across the world who have warmly welcomed me as a visitor.

I would like to thank all the co-organisers of *Seminars on Groups and Graphs* and *Bristol Junior Algebra and Combinatorics Seminar* for sustaining these valuable seminars with me.

I am grateful to have shared an office with Alec, Desmond, and Stelios. Their camaraderie has greatly enriched my PhD experience in Bristol.

I acknowledge the financial support from the China Scholarship Council for my doctoral studies. I also appreciate the support from the School of Mathematics and the Alumni Grant of the University of Bristol for my research activities over the past four years.

Let me also extend my heartfelt thanks to my close friends, especially Sicheng Xu, for understanding me as always, even when my PhD life might have seemed dull to them at times.

Finally, I owe my deepest gratitude to my family. My parents, grandparents and my beloved Bo Lan especially, whose unwavering love and support have been my greatest source of motivation throughout the PhD journey.

Author's declaration

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

SIGNED: .... DATE: 19/5/25

Table of Contents

List of Tables

Table **Page**

Chapter 1

Introduction

1.1 Background

In this thesis, we study bases for finite permutation groups and related problems. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group on a finite set Ω of size n. Then a *base* for G is a subset of Ω with trivial pointwise stabiliser, and the *base size* of G, denoted $b(G)$, is the minimal size of a base for G. For example, if $\Omega = V$ is a vector space and $G = \mathrm{GL}(V)$ is the general linear group, then we have $b(G) = \dim V$.

This classical invariant has been studied intensively for many decades, stretching all the way back to the early years of permutation group theory in the nineteenth century. The study of bases has found a diverse range of applications and connections to other areas of mathematics, including the study of relational complexity in model theory [58], and the metric dimension of graphs [6]. Following the pioneering work of Sims [111], bases have also been used extensively in the computational study of finite groups. For example, if Δ is a base for G, then there is a one-to-one correspondence between the elements of G and the pointwise images of Δ under G (this observation implies that $b(G) \geqslant \log_n |G|$), and hence elements of G can be stored as $|\Delta|$-tuples, rather than $|\Omega|$-tuples.

Historically, there has been an intense focus on studying the base sizes of finite primitive groups (recall that a transitive permutation group is *primitive* if its point stabiliser is a maximal subgroup), which can be viewed as the basic building blocks of all finite permutation groups. For example, a classical result of Bochert from 1889 [8] shows that $b(G) \leqslant n/2$ if G is a primitive group not containing A_n.

Two truly remarkable theorems proved in the 1980s have revolutionised the study of primitive groups, namely the O'Nan-Scott theorem and the Classification of Finite Simple Groups (CFSG). The former, recorded as Theorem 2.1.1 in Section 2.2.1, describes the finite primitive groups in terms of the structure and action of the socle of the group, while the latter theorem (see Theorem 2.2.1) is widely regarded as one of the greatest mathematical achievements of the 20th century.

With these powerful tools in hand, Bochert's bound has been significantly strengthened, and it turns out that all primitive groups admit small bases in the sense that there is an absolute constant c such that $b(G) \leqslant c\log_n |G|$ for every primitive group G. This was originally conjectured by Pyber [106] in the 1990s and the proof was completed by Duyan et al. in [48]. It was subsequently extended by Halasi et al. [67], who show that

$$b(G) \leqslant 2\log_n |G| + 24$$

and the multiplicative constant 2 is best possible. In fact, one can prove stronger bounds in special cases. For example, Seress [110] proves that $b(G) \leqslant 4$ if G is soluble, and this result was recently extended by Burness [14], who shows that $b(G) \leqslant 5$ if G has a soluble point stabiliser (both bounds in [14] and [110] are best possible).

1.2 Main problems

In general, determining $b(G)$ is a difficult problem and there are no efficient algorithms for computing $b(G)$, or for constructing a base of minimal size. Blaha [7] proves that determining whether or not G has a base of size at most a given constant is an NP-complete (nondeterministic polynomial-time complete) problem. However, determining the precise base size of a primitive group is an interesting (and ambitious) problem, which has seen a wide range of applications.

Problem I. *Determine the base size of every finite primitive group.*

For example, a project initiated by Saxl in the 1990s has the ultimate goal of determining all the primitive groups with a base of size 2 (these are the so-called *base-two* groups). Base-two groups arise naturally in many other problems, including the proof of the $k(GV)$-conjecture [59], the study of strong 2-generation properties of simple groups [24], the classification of extremely primitive groups [31], and bounding the diameter of the soluble graph of an almost simple group [29]. We will discuss this general problem in more detail in Section 2.3.

In [20], Burness and Giudici introduced the *Saxl graph* (named after Jan Saxl) of a base-two permutation group $G \leqslant \mathrm{Sym}(\Omega)$, as a tool for studying these groups. Here the vertex set is Ω and two vertices are adjacent if and only if they form a base for G. Many new problems were opened up to investigate the Saxl graphs of finite transitive permutation groups G with $b(G) = 2$, including the connectivity, automorphisms and various invariants of the graph. We refer the reader to [27, Section 7] for more details.

In Chapter 3, we will extend this concept by defining the following graph.

Definition. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group with $b(G) \geqslant 2$. Then the *generalised Saxl graph* of G, denoted $\Sigma(G)$, is the graph with vertex set Ω, with two vertices α and β adjacent if and only if $\{\alpha, \beta\}$ is a subset of a base for G of size $b(G)$.

For the remainder of this chapter, let $\Sigma(G)$ be the generalised Saxl graph of a permutation group $G \leqslant \mathrm{Sym}(\Omega)$ with $b(G) \geqslant 2$. Clearly, $\Sigma(G)$ is vertex-transitive if G is transitive on Ω, and it is connected if G is primitive. An intriguing conjecture [20, Conjecture 4.5] of Burness and Giudici asserts that if G is a primitive base-two group then any two vertices in $\Sigma(G)$ have a common neighbour. We extend this conjecture to general primitive groups as follows.

Conjecture II. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive group with $b(G) \geqslant 2$. Then any two vertices in $\Sigma(G)$ have a common neighbour.*

We will also consider the following two problems concerning the generalised Saxl graphs.

Problem III. *Classify the primitive groups G such that $\Sigma(G)$ is G-arc-transitive.*

Problem IV. *Classify the primitive groups G such that $\Sigma(G)$ is a complete graph.*

We refer the reader to Section 3.3 for more detailed discussion on these problems.

1.3 Main results

The main results in this thesis are selected from the following papers

T.C. Burness and H.Y. Huang, *On base sizes for primitive groups of product type*, J. Pure Appl. Algebra **227** (2023), Paper No. 107228, 43 pp.

T.C. Burness and H.Y. Huang, *On the Saxl graphs of primitive groups with soluble stabilisers*, Algebr. Comb. **5** (2022), 1053–1087.

S.D. Freedman, H.Y. Huang, M. Lee and K. Rekvényi, *On the generalised Saxl graphs of permutation groups*, submitted (2024), arXiv:2410.22613.

H.Y. Huang, *Base sizes of primitive groups of diagonal type*, Forum Math. Sigma **12** (2024), Paper No. e2, 43 pp.

which are [26], [27], [52] and [71] respectively.

We first focus on Problem I, and we will give a complete answer for the family of *diagonal type* primitive groups (this will be presented in Chapter 5). Here

$$T^k \trianglelefteqslant G \leqslant T^k.(\mathrm{Out}(T) \times S_k) \leqslant \mathrm{Sym}(\Omega) \tag{1.3.1}$$

for some non-abelian simple group T and integer $k \geqslant 2$, where Ω can be identified with the cosets $[T^k : D]$ of the diagonal subgroup D of T^k, and the subgroup $P \leqslant S_k$ induced by the action of G on the k factors of T^k is either primitive, or $(k, P) = (2, 1)$. An earlier paper of Fawcett [51] from 2013 determines the base size of G up to one of two possible values (see Theorem 5.2.3). However, determining the precise base size is challenging, and a new approach is required. This will be discussed in Chapter 5 in further detail, where we resolve Problem I for diagonal type primitive groups in full generality (a precise statement will be given in Theorem 5.1).

In terms of the O'Nan-Scott theorem, this is the first family of primitive groups for which the exact base sizes have been computed in all cases.

Theorem A. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive group of diagonal type. Then $b(G)$ is known.*

Next let us turn to the primitive groups of *product type*. Here

$$T^k \trianglelefteqslant G \leqslant L \wr P \tag{1.3.2}$$

for some primitive group $L \leqslant \mathrm{Sym}(\Gamma)$ with socle T and some transitive group $P \leqslant S_k$, and Ω can be identified with the Cartesian product Γ^k. We refer the reader to Section 6.2.2 for the formal definition of a product type primitive group. In particular, we may assume L is either almost simple or of diagonal type.

Base sizes for product type groups of the form $G = L \wr P$ have been considered by Bailey and Cameron [6]. Indeed, they describe $b(L \wr P)$ in terms of the number of regular L-orbits on Γ^m for some integer m, and the so-called *distinguishing number* of P in its action on $\{1,\dots,k\}$ (see Section 6.2.1). We refer the reader to Theorem 6.2.6 for this result.

As one might expect, there is a natural distinction to make in the study of Problem I between the full wreath product $L \wr P$ and its proper (primitive) subgroups. The analysis of bases in the latter setting is significantly more difficult and there are very few (if any) existing results in the literature that are tailored to this particular situation. In Chapter 6 we will take the first step towards developing a general theory in this direction, and we will establish the following result (see Theorem 6.6 for a more detailed statement).

Theorem B. *Let $G \leqslant L \wr P$ be a product type primitive group as in* (1.3.2)*, where $k = b(L) = 2$, $P \leqslant G$ and G has soluble point stabilisers. Then $b(G)$ is known.*

Next, we discuss our main results concerning the generalised Saxl graphs of primitive groups. The first theorem studies Conjecture II for almost simple primitive groups.

Theorem C. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive group with socle T. Then any two vertices in $\Sigma(G)$ have a common neighbour if one of the following holds:*

(i) T is a sporadic simple group and $b(G) \geqslant 3$.

(ii) G has soluble point stabilisers.

We are also able to establish Conjecture II for the almost simple groups G with socle $\mathrm{L}_2(q)$, except for one difficult case where the point stabilisers have a particular structure (see Theorem 4.2(i)), which we leave as an open problem. In particular, since the latter case only occurs when $G > \mathrm{L}_2(q)$, we deduce that Conjecture II holds for all primitive actions of $\mathrm{L}_2(q)$.

We will also establish Conjecture II for some base-two primitive groups of diagonal and twisted wreath types. See Theorems 5.6 and 5.9.1, respectively.

Now we turn to Problem III, which involves determining the groups G such that $\Sigma(G)$ is a G-arc-transitive graph. We will resolve this problem for the diagonal type primitive groups in Chapter 5 (see Theorem 5.3).

Theorem D. *The diagonal type primitive groups G as in* (1.3.1) *such that $\Sigma(G)$ is G-arc-transitive are classified.*

We are also able to resolve this problem for the groups with socle $\mathrm{L}_2(q)$ apart from the aforementioned special case (see Theorem 4.3 for more details). We refer the reader to Theorem 5.9.2 for a partial result on Problem III for primitive twisted wreath products.

Let $\mathrm{reg}(G)$ be the number of regular G-orbits on $\Omega^{b(G)}$, with the componentwise action of G. Then $\mathrm{reg}(G) \geqslant 1$, and the equality implies that $\Sigma(G)$ is G-arc-transitive (see Lemma 3.2.5). With this observation in mind, we are also interested in classifying the primitive groups G with $\mathrm{reg}(G) = 1$. The following result is a simplified version of Theorem 4.5.

Theorem E. *The almost simple primitive groups G with soluble point stabilisers and* $\mathrm{reg}(G) = 1$ *are classified.*

Finally, we present our main result on Problem IV, which concerns classifying the groups G such that $\Sigma(G)$ is a complete graph (see Theorem 4.6).

Theorem F. *The primitive groups G with socle* $\mathrm{L}_2(q)$ *such that $\Sigma(G)$ is a complete graph are classified.*

We will also give partial solutions to Problem IV for almost simple groups with sporadic socle and diagonal type groups. See Proposition 4.4.1 and Theorem 5.4, respectively.

Remark. In this thesis, we mainly focus on the problems discussed in Section 1.2, and we have a particular interest in the following families of primitive groups:

(a) groups with socle $\mathrm{L}_2(q)$;

(b) almost simple groups with sporadic socle;

(c) almost simple groups with soluble point stabilisers;

(d) diagonal type groups as in (1.3.1);

(e) product type groups as in (1.3.2) with soluble point stabilisers.

Groups	Problem I	Conjecture II	Problem III	Problem IV
(a)	4.1 ☺	4.2(i)	4.3	4.6 ☺
(b)	[30, 104] ☺	[20, Section 6], 4.2(ii)		4.4.1
(c)	[14] ☺	4.2(iii) ☺	4.5	
(d)	5.1 ☺	5.6	5.3 ☺	5.4
(e)	6.1, 6.6, 6.6.11		6.2	

Table 1.1: Road map of the results

For these groups, Table 1.1 gives a brief road map of the results concerning Problems I, III, IV and Conjecture II. In the table, a happy face ☺ is given if the problem is completely resolved for the relevant groups (see the corresponding reference). The cases that remain open (that is, without ☺ or even blank (which means partial results are given, or no progress so far) in Table 1.1) will be the subject of future work.

1.4 Methods

Let us briefly discuss the methods we will use to establish our main theorems.

In general, it is difficult to construct a base of "small" size. To overcome this difficulty, we will adopt a widely used probabilistic method for studying bases, which was first introduced by Liebeck and Shalev in 1999 [96]. Suppose $G \leqslant \mathrm{Sym}(\Omega)$ is a transitive permutation group with point stabiliser H. For a positive integer c, define

$$Q(G,c) = \frac{|\{(\alpha_1,\dots,\alpha_c) \in \Omega^c \ : \ \bigcap_i G_{\alpha_i} \neq 1\}|}{|\Omega|^c},$$

which is the probability that a uniformly random c-tuple of points in Ω is not a base for G. Note that $Q(G,c) < 1$ if and only if $b(G) \leqslant c$.

An upper bound on $Q(G,c)$ can be obtained by estimating the *fixed point ratios* of prime order elements in G with respect to their action on Ω. More precisely, let $\mathrm{fpr}(x)$ be the probability that $x \in G$ fixes a randomly chosen element of Ω. In view of [91, Lemma 2.5], we have $\mathrm{fpr}(x) = |x^G \cap H|/|x^G|$, and it is straightforward to show that

$$Q(G,c) \leqslant \sum_{i=1}^{k} |x_i^G| \cdot \mathrm{fpr}(x)^c = \sum_{i=1}^{k} \frac{|x_i^G \cap H|^c}{|x_i^G|^{c-1}} =: \widehat{Q}(G,c),$$

where $\{x_1,\dots,x_k\}$ is a complete set of representatives of the conjugacy classes of prime order elements in G. In particular, $b(G) \leqslant c$ if $\widehat{Q}(G,c) < 1$. One can observe from the definition of $\widehat{Q}(G,c)$ that the study of prime order elements and their conjugacy classes plays a central role in applying this method. Indeed, this approach turns out to be effective when G is an almost simple primitive group thanks to a series of works on estimating the fixed point ratios (for example, [15–18, 22, 82, 91, 96]).

The same approach can also be applied to study the generalised Saxl graph $\Sigma(G)$. Intuitively, if the probability $Q(G,b(G))$ is "small", then there are "many" bases of size $b(G)$, and so $\Sigma(G)$ has "many" edges. For example, if $\widehat{Q}(G,b(G)) < 1/2$ (and so $Q(G,b(G)) < 1/2$), then any two vertices in $\Sigma(G)$ have a common neighbour (see Lemma 3.2.6(i)). This was first observed in [20] for the original Saxl graphs, and it will be one of our key tools in the study of Conjecture II.

We also introduce and apply probabilistic methods in the proof of Theorem A for diagonal type groups in Chapter 5. Here G is as in (1.3.1), and we will show that

$$b(G) = 2 \textit{ if there exists a subset } S \textit{ of } T \textit{ of size } k \textit{ such that } \mathrm{Hol}(T,S) = 1,$$

where $\mathrm{Hol}(T,S)$ is the setwise stabiliser of S in the holomorph $\mathrm{Hol}(T) = T{:}\mathrm{Aut}(T)$ of T (the precise action of $\mathrm{Hol}(T)$ on T will be discussed in Section 5.3). Given this observation, we will bound the probability that a uniformly random k-subset of T has trivial setwise stabiliser in $\mathrm{Hol}(T)$. This will be introduced and discussed in Section 5.4.1.

Computational methods also play an important part in our study of bases and generalised Saxl graphs. We refer the reader to Section 4.2 for more details.

Chapter 2

Preliminaries

In this chapter we will introduce the relevant background for our work in Chapters 3–6. In Sections 2.1 and 2.2 we will present some preliminary material on permutation groups and simple groups, highlighting the O'Nan-Scott theorem on the structure of primitive permutation groups and the Classifications of Finite Simple Groups. Some of the earlier work on bases for primitive groups will be presented in Section 2.3. Finally, we present a powerful probabilistic method for studying bases in Section 2.4.

Let us first set up the notation we will use in this thesis, which is all fairly standard. More specifically, let n, m be positive integers and let G, H be groups. Then

$[n]$ is the set $\{1,\dots,n\}$ or an unspecified group of order n (this should not cause any confusion)

(n,m) is the greatest common divisor of n and m

$\log n = \log_2 n$

C_n, or sometimes n, is the cyclic group of order n

G^n is the direct product of n copies of G

$G^\#$ is the set of non-identity elements of G

$G \times H$ is the direct product of G and H

$G.H$ is an unspecified extension of G by H

$G{:}H$ is an unspecified semidirect product of G by H

$G \wr H$ is the wreath product $G^n{:}H$, where $H \leqslant S_n$ permutes the components of G^n

$[G : H]$ is the set of right cosets of a subgroup H of G

x^g is the conjugate $g^{-1}xg$ for $x, g \in G$, and x^G is the G-conjugacy class of x

$i_m(G)$ is the number of elements of order m in G

Moreover, if $G \leqslant \mathrm{Sym}(\Omega)$ is a permutation group and $\Delta \subseteq \Omega$, then

α^g is the image of $\alpha \in \Omega$ under $g \in G$

α^G is the orbit of G containing α

G_α is the point stabiliser of α in G

$G_{(\Delta)}$ is the pointwise stabiliser of Δ in G

$G_{\{\Delta\}}$ is the setwise stabiliser of Δ in G

We adopt the standard notation for simple groups of Lie type from [80].

2.1 Permutation groups

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group on a finite set Ω. An *orbit* α^G of G is the set of images of α under G. That is,

$$\alpha^G = \{\alpha^g : g \in G\}.$$

On the other hand, the *point stabiliser* of α, denoted G_α, is the subgroup of elements in G fixing α, so

$$G_\alpha = \{g \in G : \alpha^g = \alpha\}.$$

By the orbit-stabiliser theorem, we have

$$|G| = |G_\alpha| \cdot |\alpha^G|.$$

In particular, the orbit α^G is called *regular* if $G_\alpha = 1$ (or equivalently, $|\alpha^G| = |G|$).

The group G is called *transitive* if there is a unique G-orbit on Ω. In this setting, the point stabilisers are G-conjugate subgroups, and the action of G on Ω is equivalent to its action on the set of right cosets $[G : G_\alpha]$ given by right multiplication

$$(G_\alpha x)^g = G_\alpha xg$$

for any $x, g \in G$. Thus, we can identify the set Ω with the right cosets $[G : H]$ for some point stabiliser H.

From now on, we assume G is transitive on Ω and $H = G_\alpha$ is a point stabiliser. An orbit of H on Ω is called a *suborbit* of G. Clearly, $\{\alpha\}$ is a suborbit of G. If $\Omega \setminus \{\alpha\}$ is a suborbit of G, then G is said to be 2-*transitive*. The classification of finite 2-transitive groups has been completed in [69, 73], and this relies on the Classification of Finite Simple Groups (see Theorem 2.2.1 below).

In this thesis, we are mainly interested in primitive permutation groups, which can be viewed as the basic building blocks of all finite permutation groups. Precisely, a transitive group $G \leqslant \mathrm{Sym}(\Omega)$ is called *primitive* if its point stabiliser H is a maximal subgroup of G. In particular, any 2-transitive group is primitive.

Type	Description
I	Affine: $G = V{:}H \leqslant \mathrm{AGL}(V)$, $H \leqslant \mathrm{GL}(V)$ irreducible
II	Almost simple: $T \leqslant G \leqslant \mathrm{Aut}(T)$
III	Diagonal type: $T^k \leqslant G \leqslant T^k.(\mathrm{Out}(T) \times P)$, $P \leqslant S_k$ primitive, or $k = 2$, $P = 1$
IV	Product type: $G \leqslant L \wr P$, L primitive of type II or III, $P \leqslant S_k$ transitive
V	Twisted wreath product: $G = T^k{:}P$, $P \leqslant S_k$ transitive

Table 2.1: The five families of finite primitive groups in the O'Nan-Scott theorem

There is another way to define the primitive groups. A subset B of Ω is called a *block* if $B^g \cap B = B$ or $\emptyset$ for any $g \in G$. If B is a block, then the set B^G of images of B under G is a G-invariant partition of Ω, which is said to be a *block system* of G. Note that B is a block if $B = \Omega$ or $|B| = 1$, and the associated block systems are the so-called *trivial block systems*. The group G is primitive if and only if the only block systems are the trivial ones. This is due to the fact that $G_\alpha < G_{\{B\}} < G$ if $\alpha \in B$ and B^G is a non-trivial block system, where $G_{\{B\}}$ denotes the setwise stabiliser of B.

One of the key tools for studying the finite primitive groups is the O'Nan-Scott theorem from the 1980s. Following [88], this theorem divides the primitive groups into five families, as briefly described in Table 2.1 (in the table, T denotes a non-abelian finite simple group).

Theorem 2.1.1 (O'Nan-Scott)**.** *Suppose G is a finite primitive permutation group. Then G is of one of the types described in Table 2.1.*

We will discuss the structures of the groups of types III and IV in more detail in Chapters 5 and 6, respectively. For more information on twisted wreath products, we refer the reader to [5].

2.2 Simple groups

The study of finite simple groups has a wide range of applications in many areas of mathematics. The O'Nan-Scott theorem makes it clear that understanding the finite simple groups plays a central role in the study of primitive groups, especially the almost simple primitive groups. In fact, many problems concerning the primitive groups of other types can often be reduced to questions concerning simple groups (for example, see Lemma 5.3.1 in Chapter 5). In this section, we briefly introduce the finite simple groups, highlighting the Classification Theorem, their automorphisms, subgroup structure and conjugacy classes. Throughout, let T be a non-abelian finite simple group.

2.2.1 The finite simple groups

The Classification of Finite Simple Groups (CFSG) is widely regarded as one of the greatest mathematical achievements of the 20th century, which has revolutionised the study of permutation groups in recent years. The classification is stated as below.

Theorem 2.2.1 (CFSG). *Let T be a non-abelian finite simple group. Then T is isomorphic to one of the following groups:*

(i) an alternating group A_n with $n \geqslant 5$;

(ii) a classical group defined over a finite field $\mathbb{F}_q$:

(a) linear: $\mathrm{L}_n(q)$ with $n \geqslant 2$, except $\mathrm{L}_2(2)$ and $\mathrm{L}_2(3)$;

(b) unitary: $\mathrm{U}_n(q)$ with $n \geqslant 3$, except $\mathrm{U}_3(2)$;

(c) symplectic: $\mathrm{PSp}_n(q)$ with $n \geqslant 4$ even, except $\mathrm{PSp}_4(2)$;

(d) orthogonal: $\Omega_n(q)$ with $n \geqslant 7$ odd and q odd, or $\mathrm{P}\Omega_n^{\varepsilon}(q)$ with $\varepsilon \in \{+,-\}$ and $n \geqslant 8$ even;

(iii) an exceptional group of Lie type defined over a finite field $\mathbb{F}_q$: $G_2(q)$ ($q \geqslant 3$), $F_4(q)$, $E_6(q)$, $E_7(q)$, $E_8(q)$, ${}^3D_4(q)$, ${}^2E_6(q)$, ${}^2B_2(2^{2n+1})$ ($n \geqslant 1$), ${}^2G_2(3^{2n+1})$ ($n \geqslant 1$), ${}^2F_4(2^{2n+1})$ ($n \geqslant 1$), ${}^2F_4(2)'$;

(iv) a sporadic group: M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, J_1, J_2, J_3, J_4, Co_1, Co_2, Co_3, McL, HS, He, HN, Suz, Fi_{22}, Fi_{23}, Fi_{24}', Ru, Ly, O'N, Th, $\mathbb{B}$, $\mathbb{M}$.

Moreover, all the groups listed above are simple.

Remark 2.2.2. Throughout this thesis, we will assume $n \geqslant 3$ if $T = \mathrm{U}_n(q)$, $n \geqslant 4$ is even if $T = \mathrm{PSp}_n(q)$, and $n \geqslant 7$ if $T = \mathrm{P}\Omega_n^{\varepsilon}(q)$. We will sometimes write $\mathrm{L}_n(q) = \mathrm{L}_n^+(q)$, $\mathrm{U}_n(q) = \mathrm{L}_n^-(q)$, $E_6(q) = E_6^+(q)$ and ${}^2E_6(q) = E_6^-(q)$. For the remainder of this section, if not specified otherwise, we will also exclude the groups

$$\mathrm{L}_2(4),\ \mathrm{L}_2(5),\ \mathrm{L}_2(9),\ \mathrm{L}_3(2),\ \mathrm{L}_4(2),\ \mathrm{U}_4(2),\ \mathrm{Sp}_4(2)',\ G_2(2)',\ {}^2G_2(3)' \tag{2.2.1}$$

as each of them is isomorphic to one of the following groups (see [80, Proposition 2.9.1 and Theorem 5.1.1]):

$$A_5,\ A_6,\ A_8,\ \mathrm{L}_2(7),\ \mathrm{L}_2(8),\ \mathrm{U}_3(3),\ \mathrm{PSp}_4(3).$$

2.2.2 Automorphisms

A finite group is called *almost simple* if its *socle* (the product of its minimal normal subgroups) is non-abelian simple. Equivalently, a finite group G is almost simple if and only if

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

for some non-abelian simple group T (so T is one of the groups described in Theorem 2.2.1).

To understand the almost simple groups, we first need to determine the automorphism groups of the non-abelian simple groups. If $T = A_n$, then $\mathrm{Aut}(T) = S_n$ apart from the case where $n = 6$,

T	$\mathrm{Out}(T)$	Conditions
$\mathrm{L}_n(q)$	$C_{(n,q-1)}{:}(C_f \times C_2)$	$n > 2$
	$C_{(2,q-1)} \times C_f$	$n = 2$
$\mathrm{U}_n(q)$	$C_{(n,q+1)}.C_{2f}$	
$\mathrm{PSp}_n(q)$	$C_2.C_f$	$p \neq 2$
	$C_f.C_2$	$p = 2$, $n = 4$
	C_f	$p = 2$, $n > 4$
$\Omega_n(q)$	$C_2.C_f$	nq odd
$\mathrm{P}\Omega_n^+(q)$	$C_{(2,q-1)}^2.C_f.S_3$	$n = 8$
	$C_{(2,q-1)}^2.C_f.C_2$	$n > 8$, $n \equiv 0 \pmod 4$
	$C_{(4,q^{n/2}-1)}.C_f.C_2$	$n \equiv 2 \pmod 4$
$\mathrm{P}\Omega_n^-(q)$	$C_{(4,q^n+1)}.C_{2f}$	
${}^2B_2(q)$	C_f	
${}^2G_2(q)$	C_f	
${}^2F_4(q)$	C_f	$q > 2$
${}^2F_4(2)'$	C_2	
${}^3D_4(q)$	C_{3f}	
$G_2(q)$	C_f	$p \neq 3$
	$C_f.C_2$	$p = 3$
$F_4(q)$	C_f	$p \neq 2$
	$C_f.C_2$	$p = 2$
$E_6(q)$	$C_{(3,q-1)}.C_f.C_2$	
${}^2E_6(q)$	$C_{(3,q+1)}.C_{2f}$	
$E_7(q)$	$C_{(2,q-1)}.C_f$	
$E_8(q)$	C_f	

Table 2.2: Automorphism groups of the simple groups of Lie type

and we have $\mathrm{Aut}(A_6) = A_6.2^2 \cong \mathrm{P\Gamma L}_2(9)$ (see [121, Section 2.4]). For sporadic groups, we have $|\mathrm{Out}(T)| \leqslant 2$, with equality if and only if T is one of the following groups:

$$\mathrm{M}_{12},\ \mathrm{M}_{22},\ \mathrm{HS},\ \mathrm{J}_2,\ \mathrm{McL},\ \mathrm{Suz},\ \mathrm{He},\ \mathrm{HN},\ \mathrm{Fi}_{22},\ \mathrm{Fi}_{24}',\ \mathrm{O'N} \text{ and } \mathrm{J}_3.$$

If T is a finite simple group described in parts (ii) and (iii) of Theorem 2.2.1, we say T is of *Lie type*. A classical theorem of Steinberg [116, Theorem 30] asserts that the automorphism group $\mathrm{Aut}(T)$ of a finite simple group of Lie type T is generated by $\mathrm{Inn}(T) \cong T$ and its diagonal, field and graph automorphisms (see the terminology from [60, Theorem 2.5.1]). We record the structure of $\mathrm{Out}(T) = \mathrm{Aut}(T)/T$ in Table 2.2 from the relevant information in [121] (in the table, T is a finite simple group of Lie type defined over $\mathbb{F}_q$ of characteristic p, and $f = \log_p q$, noting that we exclude the groups listed in (2.2.1)).

Example 2.2.3. Let $T = \mathrm{L}_n(q)$ be a simple linear group as in Theorem 2.2.1(ii)(a), where $q = p^f$ for some prime p, and let $V = \mathbb{F}_q^n$ be the natural module for T. Fix a basis $\{e_1,\dots,e_n\}$ for V. Define $\delta \in \mathrm{PGL}_n(q)$ to be the image of the diagonal matrix $\mathrm{diag}(1,\dots,1,\lambda) \in \mathrm{GL}_n(q)$, where λ is a

T	$\mathrm{Inndiag}(T)$
$\mathrm{L}_n(q)$	$\mathrm{PGL}_n(q)$
$\mathrm{U}_n(q)$	$\mathrm{PGU}_n(q)$
$\mathrm{PSp}_n(q)$	$\mathrm{PGSp}_n(q)$
$\Omega_n(q)$, n odd	$\mathrm{PSO}_n(q) = \mathrm{PGO}_n(q)$
$\mathrm{P}\Omega_n^{\varepsilon}(q)$, n even	T if q is even
	$\mathrm{PSO}_n^{\varepsilon}(q).2$ if q is odd (see [21, p. 57])
${}^2F_4(2)'$	${}^2F_4(2)$
$E_6^{\varepsilon}(q)$	$T.(3, q-\varepsilon)$
$E_7(q)$	$T.(2, q-1)$
Other exceptional groups	T

Table 2.3: Inner-diagonal automorphism groups of the simple groups of Lie type

T	${}^2B_2(q)$	${}^2G_2(q)$	${}^2F_4(q)'$	${}^3D_4(q)$	$G_2(q)$	$F_4(q)$	$E_6^{\varepsilon}(q)$	$E_7(q)$	$E_8(q)$
d	5	7	26	28	14	52	78	133	248

T	$\mathrm{L}_n^{\varepsilon}(q)$	$\mathrm{PSp}_n(q)$	$\mathrm{P}\Omega_n^{\varepsilon}(q)$
d	n^2-1	$(n^2+n)/2$	$(n^2-n)/2$

Table 2.4: The integer d for Lie type groups in Lemma 2.2.4

generator of $\mathbb{F}_q^{\times}$, noting that $|\delta| = (n, q-1)$ and $\langle T, \delta\rangle = \mathrm{PGL}_n(q)$. We also define ϕ to be the field automorphism of order f such that $(a_1e_1 + \cdots + a_ne_n)^{\phi} = a_1^pe_1 + \cdots + a_n^pe_n$ for all $a_i \in \mathbb{F}_q$, and we write $\mathrm{P\Sigma L}_n(q) = \langle T, \phi\rangle$ and $\mathrm{P\Gamma L}_n(q) = \langle T, \delta, \phi\rangle$. In fact, the latter group is equal to $\mathrm{Aut}(T)$ if $n = 2$. For the groups with $n > 2$, the inverse-transpose map on $\mathrm{SL}_n(q)$ induces an automorphism γ of T of order 2, which is called a graph automorphism. Then $\mathrm{Aut}(T) = \langle T, \delta, \phi, \gamma\rangle$ and $\mathrm{P\Gamma L}_n(q)$ is a subgroup of $\mathrm{Aut}(T)$ of index 2.

For a simple group T of Lie type, the group of *inner-diagonal automorphisms*, denoted $\mathrm{Inndiag}(T)$, is the subgroup of $\mathrm{Aut}(T)$ generated by T and the diagonal automorphisms (see [60, Theorem 2.5.1(b) and Definition 2.5.10(d)]). Following [60, Theorem 2.5.12(c)], we record the precise structure of $\mathrm{Inndiag}(T)$ in Table 2.3 (once again, we exclude the groups in (2.2.1)). Here we note that if $T = \mathrm{P}\Omega_n^{\varepsilon}(q)$ with n even and q odd, then $|\mathrm{PSO}_n^{\varepsilon}(q) : T| \leqslant 2$, and we refer the reader to [21, p. 57] for the precise condition on when the equality holds.

Next we present [71, Lemma 2.10].

Lemma 2.2.4. *Suppose T is a finite simple group of Lie type and let d be the integer defined in Table 2.4. Then $\frac{1}{2}q^d < |\mathrm{Inndiag}(T)| < q^d$.*

Proof. This is [16, Proposition 3.9(i)] when T is a classical group, and the bounds for exceptional groups are clear (see [121, Chapter 4] for $|T|$). ■

From Lemma 2.2.4 and Tables 2.2, 2.3, we immediately deduce the following lemma, which is [51, Lemma 4.8] (note that the statement for alternating and sporadic groups is straightforward).

Lemma 2.2.5. *If T is a non-abelian finite simple group, then* $|\mathrm{Out}(T)| < |T|^{1/3}$.

The following result was originally Schreier's conjecture, which can be deduced from CFSG immediately.

Lemma 2.2.6. *If T is a non-abelian finite simple group, then* $\mathrm{Out}(T)$ *is soluble.*

2.2.3 Subgroup structure

The problem of determining the (core-free) maximal subgroups of almost simple groups has a long history, finding many applications. For example, recall that if $G \leqslant \mathrm{Sym}(\Omega)$ is primitive, then $H = G_\alpha$ is a (core-free) maximal subgroup. The ultimate goal here is to classify all the maximal subgroups of a given almost simple group up to conjugacy (equivalently, to classify all the primitive permutation representations of a given almost simple group, up to permutation isomorphism).

Let G be an almost simple group with socle T, so T is isomorphic to one of the groups recorded in Theorem 2.2.1.

2.2.3.1 Sporadic groups

If T is a sporadic group, then the complete list of maximal subgroups of G, up to conjugacy, is given in the survey article [120] if $T \neq \mathbb{M}$, and an almost complete list of maximal subgroups of the Monster group $\mathbb{M}$ is given in the same article. This information can also be found in the Web ATLAS [123]. Recently, the result was extended to a complete list of maximal subgroups of $\mathbb{M}$ [45].

2.2.3.2 Alternating and symmetric groups

Next, let us turn to the case where $T = A_n$ is an alternating group, so $G = A_n$ or S_n unless $n = 6$. In this setting, a variation of the O'Nan-Scott theorem determines all the maximal subgroups of G, apart from an unspecified collection of almost simple subgroups (see part (iii)(d) of the theorem below). To be precise, we record the theorem for $G = S_n$ (typically, the maximal subgroups of A_n arise as $H \cap A_n$ with $H < S_n$ maximal), which can be found in [3, p. 79]. Recall that $[n] = \{1, \dots, n\}$.

Theorem 2.2.7. *Suppose $G = S_n$ with $n \geqslant 5$, and let H be a core-free maximal subgroup of G. Then one of the following holds:*

(i) $H = S_k \times S_{n-k}$ is intransitive on $[n]$, where $1 \leqslant k < n/2$;

(ii) $H = S_a \wr S_b$ is imprimitive on $[n]$, where $ab = n$ with $a, b \geqslant 2$;

(iii) H is one of the following primitive groups on $[n]$:

(a) *$H = \mathrm{AGL}_d(p)$, where p is a prime, $d \geqslant 1$ and $n = p^d$;*

(b) *$H = S_a \wr S_b$, where $n = a^b$ with $a \geqslant 5$ and $b \geqslant 2$;*

(c) *$H = R^k.(\mathrm{Out}(R) \times S_k)$ for some non-abelian simple group R, where $n = |R|^{k-1}$ and $k \geqslant 2$;*

(d) *H is an almost simple group.*

Conversely, the maximality of subgroups lying in classes (i), (ii) and (iii)(a)–(c) are determined in [89]. Now let us briefly comment on the unspecified collection (iii)(d). As discussed in [89],

> *The general problem of listing all the maximal subgroups of A_n and S_n for all degrees n remains intractable, since it involves essentially finding all primitive permutation representations of all almost simple groups.*

Indeed, if X is an almost simple group and Y is a core-free maximal subgroup of X with $|X : Y| = n$, then the action of X on $[X : Y]$ embeds X in S_n. Thus, to study the groups in (iii)(d) (before even trying to determine the maximality in S_n), we would essentially need to know all of the maximal subgroups of all almost simple groups, up to conjugacy, which seems to be a non-achievable goal.

In some special cases, the maximal subgroups of A_n and S_n are completely determined, up to conjugacy (for example, when n is odd [76, 92]).

2.2.3.3 Classical groups

Now let G be a classical group defined over a finite field $\mathbb{F}_q$ of characteristic p, and let V be the natural module of G with $n = \dim V$. The main theorem here on the subgroup structure of these groups is Aschbacher's theorem [2]. Indeed, Aschbacher defined 9 collections of subgroups of G, namely $\mathscr{C}_1, \dots, \mathscr{C}_8$ and $\mathscr{S}$, as roughly described in Table 2.5, and he proved that any core-free maximal subgroup of G is contained in a member of one of the collections (apart from the groups with $T = \mathrm{P}\Omega_8^+(q)$). We refer to [80, Section 1.2] for a more detailed description of these classes. Here an unspecified collection is the class $\mathscr{S}$ of absolutely irreducible almost simple subgroups. As discussed above, listing all maximal subgroups lying in $\mathscr{S}$ for all classical groups is not achievable, since it involves determining the degrees of all absolutely irreducible representations of all almost simple groups.

Later on, Kleidman and Liebeck [80] dealt with the maximality and conjugacy of the subgroups in $\mathscr{C}_i$ for $n \geqslant 13$, and Bray, Holt and Roney-Dougal [11] completely determined the maximal subgroups, up to conjugacy, of every classical group with $n \leqslant 12$ (this extends several earlier works; for example, work of Dickson [44] for $\mathrm{L}_2(q)$ from 1901). To summarise, let us record these results on the maximal subgroups of classical groups.

Theorem 2.2.8. *Suppose G is an almost simple classical group with socle T. Let H be a core-free maximal subgroup of G. Then the following hold:*

Class	Rough description
$\mathscr{C}_1$	Stabilisers of proper nonzero subspaces
$\mathscr{C}_2$	Stabilisers of direct sum decompositions $V = \bigoplus_{i=1}^{m} V_i$, where $\dim V_i = n/m$
$\mathscr{C}_3$	Stabilisers of extension fields of $\mathbb{F}_q$ of prime degree
$\mathscr{C}_4$	Stabilisers of tensor product decompositions $V = V_1 \otimes V_2$
$\mathscr{C}_5$	Stabilisers of subfields of $\mathbb{F}_q$ of prime index
$\mathscr{C}_6$	Normalisers of symplectic-type r-groups, where $r \neq p$ is a prime
$\mathscr{C}_7$	Stabilisers of tensor product decompositions $V = \bigotimes_{i=1}^{m} V_i$, where $n = (\dim V_i)^m$
$\mathscr{C}_8$	Classical subgroups (stabilisers of non-degenerate classical forms on V)
$\mathscr{S}$	Absolutely irreducible almost simple subgroups

Table 2.5: The Aschbacher subgroup collections

(i) $H \in \mathscr{C}_i$ for some i, or $H \in \mathscr{S}$.

(ii) The group-theoretic structure of each $H \in \mathscr{C}_i$ is known.

(iii) The conjugacy amongst the members of $\mathscr{C}_i$ is known.

(iv) For $n \leqslant 12$, the group-theoretic structure and conjugacy of each $H \in \mathscr{S}$ is known.

In this thesis, we will refer to the *type* of a maximal subgroup of a classical group, which is consistent with its usage in [80, Section 3.5]. This provides an approximate description of the structure of the maximal subgroup and can be viewed as a refinement of the classes recorded in Table 2.5. For example, if $T = \mathrm{L}_n(q)$ then a maximal subgroup of type P_m is a maximal parabolic subgroup that stabilises an m-dimensional subspace of the natural module V. For $n \geqslant 3$, we also use $P_{m,n-m}$ to denote the stabiliser of a flag of subspaces $0 < V_m < V_{n-m} < V$, where $m < n/2$ and $\dim V_i = i$, which is a maximal subgroup of G only if G is not a subgroup of $\mathrm{P\Gamma L}_n(q)$. Both groups fall into the class $\mathscr{C}_1$. For details, see the tables in [80, Section 3.5].

2.2.3.4 Exceptional groups

Finally, assume T is an exceptional group defined over $\mathbb{F}_q$ of characteristic p.

If $T \in \{{}^2B_2(q), {}^2G_2(q), {}^3D_4(q), {}^2F_4(q)'\}$ then the maximal subgroups of G are known, up to conjugacy. See [117] for $T = {}^2B_2(q)$, [78] for ${}^2G_2(q)$, [79] for ${}^3D_4(q)$, [99] for ${}^2F_4(q)$ with $q > 2$, and [118, 122] for ${}^2F_4(2)'$.

Now assume $T \in \{G_2(q), F_4(q), E_6^{\varepsilon}(q), E_7(q), E_8(q)\}$. Let X be the ambient simple algebraic group over the algebraic closure of $\mathbb{F}_q$ and σ be an appropriate Steinberg endomorphism. Note that $X_\sigma = \mathrm{Inndiag}(T)$. As summarised in [95, Theorem 2] (see also [31, Theorem 5.1]), if H is a core-free maximal subgroup of G then one of the following holds:

(i) $H = N_G(M_\sigma)$, where M is a maximal closed σ-stable positive dimensional subgroup X;

(ii) H is a subfield subgroup (possibly twisted);

(iii) H is an exotic local subgroup (the normaliser of an r-subgroup with $r \neq p$);

(iv) H is a Borovik subgroup [9] ($T = E_8(q)$, $p > 5$ and $H \cap T = (A_5 \times A_6).2^2$);

(v) H is an almost simple group which is not of type (i) or (ii).

In fact, the maximal subgroups in the collections (i)–(iv) have been determined up to conjugacy (see [9, 39, 93, 95]). It is worth noting that, apart from the groups with $T = E_7(q)$ or $E_8(q)$, the maximal subgroups of G lying in (v) have been completely determined up to conjugacy through the work of numerous authors. In particular, we refer the reader to [38, 78] for the groups with $T = G_2(q)$, and the recent paper of Craven [41] for the groups with $T = F_4(q)$ or $E_6^{\varepsilon}(q)$. For the groups with $T = E_7(q)$ or $E_8(q)$, there is a short list of candidates of maximal subgroups in (v) (for example, see [42] for $E_7(q)$).

2.2.4 Conjugacy classes

The conjugacy classes in S_n and A_n are well-understood. Indeed, it is easy to show that the conjugacy classes of S_n are determined by the cycle type of elements. Moreover, the conjugacy class of an even permutation of S_n splits into two equal size conjugacy classes of A_n if and only if its cycle type consists of distinct odd integers (see [121, Section 2.3.2]).

If G is an almost simple sporadic group, then the conjugacy classes of G can be read off from its character table, which can be found in the Web ATLAS [123] and accessed computationally via the GAP Character Table Library [12].

Now assume T is a finite simple group of Lie type defined over $\mathbb{F}_q$ of characteristic p, recalling that Inndiag(T) is the group generated by T and its diagonal automorphisms. Let $x \in \mathrm{Inndiag}(T)$ be of order m. The element x is called *semisimple* if $(m,p) = 1$, and it is called *unipotent* if m is a p-power. Roughly speaking, for a classical group with natural module V, the conjugacy classes of semisimple elements are distinguished by the multiset of eigenvalues of an appropriate lift of x in $\mathrm{GL}(V)$ over a suitable field extension of $\mathbb{F}_q$, and the conjugacy classes of unipotent elements are identified by the corresponding Jordan canonical form on V (so they are closely related to the partitions of $n = \dim V$).

In order to apply the probabilistic methods briefly discussed in Chapter 1, we need detailed information on the conjugacy classes of prime order elements in Aut(T). Assume $x \in \mathrm{Aut}(T)$ is of prime order r. If $x \in \mathrm{Inndiag}(T)$, then x is semisimple if $p \neq r$, otherwise x is unipotent. And if $x \notin \mathrm{Inndiag}(T)$, then x is a field, graph or graph-field automorphism (and if x is a graph or graph-field automorphism, then $r \in \{2,3\}$). See [21, Chapter 3] and [60, Section 2.5] for more details.

Estimating $|C_{\mathrm{Inndiag}(T)}(x)|$ for an element $x \in \mathrm{Aut}(T)$ of prime order plays a central role in efficiently applying the probabilistic methods, noting that $|x^G| = |G : C_G(x)|$ for $G \leqslant \mathrm{Aut}(T)$. We refer the reader to [94] and [97] for $|C_{\mathrm{Inndiag}(T)}(x)|$ when x is a unipotent or semisimple element of an exceptional group, respectively. For classical groups, this information is given precisely in [21, Chapter 3].

2.3 Bases and regular orbits

In this section, we introduce the study of base sizes for finite permutation groups.

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group on a finite set Ω of size n. Recall that a *base* for G is a subset of Ω with trivial pointwise stabiliser. Note that any subset of Ω containing a base is also a base, so it is natural to consider the minimal size of a base for G, which is called the *base size* of G and denoted $b(G)$. Equivalently, if G is transitive with point stabiliser H, then $b(G)$ is the smallest number b such that the intersection of some b conjugates of H in G is trivial.

Let us introduce another equivalent definition of $b(G)$. Note that if $\{\alpha_1,\dots,\alpha_c\}$ is a base for G, then the tuple

$$(\alpha_1,\dots,\alpha_c) \in \Omega^c$$

is in a G-regular orbit on Ω^c with respect to the componentwise action of G. Thus, we have

$$b(G) = \min\{c \in \mathbb{N} : G \text{ has a regular orbit on } \Omega^c\}.$$

Let $\mathrm{reg}(G)$ be the number of regular G-orbits on $\Omega^{b(G)}$, noting that $\mathrm{reg}(G) \geqslant 1$. Determining $\mathrm{reg}(G)$ is interesting in its own right, and it also arises naturally in the study of base sizes of groups with product action structures (for example, see Theorem 6.2.6). In this thesis, we will also be interested in determining the groups attaining the extremal case where $\mathrm{reg}(G) = 1$ (see Section 3.3.2 for details).

Example 2.3.1. Suppose $G = \mathrm{Sym}(\Omega)$ with $\Omega = [n]$, $n \geqslant 2$. Let Δ be a subset of Ω. Clearly, if $|\Delta| = n-1$ then Δ is a base for G. Moreover, if $|\Delta| \leqslant n-2$ then there is a transposition in G interchanging a pair of points in $\Omega \setminus \Delta$, which fixes Δ pointwise and so Δ is not a base. This gives $b(G) = n-1$, and since G is $(n-1)$-transitive (that is, G is transitive on the set of $(n-1)$-tuples of distinct elements in Ω), we have $\mathrm{reg}(G) = 1$.

Example 2.3.2. Let V be a finite vector space, $\Omega = V \setminus \{0\}$ and $G = \mathrm{GL}(V)$ is the general linear group. Then a subset Δ of Ω is a base for G if and only if Δ spans the vector space V. In particular, we have $b(G) = \dim V$, and one can see that $\mathrm{reg}(G) = 1$ (since G act transitively on the set of bases for V).

Example 2.3.3. Let $G = D_{2n}$ be a dihedral group with $n \geqslant 3$, and consider its natural action on the set Ω of n points, which we identify with the set of vertices of a regular n-gon. Here a point stabiliser is of order 2, which is generated by a reflection of the n-gon. With this observation, we see that any pair of adjacent vertices of the n-gon form a base for G of size 2, and so $b(G) = 2$ (note that $b(G) = 1$ if and only if G has a regular orbit, which is not the case here). One can compute that $\mathrm{reg}(G) = \lceil \frac{n}{2} \rceil - 1$.

Note that for a base Δ for G, there is a one-to-one correspondence between the elements of G and the pointwise images of Δ under G. This observation yields an upper bound $|G| \leqslant n^{b(G)}$, which in turn gives $b(G) \geqslant \log_n |G|$. At the other end of this spectrum, it is not difficult to see that $b(G) \leqslant \log|G|$ as

$$G > G_{\alpha_1} > G_{(\alpha_1,\alpha_2)} > \cdots > G_{(\alpha_1,\ldots,\alpha_{b(G)})} = 1,$$

where $\{\alpha_1, \ldots, \alpha_{b(G)}\}$ is a base for G. In general, however, determining $b(G)$ is a difficult problem and there are no efficient algorithms for computing $b(G)$, or for constructing a base of minimal size. Indeed, Blaha [7] proves that determining whether G has a base of size at most a given constant is an NP-complete problem.

The study of base sizes for primitive groups has a long history, stretching all the way back to the nineteenth century, and this remains a very active area of research. The earliest result in this direction might be work of Bochert in 1889 [8], which shows that $b(G) \leqslant n/2$ if G is a primitive group not containing A_n. Improvements to this bound have been made since then, especially after CFSG and in terms of the O'Nan-Scott theorem. For example, Halasi et al. [67] show that

$$b(G) \leqslant 2\log_n |G| + 24$$

for every primitive group G of degree n, and the multiplicative constant 2 is best possible.

Recall that the O'Nan-Scott theorem divides the finite primitive groups into five families as described in Table 2.1. Let us briefly discuss the work on base sizes for each family in turn.

First assume $G = VH = \mathrm{AGL}(V)$ is affine. In this setting, Halasi and Podoski [68] show that $b(G) \leqslant 3$ in the so-called coprime setting with $(|V|, |H|) = 1$, and Seress [110] shows that $b(G) \leqslant 4$ if H is soluble (both bounds are best possible). The case where H is quasisimple (that is, $H/Z(H)$ is non-abelian simple and H is a perfect group) has been studied extensively, and the problem of determining the exact base size has been reduced to the case where $H/Z(H)$ is a simple group of Lie type defined over a field of characteristic p, where p divides $|V|$. We refer the reader to [83, 84] and the references therein for further details.

Now we turn to the almost simple primitive groups G with socle T. Roughly speaking, such a group is said to be *standard* if $T = A_m$ and Ω is a set of subsets or partitions of $\{1, \ldots, m\}$, or T is a classical group and Ω is a set of subspaces of the natural module for T, otherwise G is *non-standard* (see [19, Definition 1] for the formal definition). The base size of a standard group can be arbitrarily large. For example, if $G = \mathrm{PGL}_n(q)$ and Ω is the set of 1-dimensional subspaces of $\mathbb{F}_q^n$, then $b(G) = n + 1$. For a non-standard group G, a conjecture of Cameron [33, p. 122] asserts that $b(G) \leqslant 7$, with equality if and only if $G = \mathrm{M}_{24}$ in its natural action of degree 24. This conjecture was proved in a sequence of papers by Burness et al. [19, 23, 28, 30]. In addition, the precise base sizes of all primitive groups with sporadic socle are computed in [30, 104]. Recently, the base sizes of alternating and symmetric groups acting on subsets are determined in

[43] and [101], independently. By combining with earlier results [23, 103], this means that the exact base sizes of all primitive actions of alternating and symmetric groups are known.

Partial results on the base sizes of twisted wreath products are given in [50]. For example, it is shown that if $G = T^k{:}P$ is a primitive twisted wreath product as in type V of Table 2.1, then $b(G) = 2$ if P is primitive on $[k]$. More generally, the main results in [50] determine $b(G)$ for primitive twisted wreath products up to three possibilities.

The only family of primitive groups in the O'Nan-Scott theorem for which the precise base size has been calculated in every case is the family of diagonal type groups (type III of Table 2.1). The result is stated as Theorem A in Chapter 1, which is Theorem 3 of my paper [71], and a proof will be given in Chapter 5. This extends an earlier work of Fawcett [51] (see Theorem 5.2.3 in Chapter 5).

Finally, as mentioned in Chapter 1, there are very few results in the literature on calculating $b(G)$ when G is a product type primitive group (type IV in Table 2.1). We will discuss these groups in Chapter 6.

2.4 Probabilistic method

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group on a finite set Ω with point stabiliser H. Here we recall a powerful probabilistic approach for bounding the base size of G, which was originally introduced by Liebeck and Shalev [96] in their proof of a conjecture of Cameron and Kantor on bases for almost simple primitive groups.

Fix a positive integer c and let $Q(G,c)$ be the probability that a randomly chosen c-tuple of points in Ω does not form a base for G. That is,

$$Q(G,c) = \frac{|\{(\alpha_1,\dots,\alpha_c) \in \Omega^c : \bigcap_i G_{\alpha_i} \neq 1\}|}{|\Omega|^c} \tag{2.4.1}$$

and we note that $b(G) \leqslant c$ if and only if $Q(G,c) < 1$. Clearly, a c-tuple $(\alpha_1,\dots,\alpha_c)$ of points in Ω is not a base for G if and only if there exists an element $x \in G$ of prime order fixing each α_i. Now the probability that x fixes a randomly chosen element of Ω is given by the *fixed point ratio*

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

where $C_\Omega(x)$ is the set of fixed points of x on Ω and the second equality is [91, Lemma 2.5], whence

$$Q(G,c) \leqslant \sum_{x \in \mathscr{P}} \mathrm{fpr}(x)^c = \sum_{i=1}^{k} |x_i^G| \cdot \mathrm{fpr}(x_i)^c =: \widehat{Q}(G,c), \tag{2.4.2}$$

where $\mathscr{P} = \bigcup_i x_i^G$ is the set of elements of prime order in G.

To implement this approach, one needs detailed information on the conjugacy classes of elements of prime order in both G and H, as well as an understanding of the fusion (or containment) of H-classes in G. Moreover, the fixed point ratios of elements of prime order for almost simple groups have been extensively studied for many years, and this is the main ingredient for effectively applying the probabilistic method. For example, for an almost simple group G of Lie type defined over $\mathbb{F}_q$, a result of Liebeck and Saxl [91] asserts that $\mathrm{fpr}(x) \leqslant \frac{4}{3q}$ for all non-trivial elements $x \in G$, with a small list of known exceptions. We refer the reader to [15–18, 22, 82, 96] for more work on estimating the fixed point ratios for prime order elements of almost simple groups.

Additionally, we will apply this method to study the base sizes of some diagonal type primitive groups in Section 5.4.2.

In fact, by bounding $Q(G,c)$ for $c = b(G)$, one can also obtain a lower bound on $\mathrm{reg}(G)$, noting that

$$Q(G,b(G)) = 1 - \frac{\mathrm{reg}(G)|G|}{|\Omega|^{b(G)}}.$$

In particular, $\mathrm{reg}(G) \geqslant 2$ if

$$|\Omega|^{b(G)}(1-\widehat{Q}(G,b(G))) > |G|.$$

We conclude by presenting the following elementary result ([19, Lemma 2.1]), which is a useful tool for estimating $\widehat{Q}(G,c)$.

Lemma 2.4.1. *Suppose $x_1,\ldots,x_m$ represent distinct G-classes such that $\sum_i |x_i^G \cap H| \leqslant A$ and $|x_i^G| \geqslant B$ for all i. Then*

$$\sum_{i=1}^{m} |x_i^G| \cdot \mathrm{fpr}(x_i)^c \leqslant B(A/B)^c$$

for every positive integer c.

CHAPTER 3

SAXL GRAPHS

In this chapter, we discuss the Saxl graphs of permutation groups. This concept was first introduced by Burness and Giudici in [20]. Here and throughout the thesis, a permutation group $G \leqslant \mathrm{Sym}(\Omega)$ is called *base-two* if $b(G) = 2$.

Definition. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a base-two permutation group. Then the *Saxl graph* $\Sigma(G)$ is defined to be the graph with vertex set Ω, and two vertices are adjacent if they form a base for G.

We will start by recalling some of the basic properties of Saxl graphs in Section 3.1, and we will then generalise this concept in Section 3.2. In this thesis, we will focus on three main problems concerning the generalised Saxl graphs of primitive groups, which will be presented and discussed in Section 3.3.

3.1 Preliminaries

Throughout this section, let $G \leqslant \mathrm{Sym}(\Omega)$ be a base-two transitive group with point stabiliser H and let $\Sigma(G)$ be the Saxl graph of G.

Let us start with some basic properties of Saxl graphs recorded in [20, Lemma 2.1]. Recall that a permutation group is *Frobenius* if it is not regular and no non-trivial element fixes more than one point.

Lemma 3.1.1. *The following properties hold.*

(i) $G \leqslant \mathrm{Aut}(\Sigma(G))$ *acts transitively on the set of vertices of* $\Sigma(G)$*. In particular,* $\Sigma(G)$ *is G-vertex-transitive.*

(ii) $\Sigma(G)$ *is connected if G is primitive.*

(iii) *$\Sigma(G)$ is complete if and only if G is Frobenius.*

(iv) *$\Sigma(G)$ has valency $r(G)|H|$, where $r(G)$ is the number of regular suborbits of G.*

Recall that an *orbital* of G is a G-orbit on Ω^2, and it is called *regular* if it has size $|G|$. An *orbital graph* of G is a graph with vertices Ω and (α,β) is a directed edge if it is contained in a fixed orbital of G. Note that an orbital graph of G is G-arc-transitive, and G has $r(G)$ distinct regular orbital graphs. The following is deduced from the observation in [20, Remark 2.2].

Lemma 3.1.2. *The Saxl graph $\Sigma(G)$ is the union of all the regular orbital graphs of G. In particular, $\Sigma(G)$ is G-arc-transitive if and only if $r(G) = 1$.*

Recall from (2.4.1) that $Q(G,2)$ is the probability that a random pair of points in Ω is not a base for G. Observe that

$$Q(G,2) = 1 - \frac{\mathrm{val}(G)}{|\Omega|} = 1 - \frac{r(G)|H|}{|\Omega|}, \tag{3.1.1}$$

where $\mathrm{val}(G)$ is the valency of $\Sigma(G)$.

Next, we record [20, Lemma 3.6]. Recall that the *clique number* of a graph is the maximal size of a complete subgraph, and a graph is *Hamiltonian* if it contains a cycle that visits every vertex exactly once.

Lemma 3.1.3. *Let G and H be as above, and let*

$$t := \max\{m \in \mathbb{N} : Q(G,2) < 1/m\}.$$

If $t \geqslant 2$, then $\Sigma(G)$ has the following properties:

(i) *any t vertices in $\Sigma(G)$ have a common neighbour;*

(ii) *every edge in $\Sigma(G)$ is contained in a complete subgraph of size $t+1$;*

(iii) *the clique number of $\Sigma(G)$ is at least $t+1$;*

(iv) *$\Sigma(G)$ is connected with diameter at most 2;*

(v) *$\Sigma(G)$ is Hamiltonian.*

We refer the reader to [20] for a number of examples of Saxl graphs. Here we record one of them to conclude this section.

Example 3.1.4. Let $G = \mathrm{PGL}_2(q)$ with $q \geqslant 4$, and consider the action of G on the set Ω of distinct pairs of 1-dimensional subspaces of $\mathbb{F}_q^2$. Fix a point $\alpha \in \Omega$, so $G_\alpha \cong D_{2(q-1)}$ is a $\mathscr{C}_2$-subgroup of G (see Table 2.5), which is maximal unless $q = 5$. As noted in [20, Example 2.5], we see that a point $\beta \in \Omega$ is in a regular G_α-orbit if and only if $|\alpha \cap \beta| = 1$. It follows that the Saxl graph

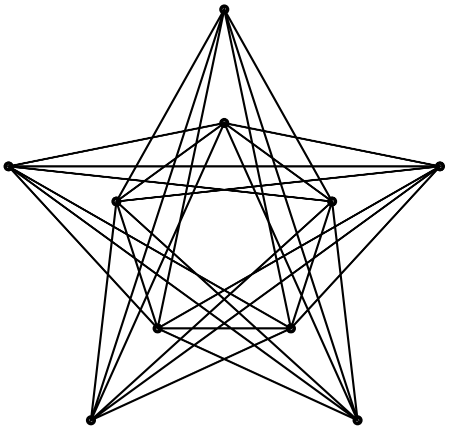

Figure 3.1: The Saxl graph $\Sigma(G)$ with $G = \mathrm{PGL}_2(4) \cong A_5$ and $G_\alpha \cong D_6$

$\Sigma(G)$ is isomorphic to the *Johnson graph* $J(q+1,2)$; the vertices of this graph correspond to the 2-element subsets of a set of size $q+1$, with two vertices joined by an edge if they have non-empty intersection. For example, if $q = 4$ then $\Sigma(G)$ is isomorphic to the complement of the *Petersen graph* as shown in Figure 3.1. In particular, we have $r(G) = 1$ and this graph is G-arc-transitive. Even though

$$Q(G,2) = 1 - \frac{\mathrm{val}(G)}{|\Omega|} = 1 - \frac{4(q-1)}{q(q+1)} \to 1 \text{ as } q \to \infty,$$

$\Sigma(G)$ still has the property that any two vertices have a common neighbour, which can be seen immediately from the isomorphism $\Sigma(G) \cong J(q+1,2)$.

3.2 Generalised Saxl graphs

The work in this section is selected from the preprint [52], which is

> S.D. Freedman, H.Y. Huang, M. Lee and K. Rekvényi, *On the generalised Saxl graphs of permutation groups*, submitted (2024), arXiv:2410.22613.

Note that the definition of the Saxl graph is restricted to the base-two groups. It is natural to seek a more general definition of the Saxl graph, which can be defined for an arbitrary permutation group with base size at least 2.

Definition 3.2.1. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group with $b(G) \geqslant 2$. Then the *generalised Saxl graph* of G, denoted $\Sigma(G)$, is the graph with vertex set Ω, and two vertices α and β are adjacent if and only if $\{\alpha,\beta\}$ is a subset of a base for G of size $b(G)$.

Note that this definition coincides with that of the Saxl graph when $b(G) = 2$. For the remainder of this thesis, we will use $\Sigma(G)$ to denote the *generalised Saxl graph* of G.

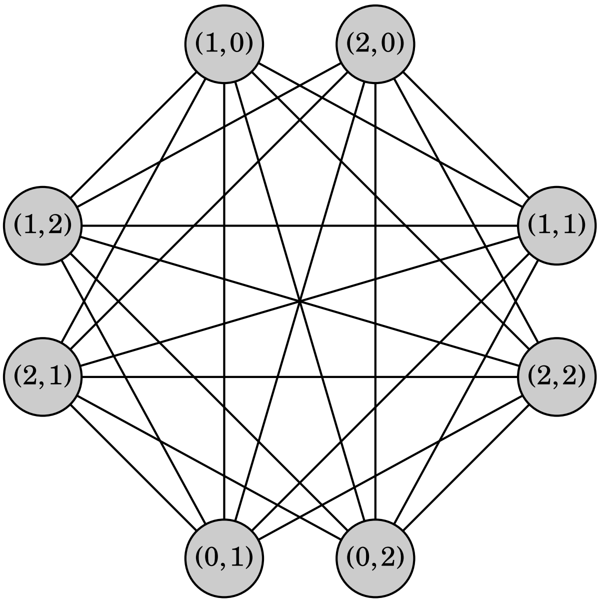

Figure 3.2: The graph $\Sigma(G)$ when $G = \mathrm{GL}_2(3)$ and $\Omega = \mathbb{F}_3^2 \setminus \{0\}$

Example 3.2.2. Let $G \leqslant \mathrm{Sym}(\Omega)$ with $G = \mathrm{GL}(V)$ and $\Omega = V \setminus \{0\}$, where V is a finite vector space. As noted in Example 2.3.2, we have $b(G) = \dim V$ and a subset Δ of Ω is a base of size $b(G)$ if and only if Δ is a basis for the vector space V. With this observation, we see that $\Sigma(G)$ is a complete multipartite graph, with each part corresponding to a 1-dimensional subspace of V (excluding the zero vector). For example, if $V = \mathbb{F}_3^2$ then $\Sigma(G)$ is shown as Figure 3.2.

The following lemma is the analogue of parts (i) and (ii) of Lemma 3.1.1 for the generalised Saxl graphs we are considering here.

Lemma 3.2.3. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group with $b(G) \geqslant 2$. Then the following properties hold.*

(i) $G \leqslant \mathrm{Aut}(\Sigma(G))$ acts transitively on the set of vertices of $\Sigma(G)$. In particular, $\Sigma(G)$ is G-vertex-transitive.

(ii) $\Sigma(G)$ is connected if G is primitive.

Proof. Part (i) is given by the fact that Δ is a base if and only if Δ^g is a base for $g \in G$. Assume G is primitive and let C be a connected component of $\Sigma(G)$. Note that C^G is a block system of Ω, and hence $|C| = 1$ or $C = \Omega$ by the primitivity of G. The former implies that $\Sigma(G)$ is an empty graph, which is clearly impossible by the definition of $\Sigma(G)$. ■

However, the statement of part (iii) of Lemma 3.1.1 does not hold for the generalised Saxl graph $\Sigma(G)$ when $b(G) > 2$. In fact, it turns out that the problem of classifying the groups G such that $\Sigma(G)$ is a complete graph (when $b(G) > 2$) is challenging. We will return to this in Section 3.3.3.

Now assume G is transitive, so $\Sigma(G)$ is G-vertex-transitive by Lemma 3.2.3(i). Let $\mathrm{val}(G)$ be the valency of $\Sigma(G)$. Recall from Lemma 3.1.1(iv) that $\mathrm{val}(G) = r(G)|G_\alpha|$ when $b(G) = 2$. When $b(G) > 2$, it is not easy to describe $\mathrm{val}(G)$, although we have the following bound. Recall that $Q(G,c)$ is the probability that a random c-tuple of Ω is not a base for G (see (2.4.1)).

Lemma 3.2.4. *We have*

$$1 - Q(G, b(G)) \leqslant \left(\frac{\mathrm{val}(G)}{|\Omega|}\right)^{b(G)-1}.$$

Proof. Let $k = b(G)$. Since G acts transitively on Ω, every element of Ω is contained in the same number of bases of size k. Hence,

$$\begin{aligned} 1 - Q(G,k) &= \frac{|\{(\alpha_1,\dots,\alpha_k) \in \Omega^k : \bigcap G_{\alpha_i} = 1\}|}{|\Omega|^k} \\ &= \frac{|\{(\alpha_2,\dots,\alpha_k) \in \Omega^{k-1} : \bigcap_{i=1}^k G_{\alpha_i} = 1\}|}{|\Omega|^{k-1}}, \end{aligned}$$

with $\alpha_1 \in \Omega$ fixed in this final expression. Now, the set of elements of Ω that appear in a tuple in

$$\left\{(\alpha_2,\dots,\alpha_k) \in \Omega^{k-1} : \bigcap_{i=1}^{k} G_{\alpha_i} = 1\right\}$$

has size $\mathrm{val}(G)$, which gives the required inequality. ∎

Recall that $\mathrm{reg}(G)$ is the number of regular G-orbits on $\Omega^{b(G)}$, with respect to the componentwise action of G. In particular, $\mathrm{reg}(G) \geqslant 1$, and $\mathrm{reg}(G) = r(G)$ is the number of regular suborbits of G if $b(G) = 2$. Recall from Lemma 3.1.2 that if $b(G) = 2$, then $\Sigma(G)$ is G-arc-transitive if and only if $\mathrm{reg}(G) = 1$. In general, however, only one direction of this statement holds.

Lemma 3.2.5. *If* $b(G) \geqslant 2$ *and* $\mathrm{reg}(G) = 1$*, then* $\Sigma(G)$ *is* G*-arc-transitive.*

Proof. If $b(G) = 2$ then this is given by Lemma 3.1.2, so we may assume $b(G) \geqslant 3$. Suppose (α_1,α_2) and (β_1,β_2) are arcs in $\Sigma(G)$. Then there exist points $\alpha_3,\dots,\alpha_{b(G)}$ and $\beta_3,\dots,\beta_{b(G)}$ in Ω such that $\{\alpha_1,\dots,\alpha_{b(G)}\}$ and $\{\beta_1,\dots,\beta_{b(G)}\}$ are bases for G. In other words, the tuples

$$(\alpha_1,\dots,\alpha_{b(G)}),(\beta_1,\dots,\beta_{b(G)}) \in \Omega^{b(G)}$$

are in regular G-orbits. Now the condition $\mathrm{reg}(G) = 1$ implies that

$$(\alpha_1,\dots,\alpha_{b(G)})^g = (\beta_1,\dots,\beta_{b(G)})$$

for some $g \in G$, and hence $(\alpha_1,\alpha_2)^g = (\beta_1,\beta_2)$, which completes the proof. ∎

It is worth noting that the converse of Lemma 3.2.5 does not hold in general if $b(G) > 2$. Indeed, if G is 2-transitive, then $\Sigma(G)$ is G-arc-transitive, while $\mathrm{reg}(G) = 1$ if and only if G is sharply $b(G)$-transitive. As another example, if G is the primitive group $\mathrm{L}_3(4)$ of degree 56, then $b(G) = 3$ and $\Sigma(G)$ is G-arc-transitive, whereas $\mathrm{reg}(G) = 4$.

Now we turn to an extension of Lemma 3.1.3.

Lemma 3.2.6. *Let G be a transitive group with $b := b(G) \geqslant 2$, and set*

$$t := \max\{m \in \mathbb{N} : Q(G,b) < 1/m\}.$$

Additionally, let $r := \max\{t, (b-1)(t-1)\}$. If $r \geqslant 2$, then the following properties hold:

(i) Any r vertices in $\Sigma(G)$ have a common neighbour.

(ii) Every edge in $\Sigma(G)$ is contained in a complete subgraph of size $r+1$.

(iii) The clique number of $\Sigma(G)$ is at least $r+1$.

(iv) $\Sigma(G)$ is connected with diameter at most 2.

(v) $\Sigma(G)$ is Hamiltonian.

Proof. We proceed as in the proof of [20, Lemma 3.6]. If $Q(G,b) < 1/t$, then

$$|\Omega|(1-1/t)^{1/(b-1)} < \mathrm{val}(G)$$

by Lemma 3.2.4. Now $(1-1/t)^{1/(b-1)} \geqslant 1 - \frac{1}{(b-1)(t-1)}$ since, for $t \geqslant 2$,

$$\left(1 - \frac{1}{(b-1)(t-1)}\right)^{b-1} \leqslant e^{-(t-1)} \leqslant 1 - \frac{1}{t-1} + \frac{1}{2(t-1)^2} \leqslant 1 - \frac{1}{t}.$$

Hence $\mathrm{val}(G) > |\Omega|(1-\frac{1}{r})$. This implies that for any r vertices in $\Sigma(G)$, the neighbourhoods of those vertices have a non-empty common intersection. That is, those vertices have a common neighbour. This gives (i), and since $r \geqslant 2$, parts (ii)–(iv) follow directly. Finally, since $\mathrm{val}(G) > |\Omega|/2$, Dirac's theorem (see [46, Theorem 3]) yields (v). ■

We conclude this section by recording the following trivial observation.

Lemma 3.2.7. *If $K \leqslant G$ and $b(K) = b(G)$, then $\Sigma(G)$ is a subgraph of $\Sigma(K)$.*

Proof. If Δ is a base for G, then Δ is also a base for K. ■

3.3 Problems

In this section, we discuss the three main problems concerning the generalised Saxl graphs that will be considered in this thesis, namely Conjecture II and Problems III and IV, as briefly described in Chapter 1. Throughout, let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group with $b(G) \geqslant 2$ and point stabiliser H, and let $\Sigma(G)$ be the generalised Saxl graph of G.

3.3.1 Common Neighbour Conjecture

We define the following property of $\Sigma(G)$:

($\star$) *Any two vertices in $\Sigma(G)$ have a common neighbour.*

Remark 3.3.1. Property ($\star$) implies that $\Sigma(G)$ has diameter at most 2. In addition, if $b(G) \geqslant 3$, then the definition of $\Sigma(G)$ implies that any two adjacent vertices have a common neighbour. Thus, for the groups with $b(G) \geqslant 3$, property ($\star$) holds if and only if $\Sigma(G)$ has diameter at most 2.

It was conjectured by Burness and Giudici that any base-two primitive group G satisfies property ($\star$) (see [20, Conjecture 4.5]). This has been verified in some special cases. For example, if G is a non-standard group (recall this definition from Section 2.3) with socle A_n, then [20, Theorem 5.1] shows that G satisfies the property ($\star$). It has been verified in my joint paper [27] with Burness that the conjecture holds if G is a base-two almost simple primitive group with soluble point stabilisers, or with socle $\mathrm{L}_2(q)$ (the latter extends an earlier result of Chen and Du [36]). These results will be discussed in Chapter 4 (with regard to the more general Conjecture 3.3.2, stated below). More recently, partial evidence of this conjecture has been given for affine groups in [85].

In my joint paper [52], we conjecture that property ($\star$) also holds for any primitive group G with $b(G) \geqslant 3$. This is stated as Conjecture II in Chapter 1.

Conjecture 3.3.2. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group with $b(G) \geqslant 2$. Then G satisfies property ($\star$).*

In this thesis, we will show that Conjecture 3.3.2 holds in several cases. More specifically, we will establish Theorem C stated in Chapter 1, which verifies this conjecture for some almost simple groups. Partial results for diagonal type groups and twisted wreath products will be given in Chapter 5 (see Theorems 5.6 and 5.9.1).

Moreover, by considering the bases for primitive wreath products, we will show in Chapter 6 that Conjecture 3.3.2 is equivalent to the following (a priori, stronger) statement. Here, as will be defined in Definition 6.5.5 in Section 6.5.2, an orbit O of G_α is called *almost-regular* if $O \cap \Delta \neq \emptyset$ for some base Δ for G of size $b(G)$ that contains α, and $N(\alpha)$ is the set of neighbours of α in $\Sigma(G)$ (which is exactly the union of the almost-regular G_α-orbits).

Conjecture 3.3.3. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group with $b(G) \geqslant 2$. Then for any $\alpha, \beta \in \Omega$, the $\Sigma(G)$-neighbourhood $N(\beta)$ meets every almost-regular G_α-orbit.*

In particular, when $b(G) = 2$, Conjecture 3.3.3 asserts that the union of regular G_β-orbits meets every regular G_α-orbit.

3.3.2 Arc-transitivity

Now we discuss the following problem, which is stated as Problem III in Chapter 1.

Problem 3.3.4. *Classify the primitive groups G such that $\Sigma(G)$ is G-arc-transitive.*

Recall that $\mathrm{reg}(G)$ is the number of regular G-orbits on $\Omega^{b(G)}$, and we have $\mathrm{reg}(G) \geqslant 1$ by definition. By Lemma 3.2.5, if $\mathrm{reg}(G) = 1$ then $\Sigma(G)$ is G-arc-transitive, and the converse holds true if $b(G) = 2$ (see Lemma 3.1.2). With this observation, we are also interested in the following special case of Problem 3.3.4.

Problem 3.3.5. *Classify the primitive groups G with* $\mathrm{reg}(G) = 1$.

A basic observation yields the following lemma.

Lemma 3.3.6. *If* $\mathrm{reg}(G) = 1$*, then*

$$Q(G, b(G)) = 1 - \frac{|G|}{|\Omega|^{b(G)}}.$$

This naturally brings into play the probabilistic method introduced in Section 2.4, noting that $\mathrm{reg}(G) \geqslant 2$ if $Q(G, b(G))$ is "small".

In this direction, we will establish Theorems D and E in Chapters 5 and 4, respectively. We will also prove Theorem 5.9.2 in Chapter 5 for primitive twisted wreath products.

3.3.3 Completeness

Our third and final main problem on the generalised Saxl graphs of primitive groups concerns their completeness, stated as Problem IV in Chapter 1.

Problem 3.3.7. *Classify the primitive groups G such that $\Sigma(G)$ is a complete graph.*

We say a group G is *semi-Frobenius* if $\Sigma(G)$ is a complete graph (that is, any two elements of Ω lie in a common base for G of size $b(G)$). In particular, G is Frobenius if and only if $b(G) = 2$ and G is semi-Frobenius. It is not difficult to see that any 2-transitive group is semi-Frobenius. Moreover, we have the following observation.

Lemma 3.3.8. *The group G is 2-transitive if and only if G is semi-Frobenius and $\Sigma(G)$ is G-arc-transitive.*

Now let us discuss more examples of semi-Frobenius groups.

Example 3.3.9. A tuple $(\alpha_1,\dots,\alpha_k)$ of Ω is said to be an *irredundant base* for G if

$$G_{\alpha_1} > G_{(\alpha_1,\alpha_2)} > \cdots > G_{(\alpha_1,\dots,\alpha_{k-1})} > G_{(\alpha_1,\dots,\alpha_k)} = 1.$$

In particular, if $(\alpha_1,\dots,\alpha_k)$ is an irredundant base then $k \geqslant b(G)$. Conversely, $(\alpha_1,\dots,\alpha_k)$ is an irredundant base if $k = b(G)$ and $\{\alpha_1,\dots,\alpha_k\}$ is a base. The group G is called *IBIS* (Irredundant Bases of Invariant Size) if every irredundant base has size $b(G)$. This concept was first introduced by Cameron and Fon-Der-Flaass [34]. Note that if G is a primitive group with $b(G) \geqslant 2$, then for any two distinct elements $\alpha_1,\alpha_2 \in \Omega$ we have $G_{\alpha_1} \neq G_{\alpha_2}$, and so there exist an integer k and elements $\alpha_3,\dots,\alpha_k \in \Omega$ such that $(\alpha_1,\dots,\alpha_k)$ is an irredundant base. Therefore, G is semi-Frobenius if G is a primitive IBIS group (for example, the actions of S_6 of degrees 10 and 15).

Example 3.3.10. Let T be a non-abelian finite simple group and let $G = \mathrm{Hol}(T) = T{:}\mathrm{Aut}(T)$ be the *holomorph* of T, which acts faithfully and primitively on T (see Section 5.3 for more details). Then as noted in the proof of Proposition 3.10 in [51], we see that $b(G) = 3$ and $\{1,x,y\}$ is a base for G if $\langle x,y\rangle = T$. Thus, G is semi-Frobenius since any non-identity element of T is contained in a generating pair by a theorem of Guralnick and Kantor [63].

Example 3.3.11. Let $G = S_m$ with $m \geqslant 5$, and let Ω be the set of 2-subsets of $\{1,\dots,m\}$. Note that G is primitive. If $m \in \{5,6\}$ then it is easy to see that G is semi-Frobenius, and we will show that G is also semi-Frobenius if $m \geqslant 7$. Let $\alpha = \{1,2\}$, $\beta = \{1,3\}$ and $\gamma = \{3,4\}$. By the 2-transitivity of G on $\{1,\dots,m\}$, it suffices to show that $\{\alpha,\beta\}$ and $\{\alpha,\gamma\}$ are edges in $\Sigma(G)$.

To see this, suppose Δ is a base of minimal size that contains α. Then there exists $\beta' \in \Delta$ such that $\alpha \cap \beta' \neq \emptyset$, otherwise $(1,2)$ fixes Δ pointwise, which is incompatible with our assumption that Δ is a base. Thus, $\{\alpha,\beta'\}$ is an edge in $\Sigma(G)$, and the 2-transitivity of G on $\{1,\dots,m\}$ implies that $\{\alpha,\beta\}$ is also an edge.

To prove that $\{\alpha,\gamma\}$ is an edge in $\Sigma(G)$, we only need to show that there exists $\gamma' \in \Delta$ such that $\alpha \cap \gamma' = \emptyset$. We argue by contradiction and assume every element in Δ meets α. Then it is straightforward to see that $|\Delta| \geqslant m-2$. As can be seen easily,

$$\{\{1,2\},\{1,3\},\{4,5\},\{5,6\},\dots,\{m-2,m-1\}\}$$

is a base for G of size $m-3$ (since we assume $m \geqslant 7$). This is a contradiction since Δ is assumed to be a base of minimal size.

We remark that $b(G) = \lceil \frac{2}{3}(m-1) \rceil$ in this setting (see [66, Theorem 3.2]). However, as can be seen above, we are able to show that G is a semi-Frobenius group even without computing the precise base size.

As mentioned in Chapter 1, we will establish Theorem F in Chapter 4, which classifies the primitive semi-Frobenius groups with socle $\mathrm{L}_2(q)$. In addition, partial results on Problem IV for almost simple sporadic groups will be given in Chapter 4, stated as Proposition 4.4.1 (in particular, we will prove that G is semi-Frobenius if $b(G) \geqslant 5$ in this setting). We will also consider Problem IV for diagonal type primitive groups and obtain partial results (see Theorem 5.4).

Chapter 4

Almost simple groups

The work in this chapter is heavily drawn from the papers

> T.C. Burness and H.Y. Huang, *On base sizes for primitive groups of product type*, J. Pure Appl. Algebra **227** (2023), Paper No. 107228, 43 pp.
>
> T.C. Burness and H.Y. Huang, *On the Saxl graphs of primitive groups with soluble stabilisers*, Algebr. Comb. **5** (2022), 1053–1087.
>
> S.D. Freedman, H.Y. Huang, M. Lee and K. Rekvényi, *On the generalised Saxl graphs of permutation groups*, submitted (2024), arXiv:2410.22613.

which are [26], [27] and [52], respectively.

Throughout this chapter, let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive group with socle T and point stabiliser H. Here we will focus on the following three cases in turn:

(a) $T \cong \mathrm{L}_2(q)$;

(b) T is a sporadic simple group;

(c) H is soluble.

The relevant groups will be discussed in Sections 4.3, 4.4 and 4.5, respectively. The results in Section 4.3 are selected from my joint papers [27] with Burness and [52] with Freedman, Lee and Rekvényi, and Section 4.4 comes from the latter paper. Section 4.5 is a combination of relevant results from my joint papers [26, 27] with Burness.

One of our goals in this section is to establish Theorem C concerning Conjecture II (see Theorem 4.2 below). We will also attack Problem III for these groups by establishing Theorems

4.3 and 4.5, the latter is briefly asserted as Theorem E in Chapter 1. In addition, we will consider Problem IV and classify the semi-Frobenius primitive groups with $T = \mathrm{L}_2(q)$ in Theorem 4.6. This is also Theorem F.

4.1 Introduction

Before stating our main results in this chapter, we first discuss the study of base sizes for almost simple primitive groups in cases (a), (b) and (c) above. First, as noted in Section 2.3, the base size of every almost simple primitive group with sporadic socle has been computed in [30] and [104]. Recently, the precise base size of every almost simple primitive group with soluble point stabilisers has been computed by Burness [14]. Hence, we know the exact value of $b(G)$ for every group G in case (b) or (c). Although there are many references giving the exact base size $b(G)$ for many primitive actions of groups G with socle $\mathrm{L}_2(q)$ (for example, [14] when H is soluble), we have not been able to find one for the case where H is of type $\mathrm{GL}_2(q_0)$ with $q_0^2 = q$. Here we will show that $b(G) = 3$ unless $G = \mathrm{P\Sigma L}_2(9)$ (see Proposition 4.3.2), completing the calculation of $b(G)$ for all almost simple primitive groups with socle $\mathrm{L}_2(q)$ by extending earlier results in [14, 19]. Note that in the following theorem, we exclude the groups with socle $\mathrm{L}_2(4)$ as $\mathrm{L}_2(4) \cong \mathrm{L}_2(5)$.

Theorem 4.1. *Let G be a primitive group with socle $T = \mathrm{L}_2(q)$, $q \geqslant 5$ and point stabiliser H. Then $b(G) > 2$ if and only if one of the following holds.*

(i) H is of type P_1, in which case $b(G) \in \{3,4\}$. Furthermore, $b(G) = 3$ if and only if either $G \leqslant \mathrm{PGL}_2(q)$, or $|G:T| = 2$ and $G \not\leqslant \mathrm{P\Sigma L}_2(q)$.

(ii) H is of type $\mathrm{GL}_1(q) \wr S_2$ and $\mathrm{PGL}_2(q) < G$, in which case $b(G) = 3$.

(iii) H is of type $\mathrm{GL}_1(q^2)$ and $\mathrm{PGL}_2(q) \leqslant G$, in which case $b(G) = 3$.

(iv) H is of type $\mathrm{GL}_2(q_0)$ with $q = q_0^2 \geqslant 9$, in which case $b(G) \in \{3,4\}$. Furthermore, $b(G) = 4$ if and only if $G = \mathrm{P\Sigma L}_2(9)$.

(v) $(q,H) \in \{(5,A_4),(7,S_4),(11,A_5),(19,A_5)\}$ and $b(G) = 3$, $(q,H) \in \{(5,S_4),(9,A_5)\}$ and $b(G) = 4$, or $(q,H) = (9,S_5)$ and $b(G) = 5$.

With the precise base sizes in hand, we now turn to the generalised Saxl graph $\Sigma(G)$. Recall the following property

($\star$) *Any two vertices in $\Sigma(G)$ have a common neighbour*

defined in Section 3.3.1. Conjecture II asserts that every primitive permutation group G has this property. We will verify this for all primitive groups with soluble point stabilisers, and we also obtain partial results for groups with socle $\mathrm{L}_2(q)$ or a sporadic group. Here let

$$\mathscr{F} = \{G \ :\ T = \mathrm{L}_2(q),\ q \geqslant 16,\ |G:T| \text{ is even, and } H \text{ is of type } \mathrm{GL}_2(q_0) \text{ with } q_0^2 = q\}$$

be a collection of primitive groups, where T denotes the socle of G, and H is a point stabiliser.

Theorem 4.2. *Let G be an almost simple primitive group with socle T and point stabiliser H. Then G satisfies property $(\star)$ if one of the following holds:*

(i) $T = \mathrm{L}_2(q)$ *and* $G \notin \mathscr{F}$*;*

(ii) *T is a sporadic simple group and* $b(G) \geqslant 3$*;*

(iii) *H is soluble.*

We leave the excluded case (i.e. $G \in \mathscr{F}$) described in Theorem 4.2(i) open. In particular, since that case only occurs when $G > T$, we deduce that Conjecture II holds for all primitive actions of $\mathrm{L}_2(q)$. For partial results towards Conjecture II for base-two almost simple sporadic groups, we refer the reader to [20, Section 6].

Next, we turn to Problem III, which involves determining the groups G such that $\Sigma(G)$ is a G-arc-transitive graph. We are able to resolve this problem for the primitive groups $G \notin \mathscr{F}$ with socle $\mathrm{L}_2(q)$. Note that $\mathrm{L}_2(4) \cong \mathrm{L}_2(5) \cong A_5$ and $\mathrm{L}_2(9) \cong A_6$.

Theorem 4.3. *Let $G \notin \mathscr{F}$ be a primitive group with socle $T = \mathrm{L}_2(q)$ and point stabiliser H. Then $\Sigma(G)$ is G-arc-transitive if and only if one of the following holds:*

(i) *H is of type P_1;*

(ii) *G is 2-transitive and* $(G,H) = (\mathrm{L}_2(11), A_5)$, $(\mathrm{P\Gamma L}_2(8), D_{18}.3)$, $(\mathrm{L}_2(7), S_4)$, (S_6, S_5), (A_6, A_5), (S_5, S_4) *or* (A_5, A_4)*;*

(iii) $G = \mathrm{PGL}_2(q)$, $5 \neq q \geqslant 4$, *and H is of type* $\mathrm{GL}_1(q) \wr S_2$*; or*

(iv) $(G,H) = (\mathrm{L}_2(29), A_5)$, $(\mathrm{PGL}_2(11), S_4)$, $(\mathrm{M}_{10}, 5{:}4)$ *or* (A_5, S_3).

We will also consider Problem 3.3.5 on the groups with $\mathrm{reg}(G) = 1$, recalling that this condition implies that $\Sigma(G)$ is G-arc-transitive, and the converse implication holds if $b(G) = 2$ (see Lemmas 3.2.5 and 3.1.2, respectively). Note that if G is 2-transitive, then $\mathrm{reg}(G) = 1$ if and only if G is sharply $b(G)$-transitive.

Corollary 4.4. *Let $G \notin \mathscr{F}$ be a primitive group with socle $T = \mathrm{L}_2(q)$ and point stabiliser H. Then* $\mathrm{reg}(G) = 1$ *if and only if G is one of the groups in parts (iii) and (iv) of Theorem 4.3, or H is of type P_1 and G is sharply 3-transitive, or* $(G,H) \in \{(S_6,S_5),(A_6,A_5),(S_5,S_4)\}$.

We now turn to the almost simple primitive groups with soluble point stabilisers.

Theorem 4.5. *Let G be an almost simple primitive group with soluble point stabilisers. Then* $\mathrm{reg}(G) = 1$ *if and only if G is one of the groups listed in Table 4.1.*

$b(G)$	G	Type of G_α	Comments
2	$\mathrm{PGL}_2(q)$	$\mathrm{GL}_1(q) \wr S_2$	$q \geqslant 7$, $q \neq 9$
	$\mathrm{P}\Omega_8^+(3).2^2$	$\mathrm{O}_4^+(3) \wr S_2$	Both groups of this shape
	$\Omega_8^+(2).3$	$\mathrm{O}_2^-(2) \times \mathrm{GU}_3(2)$	
	$\mathrm{SO}_7(3)$	$\mathrm{O}_4^+(3) \perp \mathrm{O}_3(3)$	
	$\mathrm{PSp}_6(3)$	$\mathrm{Sp}_2(3) \wr S_3$	
	$\mathrm{PGL}_4(3)$	$\mathrm{O}_4^+(3)$	
	$\mathrm{U}_4(3).[4]$	$\mathrm{GU}_1(3) \wr S_4$	$G \neq T.\langle \delta^2, \phi \rangle$
	$\mathrm{U}_4(3)$	$\mathrm{GU}_2(3) \wr S_2$	
	$\mathrm{L}_3(4).D_{12}$	$\mathrm{GL}_1(4^3)$	
	$\mathrm{L}_3(4).2$	$\mathrm{GU}_3(2)$	$G \neq \mathrm{P\Sigma L}_3(4)$
	$\mathrm{U}_3(5).S_3$	$\mathrm{GU}_1(5) \wr S_3$	
	$\mathrm{U}_3(4)$	$\mathrm{GU}_1(4) \wr S_3$	
	$\mathrm{PGL}_2(11)$	$2_-^{1+2}.\mathrm{O}_2^-(2)$	
	$G_2(3).2$	$\mathrm{SL}_2(3)^2$	
	S_7	$\mathrm{AGL}_1(7)$	
	$\mathrm{PGL}_2(9)$	D_{16}	
	M_{10}	$5{:}4$	
	A_5	D_6	
	$\mathrm{J}_2.2$	$5^2{:}(4 \times S_3)$	
	M_{11}	$2.S_4$	
3	$\mathrm{L}_2(q).2$	P_1	G is sharply 3-transitive
	$\mathrm{L}_2(q)$	P_1	q is even
	$\mathrm{U}_4(3).2$	P_1	$G \not\leqslant \mathrm{PGU}_4(3)$
	$\mathrm{Aut}(\mathrm{L}_3(q))$	$P_{1,2}$	$q \in \{8, 9, 16\}$
	$\mathrm{Aut}(\mathrm{U}_3(q))$	P_1	$q \in \{3, 4, 8\}$
	$\mathrm{L}_2(7)$	$2_-^{1+2}.\mathrm{O}_2^-(2)$	
	S_7	$S_4 \times S_3$	
	$\mathrm{PGL}_2(9)$	$3^2{:}Q_8$	
	M_{10}	$\mathrm{AGL}_1(9)$	
	S_5	$5{:}4$	
	A_5	A_4	
4	$\mathrm{L}_3(3)$	P_1, P_2	
	S_5	S_4	

Table 4.1: The almost simple primitive groups G with G_α soluble and $\mathrm{reg}(G) = 1$

In fact, we will establish a stronger result by classifying the groups with $\mathrm{reg}(G) \leqslant 4$ (see Propositions 4.5.14 and 4.5.19), which will find an application in Chapter 6. See Tables 4.7, 4.8 and 4.9 for the relevant groups. Note that Table 4.1 is generated from these tables, so we refer the reader to Remarks 4.5.15 and 4.5.20 for further comments of the groups recorded in Table 4.1.

Finally, let us discuss Problem IV on the completeness of $\Sigma(G)$. Recall that G is called *semi-Frobenius* if $\Sigma(G)$ is complete, and if $b(G) = 2$ then G is semi-Frobenius if and only if G is Frobenius. Note that there are no almost simple Frobenius groups, and so there are no base-two almost simple semi-Frobenius groups.

In Section 4.3 we will classify the semi-Frobenius primitive groups with socle $\mathrm{L}_2(q)$ in full generality.

Theorem 4.6. *Let G be an almost simple primitive group with socle $T = \mathrm{L}_2(q)$ and point stabiliser H. Then G is semi-Frobenius if and only if one of the following holds:*

(i) *H is of type P_1;*

(ii) *H is of type $\mathrm{GL}_1(q) \wr S_2$ and $\mathrm{PGL}_2(q) < G$;*

(iii) *H is of type $\mathrm{GL}_1(q^2)$ and $\mathrm{PGL}_2(q) \leqslant G$;*

(iv) *$(q,H) \in \{(5,A_4),(5,S_4),(7,S_4),(9,A_5),(9,S_5),(11,A_5),(19,A_5)\}$; or*

(v) *$q = q_0^2$ for some $q_0 \geqslant 3$, H is of type $\mathrm{GL}_2(q_0)$, and either $q_0 = 3$ or $|G:T|$ is odd.*

Equivalently, G is not semi-Frobenius if and only if either $b(G) = 2$, or $G \in \mathscr{F}$.

Probabilistic and computational methods play a key role in the proofs of our main theorems. The probabilistic method has been discussed in Section 2.4, and we will describe our main computational methods in Section 4.2. Relevant MAGMA and GAP code is recorded in Appendix A. As mentioned above, we will treat the groups in cases (a), (b) and (c) in Sections 4.3, 4.4 and 4.5, respectively.

4.2 Computational methods

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive group with point stabiliser H. We will apply computational methods to establish our main results when G is a sporadic group, or a small degree symmetric or alternating group, or a low rank group of Lie type defined over a suitably small field. We mainly use MAGMA V2.26-11 [10] to do the computations, noting that the GAP Character Table Library [12] is an important tool for the analysis of sporadic groups.

4.2.1 Construction of groups

First, let us discuss how we construct the permutation group $G \leqslant \mathrm{Sym}(\Omega)$ in MAGMA.

To do this, we first construct G as a permutation group of an appropriate degree (this is typically the primitive permutation representation of minimal degree, and will not necessarily be the permutation representation of G on Ω). Here we typically use the function `AutomorphismGroupSimpleGroup` to obtain $A = \mathrm{Aut}(T)$ as a permutation group and then we identify G by inspecting the subgroups of A containing T. We then construct H as a subgroup of G in this permutation representation via the function `MaximalSubgroups`, which returns a set of representatives of the G-classes of maximal subgroups of G. Then we use the function `CosetAction` to construct G as a permutation group on Ω, which can be identified with the set of cosets $[G:H]$.

This can be expensive (in terms of time and memory) if $|\Omega|$ is large, so we only apply this method when $|\Omega| < 5 \times 10^6$ (for example, in the proof of Proposition 4.5.19), apart from the groups discussed in Section 4.4, which will be treated separately (see Appendix A.1.2.5, for example).

4.2.2 Calculation of base sizes

Now we explain how to compute $b(G)$ in MAGMA. This requires the construction of $G \leqslant \mathrm{Sym}(\Omega)$ as explained in Section 4.2.1, so $|\Omega| < 5 \times 10^6$.

For an integer i starting from $k := \lceil \log_{|\Omega|} |G| \rceil - 1$ (note that we immediately have $b(G) \geqslant k+1$), we check whether or not G has a base of size $i+1$ (so we stop when we find the first i that works). To determine whether a base of size $i+1$ exists, we iteratively check orbits of point stabilisers until we find a base. More precisely, we first get a set of G-orbit representatives of k-tuples. This can be done by first taking H-orbits, and then taking representatives of these orbits, followed by taking the orbits of two point stabilisers and repeating this process. Then we inspect the $G_{(\alpha_1,\dots,\alpha_k)}$-orbits on Ω for every G orbit representative of k-tuple $(\alpha_1,\dots,\alpha_k)$, and if there is a regular $G_{(\alpha_1,\dots,\alpha_k)}$-orbit then $b(G) = k+1$, otherwise we check $G_{(\alpha_1,\dots,\alpha_k,\beta)}$-orbits for a representative β of each $G_{(\alpha_1,\dots,\alpha_k)}$-orbit, and we repeat until we find a regular orbit.

This method turns out to be very effective if $b(G)$ is not too large (for example, if $b(G) \leqslant 7$). The related MAGMA code will be presented in Appendix A.1.1.

The author thanks Saul Freedman for the MAGMA code, and for his discussion and comments on the computations when working on the joint paper [52].

4.2.3 Bounding $Q(G,c)$

Recall that $Q(G,c)$ is the probability that a random c-tuple of elements in Ω is not a base for G, which has an upper bound $\widehat{Q}(G,c)$ (see (2.4.2)). Estimating $\widehat{Q}(G,c)$ plays an important role in attacking many problems in this thesis. For example, if $\widehat{Q}(G,b(G)) < 1/2$, then $Q(G,b(G)) < 1/2$ and so all the properties (i)–(v) in Lemma 3.2.6 of the generalised Saxl graph $\Sigma(G)$ hold. This was first observed in [20, Section 3] for the groups with $b(G) = 2$. Another aim is to determine the groups with $Q(G,2) \geqslant 1/4$ (this is the content of Theorem 4.5.1, which will be applied to establish Proposition 4.5.14).

It is straightforward to implement an algorithm in MAGMA to compute $\widehat{Q}(G,c)$ precisely, using the functions `ConjugacyClasses` and `IsConjugate` to find a set of representatives of the conjugacy classes in H and to test conjugacy in G, respectively. This allows us to compute $|x^G \cap H|$ for each $x \in H$ of prime order, which is the main step in calculating the contribution to $\widehat{Q}(G,c)$ from the elements in the G-class of x. Note that this approach can be implemented without determining a set of representatives of the conjugacy classes in G, which can be an expensive operation in terms of time and memory. See Appendix A.1.2.3 for the relevant function.

Let us also observe that $\widehat{Q}(G,c)$ can be computed precisely if we have access to the character tables of G and H, in addition to the fusion map from H-classes to G-classes. For example, this approach works well when G is a sporadic group, using the character table data stored in the GAP Character Table Library [12]. This arises in the proofs of Theorem 4.4.4 and Proposition 4.5.5, and we refer the reader to Appendix A.2.1 for the relevant code.

In some cases, it turns out that we can work effectively with a crude bound

$$\widehat{Q}(G,c) \leqslant \widetilde{Q}(G,c) \tag{4.2.1}$$

where the contribution to $\widetilde{Q}(G,c)$ from all the elements in G of order r (for a fixed prime r) with $|x^G| = m$ is given by

$$\frac{1}{m}\left(\sum_{i=1}^{\ell} |y_i^H|\right)^c$$

and $y_1,\ldots,y_\ell$ represent the distinct H-classes of elements of order r with $|y_i^G| = m$. Notice that no `IsConjugate` commands are needed to compute $\widetilde{Q}(G,c)$, which can be a significant saving. This will arise in the proofs of Lemma 4.5.6 and Proposition 4.5.12, and the relevant code is presented in Appendix A.1.2.3.

4.2.4 Regular orbits

In order to establish Propositions 4.5.14 and 4.5.19 in this chapter, we need to calculate $\mathrm{reg}(G)$ for some groups with $b(G) \leqslant 4$.

First assume $b(G) = 2$. Here we use the approach discussed in Section 4.2.1 to construct G as a permutation group (not necessarily on Ω), and then construct H as a subgroup of G in this permutation representation. In a handful of cases (due to the size of G), this approach is ineffective and a different method is needed in order to construct H. For example, we may identify $H = N_G(K)$ for some specific p-subgroup K of G (for instance, see [14, Example 2.4]). As we explain below, there are other ways to compute $r(G) = \mathrm{reg}(G)$ without using the `CosetAction` function.

If $\widehat{Q}(G,2) \geqslant 1/4$ then, in order to establish Theorem 4.5.1, we need to either compute a better upper bound on $Q(G,2)$, or we need to determine $Q(G,2)$ precisely. In view of (3.1.1), it suffices to bound (or compute) the number $r(G)$ of regular suborbits of G. To do this, we work with double cosets (`CosetAction` is too expensive when $|\Omega|$ is large, say $|\Omega| \geqslant 5 \times 10^6$). Indeed, if R is a complete set of (H,H) double coset representatives in G, then

$$r(G) = |\{x \in R : |HxH| = |H|^2\}|. \tag{4.2.2}$$

Similarly, if R_0 is a complete set of (H_0,H) double coset representatives, where $H_0 = H \cap T$, then

$$r(T) = |\{x \in R_0 : |H_0xH| = |H_0||H|\}|.$$

It is straightforward to compute these numbers using Magma. If $|\Omega| = |G : H|$ is not prohibitively large (for example, if $|\Omega| < 10^7$), then we can use the function `DoubleCosetRepresentatives` to determine R and R_0, which then allows us to compute $r(G)$ and $r(T)$. If $|G : H|$ is large, then we may be able to use the `DoubleCosetCanonical` function to identify sufficiently many distinct double cosets of size $|H|^2$ so that the corresponding lower bound on $r(G)$ forces $Q(G,2) < 1/4$ (this will arise in the proofs of Propositions 4.5.11 and 4.5.12, and for the relevant Magma code, see Appendix A.1.2.4). It is straightforward to implement all of these methods in Magma.

In the proof of Proposition 4.5.19 we will also need to compute $\mathrm{reg}(G)$ in a number of cases with $b(G) = 3$ or 4. Fix $\gamma \in \Omega$ and set $H = G_\gamma$. Decompose $\Omega = \Lambda_1 \cup \cdots \cup \Lambda_t$ as a disjoint union of H-orbits and fix $\lambda_i \in \Lambda_i$ and $K_i = H_{\lambda_i}$.

Suppose $b(G) = 3$. Then every regular G-orbit on Ω^3 is represented by an element of the form $(\gamma, \lambda_i, \beta)$, where β is contained in a regular orbit of K_i on Ω. Therefore,

$$\mathrm{reg}(G) = \sum_{i=1}^{t} r_i, \tag{4.2.3}$$

where r_i is the number of regular orbits of K_i on Ω.

Now assume $b(G) = 4$. Fix $i \in \{1,\dots,t\}$. Let $\Lambda_{i,1},\dots,\Lambda_{i,m_i}$ be the orbits of K_i on Ω and for each $j \in \{1,\dots,m_i\}$ set $K_{i,j} = (K_i)_{\omega_j} = H_{\lambda_i} \cap H_{\omega_j}$ for some fixed $\omega_j \in \Lambda_{i,j}$. Notice that every regular G-orbit on Ω^4 is represented by an element of the form $(\gamma, \lambda_i, \omega_j, \beta)$, where β is in a regular orbit of $K_{i,j}$ on Ω. Therefore, if $r_{i,j}$ denotes the number of regular orbits of $K_{i,j}$ on Ω, then

$$\mathrm{reg}(G) = \sum_{i=1}^{t} \sum_{j=1}^{m_i} r_{i,j}. \tag{4.2.4}$$

Once again, we can implement this approach in Magma in order to compute $\mathrm{reg}(G)$. As before, we first construct G and H, and then we work with the function `CosetAction` to construct G as a permutation group on Ω, which then allows us to construct stabilisers and their orbits.

4.2.5 Generalised Saxl graphs

To conclude this section, we discuss the computational methods we will use to handle the problems on the generalised Saxl graph $\Sigma(G)$ of a primitive group G.

First note that $\Sigma(G)$ is G-vertex-transitive since G is transitive (see Lemma 3.2.3(i)). It follows that $\Sigma(G)$ is the union of some orbital graphs of G (recall that an orbital graph of G is a graph with vertices Ω and (α,β) is a directed edge if it is contained in a fixed orbital of G). With this observation in mind, we first obtain a set of G-orbit representatives of pairs of points in Ω that can be extended to a base of size $b(G)$ (the base size is calculated by implementing the approach in Section 4.2.2). This can be obtained via the function `PairsInMinSizeBase` and will be used to check property

($\star$) *Any two vertices in $\Sigma(G)$ have a common neighbour*

using MAGMA via the function `FastMinSizeComNeighbTest`. Both functions will be presented in Appendix A.1.2.1.

Note that G is semi-Frobenius if and only if for each point $\beta \neq \alpha$ in a set of G_α-orbit representatives, the set $\{\alpha,\beta\}$ extends to a base of size $b(G)$. This allows us to use a similar method as described in Section 4.2.2 for iteratively checking each point stabiliser of G_α (up to conjugacy) until a base of size $b(G)$ is found. We refer the reader to Appendix A.1.2.2 for the function `FastMinSizeIsComplete`.

4.3 Two-dimensional linear groups

In this section, we will establish Theorems 4.1, 4.2(i), 4.3 and 4.6. Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive group with socle $T = \mathrm{L}_2(q)$ and point stabiliser H, where $q = p^f \geqslant 5$ for some prime p and integer f. Then H is of one of the following types (recall that the type of H provides an approximate description of the structure of H, which is consistent with its usage in [80]; see Section 2.2.3 for a brief discussion):

(4.3.1) P_1, $2_-^{1+2}.\mathrm{O}_2^-(2)$, A_5, $\mathrm{GL}_2(q_0)$ (where $q = q_0^s$ for some prime s), $\mathrm{GL}_1(q)\wr S_2$, $\mathrm{GL}_1(q^2)$.

4.3.1 Base sizes

We first determine the precise base size of every primitive action of G, focusing on the groups with H of type $\mathrm{GL}_2(q^{1/2})$, which establishes Theorem 4.1. To do so, we require the following technical lemma. In what follows, for an element $t \in \mathbb{F}_q$, we write $\langle t\rangle$ to denote the smallest subfield of $\mathbb{F}_q$ containing t.

Lemma 4.3.1. *Let q be a prime power not equal to 3, and let s be a primitive element of $\mathbb{F}_q$. Then there exists an element $t \in \mathbb{F}_q^\times$ such that:*

(i) if q is even, then $\langle t\rangle = \mathbb{F}_q$ and the polynomial $x^2 + x + t$ is irreducible over $\mathbb{F}_q$;

(ii) if q is odd, then $\langle t^2/s\rangle = \mathbb{F}_q$ and $t^2 + s$ is a (non-zero) square in $\mathbb{F}_q$; and

(iii) if $q \equiv 3 \pmod 4$*, then* $\langle t^2\rangle = \mathbb{F}_q$ *and* t^2+1 *is a (non-zero) square in* $\mathbb{F}_q$.

Proof. We shall write $q = p^f$, with p prime. Suppose first that q is even, and let r be a divisor of f. For $a \in \mathbb{F}_{2^r}$, the polynomial x^2+x+a is reducible over $\mathbb{F}_q$ if and only if there exists $b \in \mathbb{F}_q$ such that $b^2+b=a$. In this case, there are precisely two such elements, namely b and $b+1$. Moreover, x^2+x+a is reducible over $\mathbb{F}_q$ if and only if either x^2+x+a is reducible over $\mathbb{F}_{2^r}$ or $2r \mid f$, and in the latter case x^2+x+a is reducible over $\mathbb{F}_q$ for all $a \in \mathbb{F}_{2^r}$ (the splitting field of x^2+x+a over $\mathbb{F}_{2^r}$ is $\mathbb{F}_{2^{2r}}$ if it is irreducible over $\mathbb{F}_{2^r}$). Note also that since x^2+x+0 is reducible, there are precisely 2^{r-1} elements $a \in \mathbb{F}_{2^r}$ such that x^2+x+a is irreducible over $\mathbb{F}_{2^r}$. Therefore, the number of elements $a \in \mathbb{F}_q^\times$ that lie in a proper subfield of $\mathbb{F}_q$, with x^2+x+a irreducible over $\mathbb{F}_q$, is at most

$$\sum_{\substack{1\leqslant r<f\\ r\mid f}} 2^{r-1} < 2^{f-1}.$$

Therefore, among the 2^{f-1} elements $t \in \mathbb{F}_q$ such that x^2+x+t is irreducible, there exists at least one such that $\langle t\rangle = \mathbb{F}_q$, and hence t satisfies (i).

Now assume q is odd. Since s is not a square in $\mathbb{F}_q$, exactly one of $1+s$ and $s(1+s)=s^2+s$ is a square. Thus some $t \in \{1,s\}$ satisfies (ii). If $q \equiv 3 \pmod 4$, then it follows from [1, Theorem 3.1] and a simple counting argument that the number of squares in the set $\{c^2+1 \mid c \in \mathbb{F}_q^\times\}$ is $(q-3)/4$, which is non-zero since $q>3$. Notice that f is odd, and so $\langle m^2\rangle = \langle m\rangle$ for all $m \in \mathbb{F}_q$. Therefore, the number of squares in $\mathbb{F}_q^\times$ that lie in a proper subfield of $\mathbb{F}_q = \mathbb{F}_{p^f}$ is at most

$$\sum_{\substack{1\leqslant r<f\\ r\mid f}} (p^r-1)/2 < (p^{f-1}-1)/2 < (p^f-3)/4 = (q-3)/4.$$

Thus there exists $t \in \mathbb{F}_q^\times$ such that t^2+1 is a square, and such that $\langle t^2\rangle = \langle t\rangle = \mathbb{F}_q$. Note finally that -1 has no square root in $\mathbb{F}_q$ since $q \equiv 3 \pmod 4$, and so t satisfies (iii). ■

The following is the main original content of Theorem 4.1.

Proposition 4.3.2. *Let* G *be an almost simple primitive group with socle* $T = \mathrm{L}_2(q)$ *and point stabiliser* H *of type* $\mathrm{GL}_2(q_0)$*, with* $q = q_0^2$ *for some* $q_0 \geqslant 3$*. If* $G = \mathrm{P\Sigma L}_2(9)$*, then* $b(G)=4$*, and otherwise* $b(G)=3$.

Proof. It is straightforward to use MAGMA to calculate $b(G)$ in the case $q_0=3$. Assume therefore that $q_0 \geqslant 4$. By [49, p. 354], T has no regular suborbits in its action on the right cosets of $H\cap T$. Therefore, $b(G) \geqslant b(T) \geqslant 3$. Additionally, the maximality of H implies that $G \leqslant \mathrm{P\Sigma L}_2(q)$ (see [11, Table 8.1]). To complete the proof, we will assume that $G = \mathrm{P\Sigma L}_2(q)$ and show that $b(G)=3$. We shall write $q=p^f$, with p prime.

It will be convenient to identify the action of G on the right cosets of H with an equivalent action on certain 1-dimensional subspaces of $\mathbb{F}_{q_0}^4$, corresponding to the isomorphism $T \cong \Omega_4^-(q_0) \cong \mathrm{P\Omega}_4^-(q_0)$ (see [80, Proposition 2.9.1]). To define this action, let s be a primitive element of $\mathbb{F}_{q_0}$, and let Q be a non-degenerate quadratic form of minus type on $V := \mathbb{F}_{q_0}^4$, with polar form β. By [11, Propositions 1.5.39 & 1.5.42] and [80, Proposition 2.5.12], there exists a basis $\{e_1, e_2, e_3, e_4\}$ for V such that the matrix of Q (defined so that the (i,j) entry is equal to $\beta(e_i, e_j)$ if $i < j$, to $Q(e_i)$ if $i = j$, and to 0 otherwise) is

$$M_Q := \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & \zeta & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

if q is even and

$$M_Q := \begin{pmatrix} s/2 & 0 & 0 & 0 \\ 0 & 1/2 & 0 & 0 \\ 0 & 0 & 1/2 & 0 \\ 0 & 0 & 0 & 1/2 \end{pmatrix},$$

if q is odd, where ζ is an arbitrary element of $\mathbb{F}_{q_0}^\times$ such that the polynomial $x^2 + x + \zeta$ is irreducible over $\mathbb{F}_{q_0}$. By Lemma 4.3.1, we may assume that $\langle \zeta \rangle = \mathbb{F}_{q_0}$. The Gram matrix M_β of β is equal to $M_Q + M_Q^T$.

Next, define $\sigma : V \to V$ by

$$\sigma : \sum_{i=1}^{4} a_i e_i \mapsto a_3^2 \zeta e_2 + \sum_{i=1}^{4} a_i^2 e_i,$$

if q is even, and

$$\sigma : \sum_{i=1}^{4} a_i e_i \mapsto a_1^p s^{(p-1)/2} e_1 + \sum_{i=2}^{4} a_i^p e_i,$$

if q is odd. Hence for each positive integer k, the map σ^k is defined by

$$\sigma^k : \sum_{i=1}^{4} a_i e_i \mapsto a_3^{2^k} \sum_{j=0}^{k-1} \zeta^{2^j} e_2 + \sum_{i=1}^{4} a_i^{2^k} e_i,$$

if q is even, and

$$\sigma^k : \sum_{i=1}^{4} a_i e_i \mapsto a_1^{p^k} s^{(p^k-1)/2} e_1 + \sum_{i=2}^{4} a_i^{p^k} e_i,$$

if q is odd. Additionally, $|\sigma| = f$, and σ is induced by an automorphism of the simple derived subgroup $\Omega_4^-(q_0)$ of the isometry group $\mathrm{O}_4^-(q_0)$ of Q (see [21, pp. 58–59]). Slightly abusing notation and denoting this automorphism by σ, we may identify G with $\langle \Omega_4^-(q_0), \sigma \rangle / \langle -I \rangle$, where I is the 4×4 identity matrix (cf. [11, Tables 8.1 & 8.17]). Note that $L := \langle \Omega_4^-(q_0), \sigma \rangle = \langle \sigma \rangle \mathrm{O}_4^-(q_0)$, and that $\langle \sigma \rangle \cap \mathrm{O}_4^-(q_0)$ is generated by $\sigma^{f/2}$. Let Y be a one-dimensional subspace of V and $y \in Y \setminus \{0\}$. We write $Y \in \Delta$ if $Q(y)$ is a non-zero square in $\mathbb{F}_{q_0}$, and $Y \in \overline{\Delta}$ if $Q(y)$ is a non-square. The action of G on the right cosets of H is equivalent to its action on Δ, and also to its action on $\overline{\Delta}$ if q is odd.

Suppose now that q is even, and let $u := e_2$, $v := e_1 + e_2$ and $w := e_3$. Then $Q(u) = Q(v) = 1$ and $Q(w) = \zeta$, and so $\langle u \rangle, \langle v \rangle, \langle w \rangle \in \Delta$. By [11, Lemma 1.5.21], a matrix $A \in \mathrm{GL}_4(q_0)$ lies in $\mathrm{O}_4^-(q_0)$ if and only the diagonal entries of AM_QA^T are equal to the corresponding diagonal entries of M_Q, and $AM_\beta A^T = M_\beta$. Therefore, the pointwise stabiliser X of $\{\langle u\rangle, \langle v\rangle\}$ in L consists of all elements of the form

$$\sigma^k \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ a & b & 1 & 0 \\ a^2 & a & 0 & 1 \end{pmatrix},$$

where $a \in \mathbb{F}_{q_0}^\times$, $b \in \{0,1\}$ and $k \in \{0,\dots,f/2-1\}$. We also observe that an element of X fixes $\langle w\rangle$ if and only if $a = 0$ and $\sum_{j=0}^{k-1}\zeta^{2^j} = b$. Since $b = b^2$, this implies that

$$\sum_{j=0}^{k-1}\zeta^{2^j} = \left(\sum_{j=0}^{k-1}\zeta^{2^j}\right)^2 = \sum_{j=0}^{k-1}(\zeta^{2^j})^2 = \sum_{j=1}^{k}\zeta^{2^j},$$

and hence $\zeta = \zeta^{2^k}$. Since $\langle\zeta\rangle = \mathbb{F}_{q_0}$ by our assumption above, it follows that $k = 0$, and so $b = 0$. Thus $\{\langle u\rangle, \langle v\rangle, \langle w\rangle\}$ is a base for G, and hence $b(G) = 3$.

Next, suppose that q is odd, let $\delta \in \{1,3\}$ such that $q_0 \equiv \delta \pmod 4$, and let $\gamma_1 := s$ and $\gamma_3 := 1$. By Lemma 4.3.1, there exists $t \in \mathbb{F}_{q_0}^\times$ such that $t^2 + \gamma_\delta$ is a (non-zero) square in $\mathbb{F}_{q_0}$ and $\langle t^2/\gamma_\delta\rangle = \mathbb{F}_{q_0}$. Define $u := e_2$, $v := e_\delta + te_2$ and $w := e_2 + ze_4 + e_{4-\delta}$, where $z := s^{(q_0-2+\delta)/4}$. Then $Q(v) = (t^2+\gamma_\delta)/2$, and $Q(w) = (1+z^2+\gamma_{4-\delta})/2 = 1/2 = Q(u)$. Thus $\langle u\rangle, \langle v\rangle, \langle w\rangle \in \Gamma$ for some $\Gamma \in \{\Delta, \overline{\Delta}\}$. In this case, a matrix $A \in \mathrm{GL}_4(q_0)$ lies in $\mathrm{O}_4^-(q_0)$ if and only if $AM_\beta A^T = M_\beta$. Using the fact that $\langle t^2/\gamma_\delta\rangle = \mathbb{F}_{q_0}$, we deduce that the pointwise stabiliser of $\{\langle u\rangle, \langle v\rangle\}$ in L lies in $\mathrm{O}_4^-(q_0)$, and consists of all matrices of the form

$$\begin{pmatrix} a & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & b_1 & c_1 \\ 0 & 0 & \varepsilon c_1 & -\varepsilon b_1 \end{pmatrix},$$

if $\delta = 1$, or

$$\begin{pmatrix} b_2 & 0 & 0 & c_2 \\ 0 & a & 0 & 0 \\ 0 & 0 & a & 0 \\ -\varepsilon c_2 s^{-1} & 0 & 0 & \varepsilon b_2 \end{pmatrix},$$

if $\delta = 3$, where $a, \varepsilon \in \{\pm 1\}$ and $b_1^2 + c_1^2 = b_2^2 + c_2^2 s^{-1} = 1$. It is now straightforward to show that the pointwise stabiliser of $\{\langle u\rangle, \langle v\rangle, \langle w\rangle\}$ in L consists of scalar matrices. Therefore, $b(G) = 3$. ■

By combining Proposition 4.3.2 with results from the literature, we are able to determine the exact base size of every primitive group with socle $\mathrm{L}_2(q)$. Here we exclude the groups with socle $\mathrm{L}_2(4)$, as $\mathrm{L}_2(4) \cong \mathrm{L}_2(5)$. The theorem is stated as Theorem 4.1 in Section 4.1.

Theorem 4.3.3. *Let G be a primitive group with socle $T = \mathrm{L}_2(q)$, $q \geqslant 5$ and point stabiliser H. Then $b(G) > 2$ if and only if one of the following holds.*

(i) *H is of type P_1, in which case $b(G) \in \{3,4\}$. Furthermore, $b(G) = 3$ if and only if either $G \leqslant \mathrm{PGL}_2(q)$, or $|G:T| = 2$ and $G \not\leqslant \mathrm{P\Sigma L}_2(q)$.*

(ii) *H is of type $\mathrm{GL}_1(q) \wr S_2$ and $\mathrm{PGL}_2(q) < G$, in which case $b(G) = 3$.*

(iii) *H is of type $\mathrm{GL}_1(q^2)$ and $\mathrm{PGL}_2(q) \leqslant G$, in which case $b(G) = 3$.*

(iv) *H is of type $\mathrm{GL}_2(q_0)$ with $q = q_0^2 \geqslant 9$, in which case $b(G) \in \{3,4\}$. Furthermore, $b(G) = 4$ if and only if $G = \mathrm{P\Sigma L}_2(9)$.*

(v) *$(q,H) \in \{(5,A_4),(7,S_4),(11,A_5),(19,A_5)\}$ and $b(G) = 3$, $(q,H) \in \{(5,S_4),(9,A_5)\}$ and $b(G) = 4$, or $(q,H) = (9,S_5)$ and $b(G) = 5$.*

Proof. If H is soluble, then [14, Theorem 2] gives the precise base size of G. This includes the cases where H is of type P_1, $\mathrm{GL}_1(q) \wr S_2$, $\mathrm{GL}_1(q^2)$ or $2_-^{1+2}.\mathrm{O}_2^-(2)$. For the groups with H of type A_5, or of type $\mathrm{GL}_2(q_0)$ with $q_0^k = q$ for some odd prime k, we deduce the base size from [19, Tables 1 and 3]. Suppose finally that H is of type $\mathrm{GL}_2(q_0)$ with $q_0^2 = q$. Here $q \geqslant 9$, and we obtain $b(G)$ from Proposition 4.3.2. ■

We now turn to the proofs of Theorems 4.2(i), 4.3 and 4.6, and consider each case in (4.3.1) in turn. We shall use Theorem 4.1 to read off $b(G)$.

4.3.2 H is of type P_1, $2_-^{1+2}.\mathrm{O}_2^-(2)$ or A_5

Lemma 4.3.4. *If H is of type P_1, then G is semi-Frobenius and $\Sigma(G)$ is G-arc-transitive.*

Proof. Here G is 2-transitive, so the result follows from Lemma 3.3.8. ■

Lemma 4.3.5. *If H is of type $2_-^{1+2}.\mathrm{O}_2^-(2)$, then*

(i) *Property $(\star)$ holds.*

(ii) *$\Sigma(G)$ is G-arc-transitive if and only if $G \in \{\mathrm{PGL}_2(11), \mathrm{L}_2(7), S_5, A_5\}$.*

(iii) *G is semi-Frobenius if and only if $b(G) > 2$.*

Proof. The bound in the proof of [14, Lemma 4.10] is good enough to show that $Q(G,2) < 1/2$ if $q \geqslant 71$, which implies that $(\star)$ holds and $\mathrm{reg}(G) > 1$ (by Lemma 3.1.2, this implies that $\Sigma(G)$ is not G-arc-transitive). And we can use MAGMA to handle the groups with $q < 71$. ■

Lemma 4.3.6. *If H is of type A_5, then either $q \in \{9,11,19\}$, $b(G) = 3$ and G is semi-Frobenius, or $b(G) = 2$ and $(\star)$ holds. Moreover, $\Sigma(G)$ is G-arc-transitive if and only if $G \in \{\mathrm{L}_2(29), \mathrm{L}_2(11), S_6, A_6\}$.*

Proof. Recall that $i_m(H)$ is the number of elements of order m in H, and let $x \in H$ be an element of prime order m and note that $m \in \{2,3,5\}$. If $m = 2$ then $|x^G| \geqslant \frac{1}{2}q^{1/2}(q+1) = b_1$ (minimal if x is an involutory field automorphism) and we note that $i_2(H) \leqslant 25 = a_1$. Similarly, if $m \in \{3,5\}$ then $|x^G| \geqslant q(q-1) = b_2$ and $i_3(H) + i_5(H) = 44 = a_2$. Therefore, Lemma 2.4.1 implies that

$$\widehat{Q}(G,2) \leqslant a_1^2/b_1 + a_2^2/b_2$$

and we deduce that $\widehat{Q}(G,2) < 1/2$ if $q \geqslant 197$. In particular, $\mathrm{reg}(G) > 1$ for these groups since $2|H|^2 < |G|$, and so $\Sigma(G)$ is not G-arc-transitive by Lemma 3.1.2. The remaining cases with $q < 197$ can be verified using MAGMA. ■

4.3.3 H is of type $\mathrm{GL}_2(q_0)$

Suppose $q = q_0^s$ for some prime s and let H be a maximal subgroup of G of type $\mathrm{GL}_2(q_0)$. We first deal with the case where s is odd. Recall that $b(G) = 2$ in this setting, so $\Sigma(G)$ is G-arc-transitive if and only if $\mathrm{reg}(G) = 1$ (see Lemma 3.1.2).

Lemma 4.3.7. *If H is of type $\mathrm{GL}_2(q_0)$ with $q = q_0^s$ for some prime $s \geqslant 3$, then $b(G) = 2$, $(\star)$ holds and $\Sigma(G)$ is not G-arc-transitive.*

Proof. The cases where $q \leqslant 125 = 5^3$ can be handled using MAGMA, so we may assume $q > 125$. Notice that if we can show that $\widehat{Q}(G,2) < 1/2$, then $(\star)$ holds and $\mathrm{reg}(G) > 1$ (the latter property holds since $2|H|^2 < |G|$).

First assume $s \geqslant 5$ and let $x \in H$ be an element of prime order. If x is an involutory field automorphism of T, then $|x^G| \geqslant \frac{1}{2}q^{1/2}(q+1) = b_1$ and we note that there are at most $a_1 = q_0^{1/2}(q_0+1)$ such elements in H. In each of the remaining cases, we have $|x^G| \geqslant \frac{1}{2}q(q-1) = b_2$ and we observe that $|H| \leqslant q_0(q_0^2-1)\log q = a_2$. By applying Lemma 2.4.1 we deduce that

$$\widehat{Q}(G,2) \leqslant a_1^2/b_1 + a_2^2/b_2$$

and this gives $\widehat{Q}(G,2) < 1/2$ as required.

To complete the proof, we may assume $s = 3$, so $q_0 \geqslant 7$. This case requires a more refined treatment. First let $x \in H \cap \mathrm{PGL}_2(q)$ be an element of prime order m. If x is unipotent (so $m = p$) then $|x^G| \geqslant \frac{1}{2}(q^2-1) = b_1$ and we note that there are exactly $a_1 = q_0 - 1$ such elements in H. Similarly, if x is a semisimple involution then $|x^G| \geqslant \frac{1}{2}q(q-1) = b_2$ and we have $i_2(\mathrm{PGL}_2(q_0)) = q_0^2 = a_2$. Next suppose $m \neq p$ and $m \geqslant 3$, so m divides $q_0^2 - 1$ and there are $\frac{1}{2}(m-1)$ distinct T-classes of such elements in G (and the same number of $\mathrm{L}_2(q_0)$-classes in $H \cap \mathrm{PGL}_2(q)$). If $\{x_1, \ldots, x_t\}$ is a set of representatives of the distinct G-classes of these elements, then there exist positive integers k_i such that $\sum_i k_i = \frac{1}{2}(m-1)$ and

$$|x_i^G \cap H| = k_i q_0(q_0+\varepsilon),\ |x_i^G| = k_i q_0^3(q_0^3+\varepsilon),$$

where $\varepsilon = 1$ if m divides $q_0 - 1$, otherwise $\varepsilon = -1$ (here $|x_i^T| = |x_i^{\mathrm{PGL}_2(q)}| = q_0^3(q_0^3+\varepsilon)$ and k_i denotes the number of distinct T-classes that are fused under the action of field automorphisms in G). Therefore, the contribution to $\widehat{Q}(G,2)$ from elements of order m is equal to

$$\sum_{i=1}^{t} \frac{(k_i q_0(q_0+\varepsilon))^2}{k_i q_0^3(q_0^3+\varepsilon)} = \frac{1}{2}(m-1)\cdot\frac{(q_0+\varepsilon)^2}{q_0(q_0^3+\varepsilon)}.$$

If m divides q_0+1 then $m-1 \leqslant q_0$ and there are at most $\log(q_0+1)$ possibilities for m, so the total contribution to $\widehat{Q}(G,2)$ from these elements is at most

$$f_1(q_0) = \log(q_0+1)\cdot\frac{1}{2}q_0\cdot\frac{(q_0-1)^2}{q_0(q_0^3-1)}.$$

Similarly, the contribution from the elements with m dividing q_0-1 is no more than

$$f_2(q_0) = \log(q_0-1)\cdot\frac{1}{2}(q_0-2)\cdot\frac{(q_0+1)^2}{q_0(q_0^3+1)}.$$

Finally, let us assume $x \in G$ is a field automorphism of order m. As above, if $m = 2$ then $|x^G| \geqslant \frac{1}{2}q^{1/2}(q+1) = b_3$ and there are at most $a_3 = q_0^{1/2}(q_0+1)$ of these elements in H. Next suppose $m = 3$. Here $|x^G| \geqslant q_0^2(q_0^4+q_0^2+1) = b_4$ and we may assume $H = C_G(x)$, which implies that H contains at most

$$2(1+i_3(\mathrm{L}_2(q_0))) \leqslant 2\left(1+\frac{|\mathrm{GL}_2(q_0)|}{(q_0-1)^2}\right) = 2q_0(q_0+1)+2 = a_4$$

such elements. If $m = 5$ then $|x^G| > q_0^{36/5} = b_5$ and there are at most $8q_0^{12/5} = a_5$ of these elements in H. Finally, if $m \geqslant 7$ then $|x^G| > q_0^{54/7} = b_6$ and we observe that $|H| \leqslant q_0(q_0^2-1)\log q = a_6$.

Set $\alpha = 1$ if $q_0 = q_1^2$ for some q_1, otherwise $\alpha = 0$. Similarly, let $\beta = 1$ if $q_0 = q_1^5$ and $\gamma = 1$ if $q_0 = q_1^m$ for some prime $m \geqslant 7$ (otherwise $\beta = 0$ and $\gamma = 0$, respectively). Then by bringing all of the above estimates together, we conclude that

$$\widehat{Q}(G,2) < f_1(q_0) + f_2(q_0) + \left(a_1^2/b_1 + a_2^2/b_2 + a_4^2/b_4\right) + \alpha a_3^2/b_3 + \beta a_5^2/b_5 + \gamma a_6^2/b_6$$

and one checks that this upper bound is less than 1/2 for all $q_0 \geqslant 7$. ■

Now we consider the case where $q = q_0^2$. We determine which groups in this setting are semi-Frobenius.

Lemma 4.3.8. *Suppose H is of type $\mathrm{GL}_2(q_0)$, where $q = q_0^2$. Then G is not semi-Frobenius if and only if $q \geqslant 16$ and $|G:T|$ is even.*

Proof. First assume $o = |G:T|$ is odd. Let $\alpha \in \Omega$ be such that $H = G_\alpha$. We first note that, up to conjugacy in $H_0 := H \cap T$, the point stabilisers in H_0 are as follows (see [49, p. 354]):

$$H_0,\ C_p^{f/2},\ C_{q_0+1}\ ((q_0-2)/2 \text{ copies}),\ C_{q_0-1}\ (q_0/2 \text{ copies})$$

if q is even, and

$$H_0,\ D_{2(q_0+\varepsilon)},\ C_p^{f/2},\ C_{q_0+1}\ ((q_0-4-\varepsilon)/4 \text{ copies}),\ C_{q_0-1}\ ((q_0-2+\varepsilon)/4 \text{ copies})$$

if q is odd, where $\varepsilon = \pm 1$ satisfies $q_0 \equiv \varepsilon \pmod 4$.

Now, for each $\delta \in \{1,-1\}$, let Z_δ be the subgroup of $\mathbb{F}_q^\times$ of order $q_0+\delta$. As discussed in [49, p. 354], the fusion of T-suborbits of length $q_0(q_0-\delta)$ (i.e. with point stabiliser $C_{q_0+\delta}$) under a field automorphism of T corresponds to the fusion under the corresponding field automorphism of $\mathbb{F}_q$ of the sets $\{x, x^{-1}\}$, for elements $x \in \mathbb{F}_q^\times/Z_\delta$ of order at least 3. It follows that the point stabilisers in $H = G_\alpha$ are isomorphic to the following groups, for certain divisors i_+ and i_- of o:

$$H,\ C_p^{f/2}.o,\ C_{q_0+1}.i_+,\ C_{q_0-1}.i_-,\ \text{and (if } q \text{ is odd and } q_0 \equiv \varepsilon \pmod 4))\ D_{2(q_0+\varepsilon)}.o.$$

We claim that $C_{q_0\pm 1}$ always appears as a point stabiliser. To prove this, it suffices to show that the primitive element μ of $\mathbb{F}_q$ satisfies $|Z_\delta \mu^{\langle\sigma\rangle}| = o$, where σ is the automorphism of $\mathbb{F}_q$ of odd order o. Let q_1 be such that $q_1^o = q$ and hence $\mu^{\langle\sigma\rangle} = \{\mu^{q_1^m} \mid 0 \leqslant m \leqslant o-1\}$. Now $|Z_\delta \mu^{\langle\sigma\rangle}| = o$ if and only if $\mu^{q_1^m - q_1^l} \notin Z_\delta$ for all $0 \leqslant \ell < m \leqslant o-1$. Suppose for a contradiction that $\mu^{q_1^m - q_1^\ell} \in Z_\delta$ for such ℓ and m. Then $\mu^{(q_1^m - q_1^\ell)(q_0+\delta)} = 1$, and so $(q-1) \mid (q_1^m - q_1^\ell)(q_0+\delta)$. Hence $(q_0-\delta) \mid q_1^\ell(q_1^{m-\ell}-1)$, which implies $(q_0-\delta) \mid (q_1^{m-\ell}-1)$. It follows easily that either $(q_0-\delta) = (q_1^{m-\ell}-1)$ or $(q_0-\delta) \mid (q_1^{m-\ell}q_0^{-1}-\delta)$. However, since o is odd and $q_1^{m-1}q_0^{-1} < q_0$, neither case can occur, a contradiction. Next, let $\beta \in \Omega \setminus \{\alpha\}$, and choose $\gamma \in \Omega$ so that (up to isomorphism) the ordered pair (H_β, H_γ) is one of $(C_p^{f/2}.o, C_{q_0+1})$, $(D_{2(q_0+\varepsilon)}.o, C_{q_0-\varepsilon})$ and $(C_{q_0\pm1}.i, C_{q_0\mp1})$, with i a divisor of o. Since $H_\gamma \leqslant T$, we observe that $H_\beta \cap H_\gamma = (H_\beta \cap T) \cap H_\gamma$. In particular, if $H_\beta \cong C_p^{f/2}.o$, then $H_\beta \cap H_\gamma = 1$, and so $\{\alpha, \beta, \gamma\}$ is a base for G. Thus $\{\alpha, \beta\}$ is an edge in $\Sigma(G)$. In the remaining two cases, either $H_\beta \cap H_\gamma = 1$ and $\{\alpha, \beta\}$ is again an edge, or $H_\beta \cap H_\gamma = \langle g \rangle$, where g is the unique involution of H_γ. As H_β is a core-free subgroup of H, there exists $h \in H$ such that $g \notin H_\beta^h$, and hence $g \notin H_{\beta^h} \cap H_\gamma$, which yields $H_{\beta^h} \cap H_\gamma = 1$. This shows that $\{\alpha, \beta, \gamma^{h^{-1}}\}$ is a base for G, and thus $\Sigma(G)$ is complete.

To complete the proof, assume $|G:T|$ is even. To show that $\Sigma(G)$ is not complete, it suffices to consider the case where G is generated by T and an involutory field automorphism. As in the proof of Proposition 4.3.2, we identify G with the orthogonal group $\mathrm{PO}_4^-(q_0)$, where $\mathrm{O}_4^-(q_0)$ is the isometry group of a non-degenerate quadratic form Q of minus type on $V := \mathbb{F}_{q_0}^4$. As above, the action of G on the right cosets of H is equivalent to its action on the set Δ of one-dimensional subspaces Y of V such that there exists $y \in Y$ with $Q(y)$ a non-zero square in $\mathbb{F}_{q_0}$. We shall therefore complete the proof by identifying a pair of elements of Δ that does not extend to a base for G of size $b(G) = 3$.

Assume first that q_0 is even, and let ρ be the polar form of Q. As in the proof of Proposition 4.3.2, there exists a basis $\{e_1, \ldots, e_4\}$ for V so that the matrix of Q is

$$M_Q := \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & \zeta & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

for an arbitrary $\zeta \in \mathbb{F}_{q_0}^\times$ such that the polynomial $x^2+x+\zeta$ is irreducible over $\mathbb{F}_{q_0}$. Since $q_0 \geqslant 4$, there are at least two choices for ζ, and so we will assume without loss of generality that $\zeta \neq 1$.

Now, let $v_1 := e_1+\zeta e_2+e_3+\zeta e_4$, $v_2 := e_2$, $v_3 := e_1$ and $v_4 := e_3$, so that $\{v_1,v_2,v_3,v_4\}$ is a basis for V. Then $Q(v_2)=1$, and

$$Q(v_1)=\zeta\rho(e_1,e_4)+\zeta^2 Q(e_2)+\zeta\rho(e_2,e_3)+Q(e_3)=\zeta+\zeta^2+\zeta+\zeta=\zeta(1+\zeta)\neq 0.$$

Hence $\langle v_1\rangle$ and $\langle v_2\rangle$ are distinct subspaces in Δ. Additionally, let $u \in V \setminus \langle v_1,v_2\rangle$, so that $u = \sum_{i=1}^4 \alpha_i v_i$ with $\alpha_i \in \mathbb{F}_{q_0}$ such that α_3 and α_4 are not both 0. Finally, let $m := \zeta\alpha_3^2+\alpha_4(\alpha_3+\alpha_4)$ and

$$A := m^{-1}\begin{pmatrix} \zeta\alpha_3^2 & \zeta\alpha_3\alpha_4 & 0 & \zeta\alpha_4^2 \\ 0 & m & 0 & 0 \\ \alpha_3(\alpha_3+\alpha_4) & \zeta\alpha_3^2 & m & \zeta\alpha_3\alpha_4 \\ \zeta^{-1}(\alpha_3+\alpha_4)^2 & \alpha_3(\alpha_3+\alpha_4) & 0 & \zeta\alpha_3^2 \end{pmatrix}.$$

Note that if $\alpha_3=0$, then $m=\alpha_4^2\neq 0$, and otherwise $m=(\alpha_3^2)((\alpha_4\alpha_3^{-1})^2+\alpha_4\alpha_3^{-1}+\zeta)$, which is again non-zero by the definition of ζ. It is straightforward to check that $\det(A)=1$, that the diagonal entries of AM_QA^T are equal to the corresponding diagonal entries of M_Q, and that the Gram matrix $M_\rho = M_Q+M_Q^T$ of the polar form ρ satisfies $AM_\rho A^T = M_\rho$. Hence $A \in \mathrm{O}_4^-(q_0)$. We also observe that A is a non-scalar matrix that fixes u and each vector in $\langle v_1,v_2\rangle$. Since each subspace in Δ is spanned either by such a vector u or by a vector in $\langle v_1,v_2\rangle$, the subset $\{\langle v_1\rangle,\langle v_2\rangle\}$ of Δ does not extend to a base for G of size 3.

Next, suppose that q_0 is odd. We deduce from [80, p. 45] that there exists a basis $\{e_1,\dots,e_4\}$ for V so that the matrix of Q is

$$M_Q := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & -r \\ 0 & 0 & 0 & -s \end{pmatrix},$$

where $r := \omega+\omega^{q_0}$ and $s := \omega^{q_0+1}$ for an arbitrary element ω of $\mathbb{F}_q \setminus \mathbb{F}_{q_0}$. Note that r and s do indeed lie in $\mathbb{F}_{q_0}$, as they are each equal to their q_0-th power.

We now proceed similarly to above. Since $q_0>3$, there exists $y \in \mathbb{F}_{q_0}^\times \setminus \{\pm 1\}$. Let $v_1 := e_1+e_2$, $v_2 := e_1+y^2e_2$, $v_3 := e_3$ and $v_4 := e_4$, so that $\{v_1,v_2,v_3,v_4\}$ is a basis for V. As $Q(v_1)=1$ and $Q(v_2)=y^2$ are both non-zero squares in $\mathbb{F}_{q_0}$, it follows that $\langle v_1\rangle$ and $\langle v_2\rangle$ are distinct subspaces in Δ. Additionally, each $u \in V\setminus\langle v_1,v_2\rangle$ satisfies $u=\sum_{i=1}^4\alpha_i v_i$ for some $\alpha_i \in \mathbb{F}_{q_0}$ such that α_3 and α_4 are not both 0. For such a vector u, let $t := (\alpha_3+\alpha_4\omega)(\alpha_3+\alpha_4\omega^{q_0})$ and

$$A := t^{-1}\begin{pmatrix} t & 0 & 0 & 0 \\ 0 & t & 0 & 0 \\ 0 & 0 & \alpha_3^2-s\alpha_4^2 & (2\alpha_3+r\alpha_4)\alpha_4 \\ 0 & 0 & (r\alpha_3+2s\alpha_4)\alpha_3 & -\alpha_3^2+s\alpha_4^2 \end{pmatrix}.$$

Note that $t \in \mathbb{F}_{q_0}$ as $t^{q_0} = t$, and that $t \neq 0$ since α_3 and α_4 lie in $\mathbb{F}_{q_0}$, while ω and ω^{q_0} do not. As above, A is a non-scalar matrix in $\mathrm{O}_4^-(q_0)$ (this time with determinant -1) that fixes u and each vector in $\langle v_1, v_2\rangle$. We conclude that $\{\langle v_1\rangle, \langle v_2\rangle\}$ does not extend to a base for G of size 3, as required. ■

In particular, this immediately implies that $(\star)$ holds and $\Sigma(G)$ is not G-arc-transitive for the groups G with $|G:T|$ odd. However, for the relevant groups with $|G:T|$ even (that is, $G \in \mathscr{F}$), G contains an involutory field automorphism φ, and one can calculate that the contribution of the involutory field automorphisms to $\widehat{Q}(G,3)$ is exactly

$$|\varphi^G| \cdot \mathrm{fpr}(\varphi)^3 = (2,q-1)^2 \cdot \frac{q^2}{(q+1)^2}$$

Thus, using the probabilistic method to verify $(\star)$ or to estimate $\mathrm{reg}(G)$ is not feasible in this setting, and we leave these problems open for the groups with $G \in \mathscr{F}$. Note that these groups are excluded in the statements of Theorems 4.2(i) and 4.3.

The remaining two cases in (4.3.1), namely where H is of type $\mathrm{GL}_1(q) \wr S_2$ or $\mathrm{GL}_1(q^2)$, need more detailed treatment. Here a key ingredient is the following result of Chen and Du [36].

Theorem 4.3.9 (Chen & Du, [36]). *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite almost simple primitive group with socle $T = \mathrm{L}_2(q)$ and $b(G) = 2$. Then the Saxl graph $\Sigma(G)$ has diameter* 2.

This establishes a special case of Conjecture II, which asserts that $\Sigma(G)$ has diameter at most 2 for every finite primitive permutation group G with $b(G) = 2$. In view of Theorem 4.3.9, in order to establish $(\star)$ for base-two groups, it suffices to show that if $\{\alpha,\beta\}$ is a base for G, then there exists $\gamma \in \Omega$ such that $\{\alpha,\gamma\}$ and $\{\beta,\gamma\}$ are bases.

Let us fix some notation, following Example 2.2.3. Let V be the natural module for T. Fix a basis $\{e_1, e_2\}$ for V and write $\mathbb{F}_q^\times = \langle \mu \rangle$. Let $\delta \in \mathrm{PGL}_2(q)$ be the image (modulo scalars) of the diagonal matrix $\mathrm{diag}(\mu,1) \in \mathrm{GL}_2(q)$, which induces a diagonal automorphism on T. Similarly, let ϕ be a field automorphism of order f such that $(ae_1 + be_2)^\phi = a^p e_1 + b^p e_2$ for all $a, b \in \mathbb{F}_q$ and note that

$$\mathrm{Aut}(T) = \langle T, \delta, \phi \rangle$$

and $\mathrm{P\Sigma L}_2(q) = \langle T, \phi\rangle$. For $g \in \mathrm{Aut}(T)$, if we write $\ddot{g}$ for the coset Tg, then

$$\mathrm{Out}(T) = \{\ddot{g} : g \in \mathrm{Aut}(T)\} = \langle \ddot{\delta} \rangle \times \langle \ddot{\phi} \rangle = C_{(2,q-1)} \times C_f.$$

As before, we set $H_0 = H \cap T$.

It is convenient to use computational methods (as discussed in Section 4.2) to handle the cases where q is small. To this end, we present the following result. Note that the primitivity of G implies that $q \neq 5$ in part (ii)(a), and $\mathrm{L}_2(9).2 = \mathrm{L}_2(9).\langle \delta\phi \rangle \cong \mathrm{M}_{10}$ in part (ii)(b).

Proposition 4.3.10. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite almost simple primitive group with socle $T = \mathrm{L}_2(q)$ and point stabiliser H of type $\mathrm{GL}_1(q) \wr S_2$ or $\mathrm{GL}_1(q^2)$. If $q \leqslant 27$, then the following hold:*

(i) Property $(\star)$ *holds.*

(ii) $\Sigma(G)$ *is G-arc-transitive if and only if one of the following holds:*

(a) $G = \mathrm{PGL}_2(q)$*,* $5 \neq q \geqslant 4$*, and* $H = D_{2(q-1)}$*; or*

(b) $(G,H) = (\mathrm{L}_2(5), D_6)$*,* $(\mathrm{P\Gamma L}_2(8), D_{18}.3)$ *or* $(\mathrm{M}_{10}, 5{:}4)$*.*

(iii) G *is semi-Frobenius if and only if* $b(G) > 2$*.*

Proof. This can be done easily with the aid of MAGMA. ■

4.3.4 H is of type $\mathrm{GL}_1(q) \wr S_2$

Here $H_0 = D_{2(q-1)/h}$ and $|\Omega| = \frac{1}{2}q(q+1)$, where $h = (2, q-1)$. We may identify $\Omega = [G:H]$ with the set of unordered pairs of distinct 1-dimensional subspaces of the natural module V for T. The maximality of H implies that $q \geqslant 4$ and $q \neq 5$ (see [11, Table 8.1], for example); in view of Proposition 4.3.10, we may assume that $q > 27$. Recall that $b(G) \leqslant 3$, with equality if and only if $\mathrm{PGL}_2(q) < G$.

We first consider the groups with $b(G) = 2$ (we will return to the general case in the proof of Proposition 4.3.19 below), so $\Sigma(G)$ is G-arc-transitive if and only if $\mathrm{reg}(G) = 1$ (recall Lemma 3.1.2). As noted in Example 3.1.4, if $G = \mathrm{PGL}_2(q)$ then $\Sigma(G)$ is isomorphic to the Johnson graph $J(q+1, 2)$; the vertices of this graph correspond to the 2-element subsets of a set of size $q+1$, with two vertices joined by an edge if they have nonempty intersection. This observation immediately implies $(\star)$ and $\mathrm{reg}(G) = 1$. Therefore, we will assume that q is odd and $G \cap \mathrm{PGL}_2(q) = T$. Then as noted in the proof of [14, Lemma 4.7], this implies that one of the following holds:

(a) $G = \langle T, \phi^j \rangle$ for some j in the range $0 \leqslant j < f$; or

(b) $G = \langle T, \delta\phi^j \rangle$ with $0 < j < f$ and $f/(f,j)$ even.

Set $\alpha, \beta \in \Omega$, where $\alpha = \{\langle e_1 \rangle, \langle e_2 \rangle\}$ and $\beta = \{\langle u \rangle, \langle v \rangle\}$. Let us assume q is odd and suppose $G = \mathrm{P\Sigma L}_2(q) = \langle T, \phi \rangle$. Notice that if $u = e_1$ and $v = be_1 + e_2$, then α and β are fixed by the image in G of an element

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \phi \in \langle \mathrm{SL}_2(q), \phi \rangle$$

with $a^2 = b^{p-1}$. Similarly, the pointwise stabiliser of $\{\alpha, \beta\}$ is nontrivial if $u = e_2$. Therefore, $\{\alpha, \beta\}$ is a base for G only if $\langle u \rangle = \langle e_1 + be_2 \rangle$ and $\langle v \rangle = \langle e_1 + ce_2 \rangle$ for distinct nonzero scalars $b, c \in \mathbb{F}_q$.

In Lemma 4.3.12 below we present necessary and sufficient conditions on the scalars b and c to ensure that $\{\alpha, \beta\}$ is a base for $\mathrm{P\Sigma L}_2(q)$. To do this, we need the following more general result. Note that the condition in part (iii) is equivalent to the non-containment of bc^{-1} in a proper subfield of $\mathbb{F}_q$.

Lemma 4.3.11. *Suppose $G \cap \mathrm{PGL}_2(q) = T$ with q odd and set*

$$\alpha = \{\langle e_1\rangle, \langle e_2\rangle\},\ \ \beta = \{\langle e_1 + be_2\rangle, \langle e_1 + ce_2\rangle\}$$

with $b \neq c$. Then $\{\alpha, \beta\}$ is a base for G if the following conditions are satisfied:

(i) $bc \neq 0$;

(ii) $-bc^{-1}$ *is a non-square in* $\mathbb{F}_q$*; and*

(iii) $b^{p^k-1} \neq c^{p^k-1}$ *for all* $0 < k < f$.

Proof. Suppose b and c satisfy the three given conditions and let us assume

$$x = AB^i\phi^j \in \langle \mathrm{GL}_2(q), \phi\rangle$$

fixes α and β, where $A \in \mathrm{SL}_2(q)$, $B = \mathrm{diag}(\mu, 1)$, $0 \leqslant i < q-1$ and $0 \leqslant j < f$, with $j > 0$ if $i > 0$. It suffices to show that $x = \pm I_2$. Since x fixes α, the matrix of A with respect to the basis $\{e_1, e_2\}$ is either diagonal or anti-diagonal.

First assume x fixes the two 1-spaces comprising α, so $A = \mathrm{diag}(a, a^{-1})$ is diagonal. If x also fixes the two spaces in β, then

$$\begin{aligned}(e_1 + be_2)^x &= a\mu^i e_1 + a^{-1}b^{p^j}e_2 = \eta_1(e_1 + be_2)\\ (e_1 + ce_2)^x &= a\mu^i e_1 + a^{-1}c^{p^j}e_2 = \eta_2(e_1 + ce_2)\end{aligned}$$

for some $\eta_1, \eta_2 \in \mathbb{F}_q^\times$. Therefore

$$a^2\mu^i = b^{p^j-1} = c^{p^j-1} \tag{4.3.2}$$

and thus (iii) implies that $j = 0$, so $i = 0$ and $a^2 = 1$, which gives $x = \pm I_2$ as required. Similarly, if x interchanges the spaces in β, then

$$a^2\mu^i = b^{p^j}c^{-1} = c^{p^j}b^{-1}. \tag{4.3.3}$$

Here $b^{p^{2j}-1} = c^{p^{2j}-1}$, so (iii) implies that $2j = 0$ or f. Suppose $2j = 0$, so $i = 0$ and $a^2 = bc^{-1} = cb^{-1}$ and thus $bc^{-1} = \pm 1$. But $b \neq c$, so $bc^{-1} = -1$, which is incompatible with (ii). Now assume $2j = f$, so $q \equiv 1 \pmod 4$ and -1 is a square in $\mathbb{F}_q$. In addition, (4.3.3) gives $(bc^{-1})^{p^{f/2}+1} = 1$, so $bc^{-1} \in \langle \mu^{p^{f/2}-1}\rangle$ and thus bc^{-1} is a square. Therefore, $-bc^{-1}$ is a square, which once again is incompatible with (ii).

Now assume $A = \begin{pmatrix} 0 & a \\ -a^{-1} & 0\end{pmatrix}$ is anti-diagonal. If x fixes both spaces in β then

$$\begin{aligned}(e_1 + be_2)^x &= ab^{p^j}e_1 - a^{-1}\mu^i e_2 = \eta_1(e_1 + be_2)\\ (e_1 + ce_2)^x &= ac^{p^j}e_1 - a^{-1}\mu^i e_2 = \eta_2(e_1 + ce_2)\end{aligned}$$

for some $\eta_1, \eta_2 \in \mathbb{F}_q^\times$. This gives

$$-a^2\mu^{-i} = b^{-p^j-1} = c^{-p^j-1}. \tag{4.3.4}$$

Here $b^{p^{2j}-1} = c^{p^{2j}-1}$ and thus $2j = 0$ or f by (iii). If $2j = 0$ then $i = 0$ and $-a^2 = b^{-2} = c^{-2}$, which implies that $bc^{-1} = \pm 1$. As noted above, this is incompatible with (ii). Now assume $2j = f$, so $q \equiv 1 \pmod 4$ and -1 is a square in $\mathbb{F}_q$ once again. Then (4.3.4) gives $(bc^{-1})^{p^{f/2}+1} = 1$ and as above we deduce that bc^{-1} is a square. Hence, $-bc^{-1}$ is also a square, which contradicts (ii).

Finally, suppose A is anti-diagonal as above and assume x interchanges the 1-spaces in β. Here we get

$$-a^2\mu^{-i} = b^{-p^j}c^{-1} = c^{-p^j}b^{-1}, \tag{4.3.5}$$

so $b^{p^j-1} = c^{p^j-1}$ and the condition in (iii) implies that $j = 0$ and $i = 0$. Therefore $-bc^{-1} = (ab)^2$, which is incompatible with (ii).

We conclude that if the scalars b and c satisfy the conditions in (i), (ii) and (iii), then $\{\alpha, \beta\}$ is a base. ■

Lemma 4.3.12. *Let $G = \mathrm{P\Sigma L}_2(q)$ with q odd and set α and β as in Lemma 4.3.11. Then $\{\alpha,\beta\}$ is a base for G if and only if the scalars b and c satisfy the conditions (i)–(iii) in Lemma 4.3.11.*

Proof. By Lemma 4.3.11, it suffices to show that if any of the conditions in (i), (ii) or (iii) fail to hold, then there exists an element $x \neq \pm I_2$ in $\Sigma\mathrm{L}_2(q) = \langle \mathrm{SL}_2(q), \phi\rangle$ that fixes α and β. We proceed by inspecting the proof of Lemma 4.3.11, noting that $i = 0$ in each of the equations (4.3.2)–(4.3.5).

As explained in the discussion preceding Lemma 4.3.11, if $bc = 0$ then $\{\alpha,\beta\}$ is not a base. Next assume $-bc^{-1}$ is a square in $\mathbb{F}_q$, say $d^2 = -bc^{-1}$. Then setting $a = db^{-1}$ gives $-a^2 = b^{-1}c^{-1}$ and we get a solution to (4.3.5) with $j = 0$. Finally, suppose $b^{p^k-1} = c^{p^k-1}$ for some $0 < k < f$ and choose $a \in \mathbb{F}_q$ with $a^2 = b^{p^k-1}$. Then (4.3.2) is satisfied and we conclude that $x = \mathrm{diag}(a, a^{-1})\phi^k$ fixes α and β. ■

Let us record three corollaries of Lemma 4.3.12. The first result allows us to reduce our main problems to the special case $G = \mathrm{P\Sigma L}_2(q)$.

Corollary 4.3.13. *Suppose $G \cap \mathrm{PGL}_2(q) = T$ and q is odd. Then the Saxl graph $\Sigma(G)$ contains $\Sigma(\mathrm{P\Sigma L}_2(q))$ as a subgraph.*

Proof. Let $\{\alpha,\beta\}$ be a base for $\mathrm{P\Sigma L}_2(q)$ with $\alpha = \{\langle e_1\rangle, \langle e_2\rangle\}$ as usual. As explained in the discussion preceding Lemma 4.3.11, we have $\beta = \{\langle e_1 + be_2\rangle, \langle e_1 + ce_2\rangle\}$ for nonzero scalars b and c, which must satisfy the conditions in parts (i), (ii) and (iii) of Lemma 4.3.11 (see Lemma 4.3.12). Then Lemma 4.3.11 implies that $\{\alpha,\beta\}$ is a base for G and the result follows. ■

Corollary 4.3.14. *Let $G = \mathrm{P\Sigma L}_2(q)$ with q odd and set*

$$\beta = \{\langle e_1 + be_2\rangle, \langle e_1 + ce_2\rangle\},\ \ \gamma = \{\langle e_1 + b'e_2\rangle, \langle e_1 + c'e_2\rangle\}$$

where b, c, b', c' are nonzero scalars with $b \neq c$ and $b' \neq c'$. Then $\{\beta, \gamma\}$ is a base for G if and only if

$$\{b', c'\} = \left\{\frac{b(c-b)+dc}{c-b+d}, \frac{b(c-b)+ec}{c-b+e}\right\}$$

for scalars $d, e \in \mathbb{F}_q$ with $d, e \neq b - c$ satisfying conditions (i)–(iii) in Lemma 4.3.11.

Proof. Since G acts primitively on Ω, it follows that the normal subgroup T is transitive. Therefore, $\beta = \alpha^g$ for some $g \in T$ and we note that g maps the set of neighbours of α in $\Sigma(G)$ to the set of neighbours of β. More precisely, we can take g to be the image of the matrix

$$\begin{pmatrix} 1 & (c-b)^{-1} \\ b & c(c-b)^{-1} \end{pmatrix} \in \mathrm{SL}_2(q).$$

Suppose $\{\beta, \gamma\}$ is a base, so $\gamma = \delta^g$ for some neighbour δ of α. By Lemma 4.3.12, we have $\delta = \{\langle e_1 + de_2\rangle, \langle e_1 + ee_2\rangle\}$ for scalars $d, e \in \mathbb{F}_q$ satisfying the conditions in (i)–(iii) of Lemma 4.3.11 and by applying g we get

$$\gamma = \{\langle (1 + d(c-b)^{-1})e_1 + (b + dc(c-b)^{-1})e_2\rangle, \langle (1 + e(c-b)^{-1})e_1 + (b + ec(c-b)^{-1})e_2\rangle\}.$$

Here the coefficients $1 + d(c-b)^{-1}$ and $1 + e(c-b)^{-1}$ are nonzero, so $d, e \neq b - c$ and we deduce that γ has the required form.

Conversely, if γ has the given form then $\gamma = \delta^g$ for some $\delta \in \Omega$ with $\{\alpha, \delta\}$ a base and it follows that $\{\beta, \gamma\}$ is a base. ■

Corollary 4.3.15. *Let $G = \mathrm{P\Sigma L}_2(q)$ with q odd and let m be the number of non-squares in $\mathbb{F}_q$ that are not contained in any proper subfield of $\mathbb{F}_q$. Then $\Sigma(G)$ has valency $m(q-1)/2$ and thus G has exactly $m/2f$ regular suborbits on Ω.*

Proof. We consider the neighbours of $\alpha = \{\langle e_1\rangle, \langle e_2\rangle\}$. Suppose $\beta = \{\langle e_1 + b_0e_2\rangle, \langle e_1 + e_2\rangle\}$. By Lemma 4.3.12, $\{\alpha, \beta\}$ is a base if and only if $-b_0$ is a non-square that is not contained in any proper subfield of $\mathbb{F}_q$. Therefore, there are m choices for β. More generally, if $\beta = \{\langle e_1 + be_2\rangle, \langle e_1 + ce_2\rangle\}$ with $c \neq 0$, then $\{\alpha, \beta\}$ is a base if and only if $b = cb_0$ for some b_0 as above. Since there are $q-1$ choices for c and we can interchange the two spaces comprising β, we conclude that $\Sigma(G)$ has valency $m(q-1)/2$. Since $|H| = (q-1)f$, it follows that G has precisely $m/2f$ regular suborbits on Ω. ■

We are now in a position to prove our first main result for the base-two groups G with H of type $\mathrm{GL}_1(q) \wr S_2$. The following proposition extends Theorem 4.3.9 by establishing Conjecture II for these groups.

Lemma 4.3.16. *Property* $(\star)$ *holds if* H *is of type* $\mathrm{GL}_1(q)\wr S_2$ *and* $b(G)=2$.

Proof. We may assume $q>27$. Recall that $b(G)=2$ if and only if G does not contain $\mathrm{PGL}_2(q)$ as a proper subgroup. If $G=\mathrm{PGL}_2(q)$, then $\Sigma(G)$ is isomorphic to the Johnson graph $J(q+1,2)$ and we immediately deduce that $(\star)$ holds (as noted in Example 3.1.4).

For the remainder, we may assume that $G\cap\mathrm{PGL}_2(q)=T$ and q is odd. In view of Corollary 4.3.13, we only need to consider the group $G=\mathrm{P\Sigma L}_2(q)$. Fix $\alpha=\{\langle e_1\rangle,\langle e_2\rangle\}$ as before. By Theorem 4.3.9, it suffices to show that if $\{\alpha,\beta\}$ is a base, then there exists $\gamma\in\Omega$ such that both $\{\alpha,\gamma\}$ and $\{\beta,\gamma\}$ are bases.

By Lemma 4.3.12 we have $\beta=\{\langle e_1+be_2\rangle,\langle e_1+ce_2\rangle\}$, where $b,c\in\mathbb{F}_q$ are nonzero scalars such that $-bc^{-1}$ is a non-square and is not contained in any proper subfield of $\mathbb{F}_q$. Set $\gamma=\{\langle e_1-be_2\rangle,\langle e_1-ce_2\rangle\}\in\Omega$ and note that $\{\alpha,\gamma\}$ is a base by Lemma 4.3.11. By Corollary 4.3.14, $\{\beta,\gamma\}$ is a base if and only if there exists $d,e\in\mathbb{F}_q$ with $d,e\neq b-c$ such that

$$\{-b,-c\}=\left\{\frac{b(c-b)+dc}{c-b+d},\frac{b(c-b)+ec}{c-b+e}\right\}\tag{4.3.6}$$

and d,e satisfy the conditions in parts (i), (ii) and (iii) in Lemma 4.3.11.

Set $d=\frac{2b(b-c)}{b+c}$ and $e=\frac{b^2-c^2}{2c}$. Then $d,e\neq b-c$, (4.3.6) holds and $de\neq 0$. In addition,

$$-de^{-1}=-bc^{-1}\left(\frac{2c}{b+c}\right)^2=-4(bc^{-1}+cb^{-1}+2)^{-1}$$

and we immediately deduce that $-de^{-1}$ is a non-square in $\mathbb{F}_q$.

Finally, we claim that de^{-1} is not contained in a proper subfield of $\mathbb{F}_q$. To do this, it suffices to show that $\eta=bc^{-1}+cb^{-1}$ is not contained in such a subfield. With this aim in mind, it will be useful to observe that

$$\begin{aligned}\eta^{p^k}-\eta&=(bc^{-1})^{p^k}+(bc^{-1})^{-p^k}-bc^{-1}-(bc^{-1})^{-1}\\&=(bc^{-1})^{-p^k}((bc^{-1})^{p^k+1}-1)((bc^{-1})^{p^k-1}-1)\end{aligned}$$

for $1\leqslant k<f$, so η is contained in the subfield $\mathbb{F}_{p^k}$ of $\mathbb{F}_q$ if and only if this expression is 0. Now since b and c satisfy the condition in part (iii) of Lemma 4.3.11, it follows that $(bc^{-1})^{p^k-1}-1\neq 0$, whence $\eta\in\mathbb{F}_{p^k}$ if and only if $(bc^{-1})^{p^k+1}=1$. If the latter equality holds, then $bc^{-1}\in\mathbb{F}_{p^{2k}}$ and thus $2k=f$. In particular, this implies that both -1 and bc^{-1} are squares, which contradicts (ii) in Lemma 4.3.11.

This justifies the claim and we conclude that d and e satisfy the conditions in parts (i), (ii) and (iii) of Lemma 4.3.11. In particular, $\{\beta,\gamma\}$ is a base and the result follows. ■

Next we turn to the problem of determining when G has a unique regular suborbit on Ω. We will need the following number-theoretic result, where ϕ and $\gamma=0.57721...$ denote Euler's totient function and Euler's constant, respectively.

Lemma 4.3.17. *For every integer $n \geqslant 3$,*

$$\phi(n) > \frac{n}{e^{\gamma}\log\log n + \frac{3}{\log\log n}}.$$

Proof. See [108, Theorem 15]. ■

Lemma 4.3.18. *Suppose H is of type $\mathrm{GL}_1(q) \wr S_2$. Then G has a unique regular suborbit if and only if $G = \mathrm{PGL}_2(q)$ and $q \geqslant 4$, $q \neq 5$.*

Proof. In view of Proposition 4.3.10, we may assume $q > 27$ and we recall that $G = \mathrm{PGL}_2(q)$ has a unique regular suborbit. For the remainder we may assume $G \cap \mathrm{PGL}_2(q) = T$ and our aim is to show that G has at least two regular suborbits. By Corollary 4.3.13, we may assume that $G = \mathrm{P\Sigma L}_2(q)$, in which case G has $m/2f$ regular suborbits by Corollary 4.3.15, where m is the number of non-squares in $\mathbb{F}_q$ that are not contained in any proper subfield of $\mathbb{F}_q$. Any primitive element of $\mathbb{F}_q$ has this property and there are $\phi(q-1)$ such elements in $\mathbb{F}_q$. By applying the lower bound in Lemma 4.3.17 we deduce that $\phi(q-1) \geqslant 4f$ for all $q > 27$ and the result follows. ■

Proposition 4.3.19. *Suppose H is of type $\mathrm{GL}_1(q) \wr S_2$. Then the following hold:*

(i) Property $(\star)$ holds.

(ii) $\Sigma(G)$ is G-arc-transitive if and only if $G = \mathrm{PGL}_2(q)$ and $q \geqslant 4$, $q \neq 5$.

(iii) G is semi-Frobenius if and only if $b(G) > 2$.

Proof. In view of Lemmas 4.3.16 and 4.3.18, it suffices to prove (iii). Note that G is not semi-Frobenius if $b(G) = 2$, so we only need to consider the groups with $b(G) > 2$, which means that $\mathrm{PGL}_2(q) < G$ and $b(G) = 3$. As before, we identify Ω with the set of distinct pairs of 1-dimensional subspaces of $\mathbb{F}_q^2$, and as shown in the proof of [14, Lemma 4.7], $\{\alpha, \beta, \gamma\}$ is a base for G, where

$$\alpha := \{\langle e_1\rangle, \langle e_2\rangle\},\ \beta := \{\langle e_1\rangle, \langle e_1 + e_2\rangle\},\ \text{and } \gamma := \{\langle e_1\rangle, \langle e_1 + \mu e_2\rangle\},$$

with $\{e_1, e_2\}$ an arbitrary basis for $\mathbb{F}_q^2$ and μ a generator of $\mathbb{F}_q^\times$. Thus $\{\alpha, \beta\}$ is an edge in $\Sigma(G)$. Moreover, for each $\lambda \in \mathbb{F}_q^\times$, replacing e_2 by λe_2 shows that α and $\{\langle e_1\rangle, \langle e_1 + \lambda e_2\rangle\}$ are adjacent in $\Sigma(G)$. By symmetry, α is also adjacent to $\{\langle e_2\rangle, \langle e_1 + \lambda e_2\rangle\}$. It remains to prove that, for all distinct $\lambda_1, \lambda_2 \in \mathbb{F}_q^\times$, there exists a base for G containing both α and $\delta := \{\langle e_1 + \lambda_1 e_2\rangle, \langle e_1 + \lambda_2 e_2\rangle\}$.

We claim that there exists $\nu \in \{\mu, \mu^{-1}\}$ such that $\lambda_1\lambda_2^{-1} \neq \nu^{p^j - 1}$ for all $j \in \{1, \dots, f\}$. Otherwise, since $\lambda_1 \neq \lambda_2$, there would exist $j, k \in \{1, \dots, f-1\}$ such that $\mu^{p^j-1} = (\mu^{-1})^{p^k-1}$, i.e. $\mu^{p^j+p^k-2} = 1$. Since $p^j + p^k - 2 < 2q - 2$, this would imply that $p^j + p^k - 2 = q - 1$, which is impossible as they have different parities, and so our claim follows. Now, let $\theta := \{\langle e_1\rangle, \langle e_1 + \lambda_1 \nu e_2\rangle\}$. We will show that $\{\alpha, \theta, \delta\}$ is a base for G.

The pointwise stabiliser of $\{\alpha,\theta\}$ in $\Gamma\mathrm{L}_2(q)$ consists of all elements of the form $g_{j,x} := \sigma^j\mathrm{diag}((\lambda_1\nu)^{p^j-1}x,x)$, where $1 \leqslant j \leqslant f$, $x \in \mathbb{F}_q^\times$, and σ is the field automorphism such that $(c_1e_1+c_2e_2)^\sigma = c_1^pe_1+c_2^pe_2$ for all $c_1,c_2 \in \mathbb{F}_q$. Additionally, $g_{j,x}$ maps the subspace $U := \langle e_1+\lambda_1e_2\rangle$ to $\langle e_1+\lambda_1(\nu^{-1})^{(p^j-1)}e_2\rangle$. Suppose now that $g_{j,x}$ also stabilises δ. If $g_{j,x}$ swaps the two subspaces in δ, then it follows that $\lambda_1\lambda_2^{-1} = \nu^{p^j-1}$, contradicting the definition of ν. Hence $g_{j,x}$ fixes U, and so $(\nu^{-1})^{p^j-1} = 1$, yielding $j = f$ and $g_{j,x} \in Z(\mathrm{GL}_2(q))$. Therefore, $\{\alpha,\theta,\delta\}$ is a base for G. ■

4.3.5 H is of type $\mathrm{GL}_1(q^2)$

Now we turn to the groups with H of type $\mathrm{GL}_1(q^2)$, so $H_0 = D_{2(q+1)/h}$ and $|\Omega| = \frac{1}{2}q(q-1)$, where $h = (2,q-1)$. By Proposition 4.3.10 we may assume $q > 27$ and we recall that $b(G) \leqslant 3$, with equality if and only if $\mathrm{PGL}_2(q) \leqslant G$.

Once again, we first treat the base-two groups, and hence we may assume q is odd and $G \cap \mathrm{PGL}_2(q) = T$, so either

(a) $G = \langle T,\phi^j\rangle$ for some j in the range $0 \leqslant j < f$; or

(b) $G = \langle T,\delta\phi^j\rangle$ with $0 < j < f$ and $f/(f,j)$ even.

Following [14], it will be helpful to identify T with the unitary group $X_0 = \mathrm{U}_2(q)$ and H with a maximal subgroup of type $\mathrm{GU}_1(q)\wr S_2$. We may then identify Ω with the set of orthogonal pairs of nondegenerate 1-dimensional subspaces of the natural module U for X_0, which is defined over $\mathbb{F}_{q^2}$. As in the proof of [14, Lemma 4.8], fix an orthonormal basis $\{u,v\}$ for U and set $\alpha = \{\langle u\rangle,\langle v\rangle\} \in \Omega$. For each nonzero scalar $b \in \mathbb{F}_{q^2}$ with $b^{q+1} \neq -1$ we define

$$\omega_b = \{\langle u+bv\rangle,\langle u-b^{-q}v\rangle\} \in \Omega. \tag{4.3.7}$$

Then

$$\Omega = \{\alpha\} \cup \{\omega_b : b \in \mathbb{F}_{q^2}^\times,\, b^{q+1} \neq -1\}$$

and we note that $\omega_b = \omega_{-b^{-q}}$. We will abuse notation by writing ϕ for the field automorphism of X_0 that corresponds to the map $\eta \mapsto \eta^p$ on $\mathbb{F}_{q^2}$ and we will assume that

$$(au+bv)^\phi = a^pu+b^pv$$

for all $a,b \in \mathbb{F}_{q^2}$. We define $\Sigma\mathrm{U}_2(q) = \langle \mathrm{SU}_2(q),\phi\rangle$ and $\mathrm{P}\Sigma\mathrm{U}_2(q) = \langle X_0,\phi\rangle = X_0.f$, noting that $X_0 \cap \langle\phi\rangle = \langle\phi^f\rangle$. In this setting, the two cases we need to consider are as described in (a) and (b) above, with T replaced by X_0. Note that in (b), the diagonal automorphism δ is the image of a diagonal matrix $\mathrm{diag}(\lambda^{q-1},1) \in \mathrm{GU}_2(q)$ with respect to the basis $\{u,v\}$ for U, where $\mathbb{F}_{q^2}^\times = \langle\lambda\rangle$.

We begin with the following result, which is the analogue of Lemma 4.3.11 for the groups with H of type $\mathrm{GL}_1(q^2)$ we are considering here. Note that the sufficient condition in the lemma is equivalent to the non-containment of $b^{\frac{1}{2}(q+1)}$ in a proper subfield of $\mathbb{F}_{q^2}$.

Lemma 4.3.20. *Suppose $G \cap \mathrm{PGL}_2(q) = T$ with q odd. Then $\{\alpha, \omega_b\}$ is a base for G if*

$$b^{\frac{1}{2}(q+1)(p^k-1)} \neq 1 \tag{4.3.8}$$

for all $0 < k < 2f$.

Proof. Suppose b satisfies the condition in (4.3.8) for all $0 < k < 2f$ and let us assume

$$x = AB^i\phi^j \in \langle \mathrm{GU}_2(q), \phi \rangle$$

fixes α and ω_b, where $A \in \mathrm{SU}_2(q)$, $B = \mathrm{diag}(\lambda^{q-1}, 1)$, $0 \leqslant i < q+1$, $0 \leqslant j < 2f$ with $j \neq f$, and $j > 0$ if $i > 0$. In order to prove that $\{\alpha, \omega_b\}$ is a base for G, it suffices to show that if x fixes α and ω_b, then $i = j = 0$ and $A = \pm I_2$. So let us assume x fixes α and ω_b, which means that A is either diagonal or anti-diagonal with respect to the basis $\{u, v\}$ for the natural $\mathrm{SU}_2(q)$-module U.

First assume $A = \mathrm{diag}(a, a^{-1})$ is diagonal, so $a^{q+1} = 1$. If x fixes the two spaces in ω_b, then

$$\begin{aligned}(u+bv)^x &= a\lambda^{i(q-1)}u + a^{-1}b^{p^j}v = \eta_1(u+bv)\\ (u-b^{-q}v)^x &= a\lambda^{i(q-1)}u - a^{-1}b^{-qp^j}v = \eta_2(u-b^{-q}v)\end{aligned}$$

for some $\eta_1, \eta_2 \in \mathbb{F}_{q^2}^\times$, whence

$$a^2\lambda^{i(q-1)} = b^{p^j-1} = b^{q(1-p^j)}. \tag{4.3.9}$$

Since $a^{q+1} = 1$ we get $(b^{q+1})^{(p^j-1)} = 1$, which implies $(b^{q+1})^{\frac{1}{2}(p^{2j}-1)} = 1$ and thus $2j = 0$ or $2f$ are the only possibilities. But we are assuming $j \neq f$, hence $j = 0$ and thus $i = 0$. Therefore, (4.3.9) gives $a^2 = 1$ and we conclude that $x = \pm I_2$.

Similarly, if x interchanges the spaces in ω_b, then

$$\begin{aligned}(u+bv)^x &= a\lambda^{i(q-1)}u + a^{-1}b^{p^j}v = \eta_1(u-b^{-q}v)\\ (u-b^{-q}v)^x &= a\lambda^{i(q-1)}u - a^{-1}b^{-qp^j}v = \eta_2(u+bv)\end{aligned}$$

for some $\eta_1, \eta_2 \in \mathbb{F}_{q^2}^\times$ and we deduce that

$$-a^2\lambda^{i(q-1)} = b^{p^j+q} = b^{-qp^j-1}. \tag{4.3.10}$$

In particular, since $a^{q+1} = 1$, it follows that

$$(b^{q+1})^{\frac{1}{2}(p^{j+f}+1)} = (-1)^{\frac{1}{2}(q+1)}\lambda^{\frac{1}{2}i(q^2-1)} = (-\lambda^{i(q-1)})^{\frac{1}{2}(q+1)}$$

and thus

$$(b^{q+1})^{\frac{1}{2}(p^{2j}-1)} = (b^{q+1})^{\frac{1}{2}(p^{2(j+f)}-1)} = (-\lambda^{i(q-1)})^{\frac{1}{2}(q+1)(p^{j+f}-1)} = 1.$$

Since (4.3.8) holds and $j \neq f$ we deduce that $j = 0$ is the only possibility, implying $i = 0$. Then (4.3.10) gives $b^{q+1} = b^{-q-1}$ and thus $b^{q+1} = \pm 1$. By construction we have $b^{q+1} \neq -1$ (since $\omega_b \in \Omega$), while (4.3.8) implies that $b^{q+1} \neq 1$. Therefore, we have reached a contradiction and this case does not arise.

Now let us assume x interchanges the two spaces in α, so

$$A = \begin{pmatrix} 0 & a \\ -a^{-1} & 0 \end{pmatrix}$$

is anti-diagonal and $a^{q+1} = 1$. If x fixes the spaces in ω_b, then

$$\begin{aligned} (u+bv)^x &= ab^{p^j}u - a^{-1}\lambda^{i(q-1)}v = \eta_1(u+bv) \\ (u-b^{-q}v)^x &= -ab^{-qp^j}u - a^{-1}\lambda^{i(q-1)}v = \eta_2(u-b^{-q}v) \end{aligned}$$

for some $\eta_1, \eta_2 \in \mathbb{F}_{q^2}^{\times}$ and we get

$$-a^2\lambda^{-i(q-1)} = b^{-p^j-1} = b^{q+qp^j}.$$

This implies that $(b^{q+1})^{\frac{1}{2}(p^{2j}-1)} = 1$, which leads to a contradiction as above. Finally, suppose x interchanges the two spaces in ω_b. Here we get

$$a^2\lambda^{i(q-1)} = b^{q-p^j} = b^{qp^j-1} \tag{4.3.11}$$

and thus $(b^{q+1})^{\frac{1}{2}(p^{f+j}-1)} = \lambda^{\frac{1}{2}i(q^2-1)} = \pm 1$ and so $(b^{q+1})^{\frac{1}{2}(p^{2(f+j)}-1)} = 1$. It follows that $j = 0$ and $i = 0$, so $(b^{q+1})^{\frac{1}{2}(p^f-1)} = 1$ and this is incompatible with (4.3.8). ■

Lemma 4.3.21. *Let $G = \mathrm{P\Sigma L}_2(q)$ with q odd. Then $\{\alpha, \omega_b\}$ is a base for G if and only if (4.3.8) holds for all $0 < k < 2f$.*

Proof. By Lemma 4.3.20, it suffices to show that if the condition in (4.3.8) fails to hold, then $\{\alpha, \omega_b\}$ is not a base for G. So let us assume k is an integer such that $0 < k < 2f$ and

$$b^{\frac{1}{2}(q+1)(p^k-1)} = 1.$$

If $k \neq f$ then by setting $j = k$ we deduce that (4.3.9) holds with $a = b^{(p^k-1)/2}$ and $i = 0$, otherwise (4.3.11) holds with $a = b^{(q-1)/2}$ and $i = j = 0$. In both cases we conclude that $\{\alpha, \omega_b\}$ is not a base and the result follows. ■

Remark 4.3.22. By inspecting the proofs of Lemmas 4.3.20 and 4.3.21, we deduce that if $G = T$ and q is odd, then $\{\alpha, \omega_b\}$ is a base for G if and only if b is a non-square in $\mathbb{F}_{q^2}$. The same criterion was established in the proof of [24, Theorem 10] for $q \equiv 3 \pmod 4$ and we note that a very similar argument can be used to reach the same conclusion when $q \equiv 1 \pmod 4$. In addition, we refer the reader to [24, Lemma 7.9] for a complete list of the subdegrees of $G = T$ when $q \geqslant 11$ is odd.

We can now reduce our main problems to the special case $G = \mathrm{P\Sigma L}_2(q)$.

Corollary 4.3.23. *Suppose $G \cap \mathrm{PGL}_2(q) = T$ and q is odd. Then the Saxl graph $\Sigma(G)$ contains $\Sigma(\mathrm{P\Sigma L}_2(q))$ as a subgraph.*

Proof. If $\{\alpha, \omega_b\}$ is a base for $\mathrm{P\Sigma L}_2(q)$, then Lemma 4.3.21 implies that (4.3.8) holds and thus $\{\alpha, \omega_b\}$ is a base for G by Lemma 4.3.20. ■

The following technical result is a key observation.

Corollary 4.3.24. *Let $G = \mathrm{P\Sigma L}_2(q)$ with q odd and let $b, c \in \mathbb{F}_{q^2}^{\times}$ be scalars such that $b^{q+1}, c^{q+1} \neq -1$ and $c \notin \{b, -b^{-q}\}$. Then $\{\omega_b, \omega_c\}$ is a base for G if and only if*

$$\frac{ba_1^{-2}(b+b^{-q}) + b^{-q}d}{a_1^{-2}(b+b^{-q}) - d} \in \{c, -c^{-q}\}$$

for scalars $a_1, d \in \mathbb{F}_{q^2}$ satisfying all of the following conditions:

(i) $a_1^{q+1} = 1 + b^{q+1}$;

(ii) $d^{q+1} \neq -1$ *and* $d \notin \{a_1^{-2}(b+b^{-q}), -b^{q+1}a_1^{-2}(b+b^{-q})\}$;

(iii) $d^{\frac{1}{2}(q+1)(p^k-1)} \neq 1$ *for all* $0 < k < 2f$.

Proof. Choose $a_1 \in \mathbb{F}_{q^2}$ such that $a_1^{q+1} = 1 + b^{q+1}$ and set $a_2 = -(b+b^{-q})a_1^{-1}$ (note that a_1 exists since $1 + b^{q+1} \in \mathbb{F}_q$). Then $a_2^{q+1} = 1 + b^{-(q+1)}$ and we deduce that both $a_1^{-1}(u+bv)$ and $a_2^{-1}(u - b^{-q}v)$ are unit vectors. Let $g \in X_0 = \mathrm{U}_2(q)$ be the image of the matrix

$$A = \begin{pmatrix} a_1^{-1} & a_2^{-1} \\ ba_1^{-1} & -b^{-q}a_2^{-1} \end{pmatrix} \in \mathrm{SU}_2(q),$$

which is expressed in terms of the basis $\{u, v\}$ for U. Note that $\alpha^g = \omega_b$.

First assume $\{\omega_b, \omega_c\}$ is a base for G, so $\omega_c = \omega_d^g$ for some neighbour ω_d of α in $\Sigma(G)$. Then $d^{q+1} \neq -1$ and Lemma 4.3.21 implies that d satisfies the condition in (iii). By applying g we get

$$(u + dv)^g = (a_1^{-1} + a_2^{-1}d)u + (ba_1^{-1} - b^{-q}a_2^{-1}d)v.$$

Since $\omega_c \neq \alpha$, the coefficients of u and v in this expression are nonzero and we deduce that d satisfies the remaining conditions in (ii). In particular,

$$\begin{aligned} \langle u + dv \rangle^g &= \left\langle u + \frac{ba_1^{-1}a_2 - b^{-q}d}{a_1^{-1}a_2 + d} v \right\rangle = \left\langle u + \frac{ba_1^{-2}(b+b^{-q}) + b^{-q}d}{a_1^{-2}(b+b^{-q}) - d} v \right\rangle \\ \langle u - d^{-q}v \rangle^g &= \left\langle u + \frac{ba_1^{-2}(b+b^{-q}) - b^{-q}d^{-q}}{a_1^{-2}(b+b^{-q}) + d^{-q}} v \right\rangle \end{aligned}$$

and we conclude that if $\{\omega_b, \omega_c\}$ is a base for G then all of the required conditions are satisfied.

Conversely, if c has the given form for scalars a_1 and d satisfying all of the given conditions, then $\{\alpha, \omega_d\}$ is a base for G (via the condition in (iii)) and $\omega_c = \omega_d^g$ for some $g \in T$ with $\omega_b = \alpha^g$. Therefore, $\{\omega_b, \omega_c\}$ is also a base for G. ■

We are now in a position to extend Theorem 4.3.9 by establishing ($\star$) for the base-two groups with H of type $\mathrm{GL}_1(q^2)$.

Lemma 4.3.25. *Property ($\star$) holds if H is of type $\mathrm{GL}_1(q^2)$ and $b(G) = 2$.*

Proof. We may assume $q > 27$ (see Proposition 4.3.10) and we recall that $b(G) = 2$ if and only if q is odd and $G \cap \mathrm{PGL}_2(q) = T$. In view of Corollary 4.3.23, we may assume that $G = \mathrm{P\Sigma L}_2(q)$. By Theorem 4.3.9, it suffices to show that if $\{\alpha, \omega_b\}$ is a base for G, then there exists $c \in \mathbb{F}_{q^2}^{\times}$ with $c^{q+1} \neq -1$ such that both $\{\alpha, \omega_c\}$ and $\{\omega_b, \omega_c\}$ are also bases. Note that $b^{q+1} \neq -1$ and b satisfies the condition in (4.3.8) for all $0 < k < 2f$ (see Lemma 4.3.21).

We claim that all of the above properties hold with $c = -b$. Clearly, we have $c^{q+1} = b^{q+1} \neq -1$ and $c^{\frac{1}{2}(q+1)(p^k-1)} \neq 1$ for all $0 < k < 2f$, so $\{\alpha, \omega_c\}$ is a base. It remains to prove that $\{\omega_b, \omega_c\}$ is a base.

As in Corollary 4.3.24, fix a scalar $a_1 \in \mathbb{F}_{q^2}^{\times}$ such that $a_1^{q+1} = 1 + b^{q+1}$ and set

$$d = \frac{2ba_1^{-2}(b + b^{-q})}{b - b^{-q}} \in \mathbb{F}_{q^2}^{\times}.$$

Then

$$c = \frac{ba_1^{-2}(b + b^{-q}) + b^{-q}d}{a_1^{-2}(b + b^{-q}) - d}$$

and it remains to show that d satisfies all the conditions in parts (ii) and (iii) of Corollary 4.3.24.

If $d \in \{a_1^{-2}(b + b^{-q}), -b^{q+1}a_1^{-2}(b + b^{-q})\}$ then $b^{q+1} = -1$, which is a contradiction. In addition, if we write $\alpha^g = \omega_b$ as in the proof of Corollary 4.3.24, then $\langle u + dv \rangle = \langle u + cv \rangle^{g^{-1}}$ and $\langle u - d^{-q}v \rangle = \langle u - c^{-q}v \rangle^{g^{-1}}$. Since $c^{q+1} \neq -1$, we have $u + cv \neq u - c^{-q}v$ and thus $u + dv \neq u - d^{-q}v$. Therefore, $d^{q+1} \neq -1$ and we conclude that d satisfies all of the conditions in part (ii) of Corollary 4.3.24.

Finally, we need to show that

$$d^{\frac{1}{2}(q+1)} = \pm 2\left(b^{\frac{1}{2}(q+1)} - b^{-\frac{1}{2}(q+1)}\right)^{-1}$$

is not contained in a proper subfield of $\mathbb{F}_{q^2}$. Set $e = b^{\frac{1}{2}(q+1)}$, which is not in a proper subfield by Lemma 4.3.21, and note that it suffices to show that $e - e^{-1}$ is also not contained in a proper subfield. Fix an integer $0 < k < 2f$ and observe that

$$(e - e^{-1})^{p^k} - (e - e^{-1}) = e^{-p^k}(e^{p^k+1} + 1)(e^{p^k-1} - 1),$$

so $e - e^{-1} \in \mathbb{F}_{p^k}$ if and only if this expression is 0. In view of (4.3.8), this holds if and only if $e^{p^k+1} = -1$. So let us assume this relation holds. Then $e^{p^{2k}-1} = (-1)^{p^k-1} = 1$ and thus $2k = 0$ or $2f$. If $2k = 2f$ then $k = f$ and so $e^{q+1} = e^{p^k+1} = -1$. This implies that

$$-1 = e^{q+1} = b^{\frac{1}{2}(q+1)^2} = b^{\frac{1}{2}(q^2+1)}b^q = -b^{q+1}$$

and so b is a square, which is incompatible with (4.3.8). Therefore $k = 0$, so $e^2 = -1$ and $e - e^{-1} = -2e^{-1}$. The result now follows since Lemma 4.3.21 implies that e^{-1} is not contained in a proper subfield of $\mathbb{F}_{q^2}$. ■

Lemma 4.3.26. *Suppose H is of type $\mathrm{GL}_1(q^2)$. Then G has a unique regular suborbit if and only if $G = \mathrm{L}_2(5)$ or $\mathrm{L}_2(9).2 = \mathrm{M}_{10}$.*

Proof. In view of Proposition 4.3.10 and Corollary 4.3.23, we may assume $q > 27$ is odd and $G = \mathrm{P\Sigma L}_2(q)$. Let r be the number of regular suborbits of G. If q is a prime then $G = T$ and [24, Lemma 7.9] gives $r = (q-\ell)/4$, where $q \equiv \ell \pmod 4$ with $\ell \in \{1,3\}$. For the remainder, we may assume $q > p$.

Let λ be a primitive element of $\mathbb{F}_{q^2}$. Then by Lemma 4.3.20, we see that $\{\alpha, \omega_\lambda\}$ is a base for G. Therefore, the valency of $\Sigma(G)$ is at least $\phi(q^2-1)/2$, where ϕ is Euler's function and thus $r \geqslant \phi(q^2-1)/2f(q+1)$ since $|H| = f(q+1)$. By applying the lower bound in Lemma 4.3.17 we deduce that

$$\frac{\phi(q^2-1)}{2f(q+1)} \geqslant 2$$

for $q > 27$ and the desired result follows. ■

Proposition 4.3.27. *Suppose H is of type $\mathrm{GL}_1(q^2)$. Then the following hold:*

(i) Property $(\star)$ holds.

(ii) $\Sigma(G)$ is G-arc-transitive if and only if $G = \mathrm{L}_2(5)$, $\mathrm{P\Gamma L}_2(8)$ or $\mathrm{L}_2(9).2 = \mathrm{M}_{10}$.

(iii) G is semi-Frobenius if and only if $b(G) > 2$.

Proof. In view of Lemmas 4.3.25 and 4.3.26, it suffices to prove (iii), and we only need to show that G is semi-Frobenius if $\mathrm{PGL}_2(q) \leqslant G$, in which case $b(G) = 3$.

Fix a generator μ of $\mathbb{F}_{q^2}^\times$, and let $\zeta \in \mathbb{F}_{q^2}^\times$ with $\zeta^{q+1} \neq -1$. We shall prove by contradiction that if $-\mu^{-(q-1)} \in X := \{\zeta^2, -\zeta^{-(q-1)}\}$, then $-(\mu^{-1})^{-(q-1)} \notin X$. First suppose that $-\mu^{-(q-1)} = -(\mu^{-1})^{-(q-1)}$. Then $1 = \mu^{2(q-1)}$, contradicting the fact that $|\mu| = q^2-1 > 2(q-1)$. Without loss of generality, we may therefore assume that $\zeta^2 = -\mu^{-(q-1)}$. Since $-1 = \mu^{(q^2-1)/(2,q-1)}$ and $\zeta^{q+1} \neq -1$, we deduce that $q \equiv 1 \pmod 4$ and $\zeta = \pm\mu^{(q-1)^2/4}$. It follows that $\zeta^{-(q-1)} = \mu^{-(q-1)^3/4}$. If $-(\mu^{-1})^{-(q-1)}$ lies in X, then it is equal to $-\zeta^{-(q-1)}$, and so $1 = \mu^{q-1+(q-1)^3/4}$. Hence $q-1+(q-1)^3/4 = k(q^2-1)$ for some positive integer k, and solving this cubic equation shows that $\sqrt{k^2+2k-1}$ is an integer. However, $k^2+2k-1 = (k+1)^2-2$ is not a square, a contradiction. We have therefore proved our claim.

Now, choose $\nu \in \{\mu, \mu^{-1}\}$ such that $-\nu^{-(q-1)} \notin X$. We shall show that $\{\alpha, \omega_\nu, \omega_\zeta\}$ is a base for G (recall the notation for points in Ω from (4.3.7)). Note that the group $\Gamma\mathrm{U}_2(q) = \langle \mathrm{GU}_2(q), \phi\rangle$ satisfies $G \leqslant \mathrm{Aut}(\mathrm{U}_2(q)) \cong \Gamma\mathrm{U}_2(q)/Z(\mathrm{GU}_2(q))$. Following the proof of [14, Lemma 4.8], we see that the pointwise stabiliser of $\{\alpha, \omega_\nu\}$ in $\Gamma\mathrm{U}_2(q)$ is generated by $Z(\mathrm{GU}_2(q))$ along with

$$M := \begin{pmatrix} 0 & -\nu^{-(q-1)} \\ 1 & 0 \end{pmatrix}.$$

Note that $M^2 \in Z(\mathrm{GU}_2(q))$. Hence it suffices to prove that M does not fix ω_ζ. It is easy to see that if M fixes each of the two subspaces in ω_ζ, then $-\nu^{-(q-1)} = \zeta^2$, and if M swaps these subspaces, then we have $-\nu^{-(q-1)} = -\zeta^{-(q-1)}$. However, $-\nu^{-(q-1)} \notin X$, and so neither of these cases occurs. Therefore, M does not fix ω_ζ, and so $\{\alpha, \omega_\nu, \omega_\zeta\}$ is a base for G. It follows immediately that G is semi-Frobenius. ■

The proofs of Theorems 4.2(i), 4.3 and 4.6 are complete by combining Lemmas 4.3.4, 4.3.5, 4.3.6, 4.3.7, 4.3.8 and Propositions 4.3.19, 4.3.27.

4.4 Sporadic groups

Let G be a primitive almost simple group with sporadic socle T and point stabiliser H. Here the base size $b(G)$ is computed in [30], apart from two special cases involving $G = \mathbb{B}$, where it was proved in the same paper that $b(G) \in \{2,3\}$. Later on, these special cases were handled in [104]. In particular, we have $b(G) \leqslant 7$ in every case, with equality if and only if $(G,H) = (\mathrm{M}_{24}, \mathrm{M}_{23})$.

In this section, we will establish Theorem 4.2(ii) by showing that ($\star$) holds if $b(G) \geqslant 3$. For partial evidence of Conjecture II for the base-two groups, we refer the reader to [20, Section 6]. For example, [20, Theorem 6.1] shows that property ($\star$) holds for every base-two group G with

$$G \in \{\mathrm{M}_{11}, \mathrm{M}_{12}, \mathrm{M}_{22}, \mathrm{M}_{23}, \mathrm{M}_{24}, \mathrm{J}_1, \mathrm{J}_2, \mathrm{J}_3, \mathrm{HS}, \mathrm{Suz}, \mathrm{McL}, \mathrm{Ru}, \mathrm{He}, \mathrm{O'N}, \mathrm{Co}_2, \mathrm{Co}_3, \mathrm{Fi}_{22}\}.$$

We start with the following result concerning the completeness of $\Sigma(G)$.

Proposition 4.4.1. *Let G be a primitive almost simple group with sporadic socle T and point stabiliser H, such that $b(G) \geqslant 3$.*

(i) If $b(G) \geqslant 5$, then G is semi-Frobenius.

(ii) If $T \notin \{\mathrm{Co}_1, \mathrm{J}_4, \mathrm{Fi}_{24}', \mathbb{B}, \mathbb{M}\}$, then G is semi-Frobenius if and only if $(G,H,b(G))$ does not appear in Table 4.2.

Proof. First note that if $b(G) \geqslant 5$ and $T \in \mathscr{A} := \{\mathrm{Co}_1, \mathrm{J}_4, \mathrm{Fi}_{24}', \mathbb{B}, \mathbb{M}\}$, then $T \in \{\mathrm{Co}_1, \mathrm{Fi}_{24}'\}$, and H is a maximal subgroup of G of minimal index. Since G is transitive, it is semi-Frobenius if and only if, for a fixed $\omega \in \Omega$ and each point $\alpha \neq \omega$ in a set of orbit representatives of G_ω, the set $\{\omega, \alpha\}$ extends to a base for G of size $b(G)$. For all groups G satisfying $T \notin \mathscr{A}$ or $b(G) \geqslant 5$, except for one special case mentioned at the end of the proof, we use MAGMA to directly check this condition on orbit representatives (see Section 4.2.5). Here if $T \notin \{\mathrm{Ly}, \mathrm{Th}\}$, then we construct G by implementing the approach explained in Section 4.2.1. If instead $T \in \{\mathrm{Ly}, \mathrm{Th}\}$, we construct a matrix group $\widehat{G}$ isomorphic to G and a subgroup $\widehat{H} < \widehat{G}$ isomorphic to H using generators from [123]. We then obtain G as the permutation group induced by the action of $\widehat{G}$ on the orbit $U^{\widehat{G}}$, where U is a low-dimensional $\widehat{H}$-submodule of the module corresponding to $\widehat{G}$. This will be discussed in Appendix A.1.2.5 in more detail.

G	H	$b(G)$	G	H	$b(G)$	G	H	$b(G)$
M_{12}	$\mathrm{L}_2(11)$	3	McL	3^4:M_{10}	3	HN	A_{12}	3
							2.HS.2	3
$\mathrm{M}_{12}.2$	$\mathrm{L}_2(11).2$	3	McL.2	3^4:$(\mathrm{M}_{10} \times 2)$	3			
	$\mathrm{L}_2(11).2$	3				HN.2	S_{12}	3
			HS	$\mathrm{L}_3(4)$:2	3		4.HS.2	3
M_{22}	2^4:S_5	3		S_8	3			
	2^3:$\mathrm{L}_3(2)$	3				He	$2^2.\mathrm{L}_3(4).S_3$	3
			HS.2	$2^5.S_6$	3			
$\mathrm{M}_{22}.2$	2^5:S_5	3		$4^3.(2 \times \mathrm{L}_3(2))$	3	He.2	$2^2.\mathrm{L}_3(4).D_{12}$	3
	2^3:$\mathrm{L}_3(2) \times 2$	3						
			Co_3	$\mathrm{U}_4(3).2.2$	3	Suz	$G_2(4)$	4
M_{23}	A_8	3		M_{23}	3		$3.\mathrm{U}_4(3)$:2	3
	2^4:$(3 \times A_5)$:2	3					$\mathrm{U}_5(2)$	3
			Co_2	HS:2	3		$2^{1+6}.\mathrm{U}_4(2)$	3
M_{24}	$\mathrm{M}_{22}.2$	4		$(2^4 \times 2^{1+6}).A_8$	3		$3^5.\mathrm{M}_{11}$	3
	$\mathrm{M}_{12}.2$	3		$\mathrm{U}_4(3)$:D_8	3			
	2^6:$3.S_6$	3				Suz.2	$G_2(4).2$	4
	$\mathrm{L}_3(4)$:S_3	3	Fi_{22}	2^{10}:M_{22}	3		$3.\mathrm{U}_4(3).2.2$	3
				2^6:$\mathrm{Sp}_6(2)$	3		$\mathrm{U}_5(2)$:2	3
J_2	$3.A_6.2$	3		$(2 \times 2^{1+8})$:$(\mathrm{U}_4(2)$:$2)$	3		$2^{1+6}.\mathrm{U}_4(2).2$	3
	$2^{1+4}.A_5$	3					$3^5.(\mathrm{M}_{11} \times 2)$	3
			$\mathrm{Fi}_{22}.2$	2^7:$\mathrm{Sp}_6(2)$	3			
$\mathrm{J}_2.2$	$3.A_6.2.2$	3		$(2 \times 2^{1+8}$:$\mathrm{U}_4(2)$:$2)$:2	3	Fi_{23}	$\mathrm{P}\Omega_8^+(3).S_3$	4
	$2^{1+4}.A_5.2$	3		$\mathrm{U}_4(3).2.2 \times S_3$	3		$2^2.\mathrm{U}_6(2).2$	3
	2^{2+4}:$(3 \times S_3).2$	3		2^{5+8}:$(S_3 \times S_6)$	3		$\mathrm{Sp}_8(2)$	3
							$2^{11}.\mathrm{M}_{23}$	3

Table 4.2: Primitive almost simple sporadic groups that are not semi-Frobenius

The one special case mentioned above is where $G = \mathrm{Fi}_{23}$ and $H = 3^{1+8}.2^{1+6}.3^{1+2}.2S_4$, with $b(G) = 3$. Here, the index of H in G is too large for the permutation group G to be constructed directly using `CosetAction`. Therefore, we search through the elements of G for a full set of representatives of the (H,H) double cosets, with the aid of the `DoubleCosetCanonical` function (see Section 4.2.4). For each representative $x \notin H$, we verify that there exists an element $y \in G$ such that $H \cap H^x \cap H^y = 1$. This implies the above condition on orbit representatives of G_ω, i.e. G is semi-Frobenius. ■

Remark 4.4.2. In Table 4.2, there are two cases with $(G,H) = (\mathrm{M}_{12}.2, \mathrm{L}_2(11).2)$, where exactly one of the two groups $H = \mathrm{L}_2(11).2$ is such that $H \cap T$ is maximal in T.

Remark 4.4.3. Using computational methods from the proof of Proposition 4.4.1, we can show that G is semi-Frobenius if $T = \mathrm{Co}_1$ and $b(G) = 4$ (so that $H = 3.\mathrm{Suz}$:2), and that G is not semi-Frobenius if $T \in \{\mathrm{Co}_1, \mathrm{J}_4\}$, $b(G) = 3$, and $|\Omega| \leqslant 2 \times 10^8$. Determining which of the remaining primitive groups with $T \in \{\mathrm{Co}_1, \mathrm{J}_4, \mathrm{Fi}_{24}', \mathbb{B}, \mathbb{M}\}$ are semi-Frobenius will likely require alternative approaches, due to the extremely large degrees of these groups.

In [20, Section 6], Burness and Giudici show that many almost simple sporadic groups G with $b(G) = 2$ satisfy Conjecture II. We now extend their results (and Proposition 4.4.1) to the groups with $b(G) \geqslant 3$ as follows, which is Theorem 4.2(ii).

Theorem 4.4.4. *Let G be a primitive almost simple group with sporadic socle, such that $b(G) \geqslant 3$. Then any two vertices in $\Sigma(G)$ have a common neighbour.*

Proof. We first observe that $(\star)$ holds if and only if, for a fixed $\omega \in \Omega$, each point $\alpha \neq \omega$ in a set of orbit representatives for G_ω is adjacent to a neighbour of ω. In particular, this is the case if the valency $\mathrm{val}(G)$ of G satisfies $\mathrm{val}(G)/|\Omega| > 1/2$. Now, by Proposition 4.4.1, it suffices to consider the case where either G and H appear in Table 4.2, or $\mathrm{soc}(G) \in \{\mathrm{Co}_1, \mathrm{J}_4, \mathrm{Fi}_{24}', \mathbb{B}, \mathbb{M}\}$ and $b(G) \in \{3,4\}$.

If G and H appear in Table 4.2, or if $G = \mathrm{Co}_1$ and $H = 2^{11}{:}\mathrm{M}_{24}$ or Co_3, then we construct the permutation group G in MAGMA via our usual method, and verify the above condition on orbit representatives. In particular, we observe that among these groups, $\mathrm{val}(G)/|\Omega| \leqslant 1/2$ if and only if $G = \mathrm{M}_{12}.2$, $H = \mathrm{L}_2(11).2$ and $H \cap T$ is maximal in T. Even in this case, computations show that $(\star)$ holds.

Next, suppose that $G = \mathrm{Fi}_{24}$ and $H = (2 \times 2.\mathrm{Fi}_{22}){:}2$, so that $b(G) = 3$. We construct G in MAGMA using the function AutomorphismGroupSimpleGroup, and H using generators from the Web ATLAS [123] (Version 2.0). Computations show that there exist elements $r, s \in G \setminus H$ such that $H \cap H^r \cap H^s = 1$ and

$$|HrH| = 1429430650440473640960000 > \frac{1}{2}|G|.$$

Thus $\omega \in \Omega$ is adjacent in $\Sigma(G)$ to each point in a G_ω-orbit of size $a := |HrH|/|H|$, and so $\mathrm{val}(G)/|\Omega| \geqslant a/|\Omega| = |HrH|/|G| > 1/2$. The MAGMA code will be given in Appendix A.1.2.5.

For the remaining cases, let $R(G)$ be a set of representatives for the G-conjugacy classes of elements of H of prime order. Recall that $(\star)$ holds if

$$\widehat{Q}(G, b(G)) = \sum_{x \in R(G)} \frac{|x^G \cap H|^{b(G)}}{|x^G|^{b(G)-1}} < 1/2.$$

In each case, the character table of G is available in the GAP Character Table Library [12] and we can use the Maxes function to access the character table of the maximal subgroup H (for the case $(G,H) = (\mathbb{M}, 2.\mathbb{B})$, the function Maxes is not available for G, and we directly construct the character table of H via CharacterTable("2.B")). Moreover, apart from a single exception $(G,H) = (\mathbb{B}, (2^2 \times F_4(2)){:}2)$, [12] also stores the fusion map from H-classes to G-classes and this allows us to compute precise fixed point ratios and subsequently determine the exact value of $\widehat{Q}(G, b(G))$ and verify that $\widehat{Q}(G, b(G)) < 1/2$ (see Appendix A.2.1). Note that if $G = \mathbb{B}$ and $H = (2^2 \times F_4(2)){:}2$, then the fusion of H-conjugacy classes in G is not stored in GAP. However, all possibilities for this fusion, as returned via the PossibleClassFusions function, yield the same value for $\widehat{Q}(G, b(G))$. ■

4.5 Soluble stabilisers

In this section, we will prove Theorems 4.2(iii) and 4.5. Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive group with socle T and soluble point stabiliser H. Recall that the exact base size of G has been computed in [14]. In particular, we have $b(G) \leqslant 5$, which is the best possible bound (for example, $b(G) = 5$ if $G = S_8$ and $H = S_4 \wr S_2$).

As a key ingredient in the proofs of our main theorems, we will establish the following theorem for base-two groups in this section. Here

$$\mathscr{G} = \{\text{almost simple primitive groups } G \text{ with } b(G) = 2 \text{ and } H = G_\alpha \text{ soluble}\}.$$

Theorem 4.5.1. *Suppose $G \in \mathscr{G}$ has socle $T \ncong \mathrm{L}_2(q)$ and point stabiliser H. Then either $Q(G,2) < 1/4$, or (G,H) is one of the cases in Tables 4.3 and 4.4.*

Remark 4.5.2. Theorem 4.5.1 will be a key ingredient in the proof of Proposition 4.5.14 classifying the base-two almost simple primitive groups with soluble stabilisers and $\mathrm{reg}(G) \leqslant 4$. More precisely, it will be proved that there is no group with $Q(G,2) < 1/4$ and $\mathrm{reg}(G) \leqslant 4$.

Remark 4.5.3. We make several comments concerning Tables 4.3 and 4.4.

(a) If G is a classical group, we record the type of H in the second column as before (see Section 2.2.3), which we recall provides an approximate description of the group theoretic structure of H. For non-classical groups, the type of H refers to the precise structure of H.

(b) In both tables, the number $r = r(G)$ of regular suborbits of G is listed in the third column.

(c) We use the standard ATLAS [40] notation for describing the almost simple groups of the form $\mathrm{L}_4(3).2$. In particular, $\mathrm{L}_4(3).2_2$ and $\mathrm{L}_4(3).2_3$ contain involutory graph automorphisms x with $C_T(x) = \mathrm{PSp}_4(3).2$ and $\mathrm{PSO}_4^-(3).2$, respectively.

(d) Suppose $G = T.S_3$, where $T = \mathrm{L}_3(4)$ and H is of type $\mathrm{GL}_1(3^4)$. There are two groups of this form, up to conjugacy in $\mathrm{Aut}(T)$, and we find that $r = 6$ and $Q(G,2) = 17/80$ if $G = T.\langle \delta, \phi \rangle$, whereas $r = 3$ and $Q(G,2) = 97/160$ if $G = T.\langle \delta, \gamma \rangle$. Here we are using the notation for automorphisms in Example 2.2.3, where δ, ϕ and γ denote diagonal, field and graph automorphisms, respectively. Following [11], we adopt similar notation to describe the relevant groups with $T = \mathrm{U}_4(3)$ or $\mathrm{P\Omega}_8^+(3)$ (in the latter case, γ is an involutory graph automorphism).

4.5.1 Alternating and sporadic groups

Proposition 4.5.4. *The conclusion to Theorem 4.5.1 holds if T is an alternating group.*

G	Type of H	r	$Q(G,2)$
A_9	$\mathrm{ASL}_2(3)$	2	17/35
S_7	$\mathrm{AGL}_1(7)$	1	13/20
M_{11}	$2.S_4$	1	39/55
M_{12}	$A_4 \times S_3$	13	16/55
$\mathrm{M}_{12}.2$	$S_4 \times S_3$	4	31/55
J_1	19:6	9	257/770
	$D_6 \times D_{10}$	34	443/1463
J_2	$5^2{:}D_{12}$	2	59/84
$\mathrm{J}_2.2$	$5^2{:}(4 \times S_3)$	1	59/84
$\mathrm{J}_3.2$	$3^{2+1+2}{:}8.2$	3	886/1615
	$2^{2+4}{:}(S_3 \times S_3)$	10	457/969
HS.2	$5^{1+2}.[2^5]$	3	106/231
McL.2	$2^{2+4}{:}(S_3 \times S_3)$	228	9419/28875
He.2	$2^{4+4}.(S_3 \times S_3).2$	5	23011/29155
Suz	$3^{2+4}{:}2.(A_4 \times 2^2).2$	16	7529/25025
Suz.2	$3^{2+4}{:}2.(S_4 \times D_8)$	4	16277/25025
HN	$5^{1+4}{:}2^{1+4}.5.4$	47	332152/1066527
HN.2	$5^{1+4}{:}2^{1+4}.5.4.2$	22	34457/96957
${}^2B_2(8)$	13:4	7	7/20
${}^2B_2(8).3$	13:12	2	31/70
${}^2F_4(2)'$	$5^2{:}4A_4$	6	27/52
${}^2F_4(2)$	$5^2{:}4S_4$	3	27/52
$G_2(3)$	$(\mathrm{SL}_2(3) \circ \mathrm{SL}_2(3)).2$	4	563/819
$G_2(3).2$	$(\mathrm{SL}_2(3) \circ \mathrm{SL}_2(3)).2.2$	1	691/819
$\mathrm{L}_4(3)$	$\mathrm{O}_4^+(3)$	6	131/195
$\mathrm{L}_4(3).2_3$	$\mathrm{O}_4^+(3)$	3	131/195
$\mathrm{L}_4(3).2_2$	$\mathrm{O}_4^+(3)$	2	457/585
$\mathrm{L}_4(3).2_1 = \mathrm{PGL}_4(3)$	$\mathrm{O}_4^+(3)$	1	521/585
$\mathrm{L}_3(9).2^2$	$\mathrm{GL}_1(9) \wr S_3$	48	4093/12285
$\mathrm{L}_3(5)$	$\mathrm{GL}_1(5) \wr S_3$	30	199/775
$\mathrm{L}_3(5).2$	$\mathrm{GL}_1(5) \wr S_3$	13	1379/3875
	$\mathrm{GL}_1(5^3)$	13	791/2000
$\mathrm{L}_3(4).2 \neq \mathrm{P\Sigma L}_3(4)$	$\mathrm{GU}_3(2)$	1	17/35
$\mathrm{L}_3(4).6$	$\mathrm{GL}_1(4^3)$	5	11/32
$\mathrm{L}_3(4).S_3 = T.\langle\delta,\gamma\rangle$	$\mathrm{GL}_1(4^3)$	3	97/160
$\mathrm{L}_3(4).D_{12}$	$\mathrm{GL}_1(4^3)$	1	59/80
$\mathrm{L}_3(3)$	$\mathrm{GL}_1(3^3)$	2	11/24
	$\mathrm{O}_3(3)$	5	19/39
$\mathrm{L}_3(3).2$	$\mathrm{O}_3(3)$	2	23/39

Table 4.3: The groups in $\mathscr{G}$ with $Q(G,2) \geqslant 1/4$, part I

G	Type of H	r	$Q(G,2)$
$\mathrm{U}_4(5).2^2$	$\mathrm{GU}_1(5)\wr S_4$	409	361747/1421875
$\mathrm{U}_4(4)$	$\mathrm{GU}_1(4)\wr S_4$	80	259/884
$\mathrm{U}_4(4).2$	$\mathrm{GU}_1(4)\wr S_4$	30	1661/3536
$\mathrm{U}_4(4).4$	$\mathrm{GU}_1(4)\wr S_4$	15	1661/3536
$\mathrm{U}_4(3)$	$\mathrm{GU}_2(3)\wr S_2$	1	187/315
$\mathrm{U}_4(3).2 = \mathrm{U}_4(3).\langle\delta^2\phi\rangle$	$\mathrm{GU}_1(3)\wr S_4$	4	1811/2835
$\mathrm{U}_4(3).2^2 \neq \mathrm{U}_4(3).\langle\delta^2,\phi\rangle$	$\mathrm{GU}_1(3)\wr S_4$	1	2323/2835
$\mathrm{U}_4(3).4$	$\mathrm{GU}_1(3)\wr S_4$	1	2323/2835
$\mathrm{U}_3(9).2$	$\mathrm{GU}_1(9)\wr S_3$	40	1913/5913
$\mathrm{U}_3(9).4$	$\mathrm{GU}_1(9)\wr S_3$	20	1913/5913
$\mathrm{U}_3(8).2$	$\mathrm{GU}_1(8)\wr S_3$	78	1097/4256
$\mathrm{U}_3(8).S_3$	$\mathrm{GU}_1(8)\wr S_3$	19	205/448
$\mathrm{U}_3(8).6$	$\mathrm{GU}_1(8)\wr S_3$	25	2437/8512
$\mathrm{U}_3(8).(3\times S_3)$	$\mathrm{GU}_1(8)\wr S_3$	6	2069/4256
$\mathrm{U}_3(7)$	$\mathrm{GU}_1(7)\wr S_3$	27	4381/14749
$\mathrm{U}_3(7).2$	$\mathrm{GU}_1(7)\wr S_3$	10	7069/14749
$\mathrm{U}_3(5).3$	$\mathrm{GU}_1(5)\wr S_3$	3	551/875
	$3^{1+2}.\mathrm{Sp}_2(3)$	5	67/175
$\mathrm{U}_3(5).S_3$	$\mathrm{GU}_1(5)\wr S_3$	1	659/875
	$3^{1+2}.\mathrm{Sp}_2(3)$	2	443/875
$\mathrm{U}_3(4)$	$\mathrm{GU}_1(4)\wr S_3$	1	133/208
$\mathrm{PSp}_6(3)$	$\mathrm{Sp}_2(3)\wr S_3$	1	853/1365
$\mathrm{Sp}_4(4).4$	$\mathrm{O}_2^-(4)\wr S_2$	2	103/153
$\mathrm{P\Omega}_8^+(3)$	$\mathrm{O}_4^+(3)\wr S_2$	12	45041/61425
$\mathrm{P\Omega}_8^+(3).2 = \mathrm{PSO}_8^+(3)$	$\mathrm{O}_4^+(3)\wr S_2$	4	151507/184275
$\mathrm{P\Omega}_8^+(3).2 = \mathrm{P\Omega}_8^+(3).\langle\gamma\rangle$	$\mathrm{O}_4^+(3)\wr S_2$	3	53233/61425
$\mathrm{P\Omega}_8^+(3).3$	$\mathrm{O}_4^+(3)\wr S_2$	3	16379/20475
$\mathrm{P\Omega}_8^+(3).2^2$	$\mathrm{O}_4^+(3)\wr S_2$	1	167891/184275
$\mathrm{P\Omega}_8^+(3).4$	$\mathrm{O}_4^+(3)\wr S_2$	2	151507/184275
$\mathrm{P\Omega}_8^+(3).S_4$	$\mathrm{O}_2^-(3)\wr S_4$	823	17810761/44778825
$\Omega_8^+(2).3$	$\mathrm{O}_2^-(2)\times\mathrm{GU}_3(2)$	1	2071/2800
$\Omega_7(3)$	$\mathrm{O}_4^+(3)\perp\mathrm{O}_3(3)$	5	1945/2457
$\mathrm{SO}_7(3)$	$\mathrm{O}_4^+(3)\perp\mathrm{O}_3(3)$	1	11261/12285

Table 4.4: The groups in $\mathscr{G}$ with $Q(G,2)\geqslant 1/4$, part II

Proof. Let $T = A_m$ be the socle of G. If $m \leqslant 12$ then the result is easily checked using MAGMA (see Section 4.2), so let us assume $m \geqslant 13$. By inspecting [87, Table 14] and [14, Table 4] we deduce that m is a prime and $H = \mathrm{AGL}_1(m) \cap G$, in which case

$$|H| \leqslant m(m-1) = a, \; |x^G| \geqslant \frac{m!}{((m-1)/2)!2^{(m-1)/2}} = b$$

for all $x \in H$ of prime order (minimal if x is an involution, noting that x has at most one fixed point on $\{1,\dots,m\}$). In view of Lemma 2.4.1, this gives $\widehat{Q}(G,2) < a^2/b < 1/4$ and the result follows. ■

Proposition 4.5.5. *The conclusion to Theorem 4.5.1 holds if T is a sporadic group.*

Proof. First assume G is not the Baby Monster $\mathbb{B}$ nor the Monster $\mathbb{M}$. In the remaining cases we first use the GAP Character Table Library [12] to identify the relevant groups with $\widehat{Q}(G,2) \geqslant 1/4$, implementing the method described in the proof of Theorem 4.4.4. This reduces the problem to a small number of cases that require further attention. To handle these groups, we adopt the method described in Section 4.2.4 to compute $Q(G,2)$ precisely. First we use the function `AutomorphismGroupSimpleGroup` to construct G as a permutation group and we obtain H via the `MaximalSubgroups` function (for $T = \mathrm{HN}$ and $H \cap T = 5^{1+4}.2^{1+4}.5.4$ we construct H using the generators given in the Web ATLAS [123]). Next we use `DoubleCosetRepresentatives` to construct a complete set R of (H,H) double coset representatives and this allows us to calculate $Q(G,2)$ via (3.1.1) and (4.2.2) (we thank Eamonn O'Brien for his assistance with this computation in the special case where $T = \mathrm{HN}$ and $H \cap T = 5^{1+4}.2^{1+4}.5.4$). In this way, we can read off the groups with $Q(G,2) \geqslant 1/4$ and they are recorded in Table 4.3.

Finally, suppose $G = \mathbb{B}$ or $\mathbb{M}$. If $G = \mathbb{B}$ then $H = [3^{11}].(S_4 \times 2S_4)$ or 47:23; in both cases we can use [12] and the `Maxes` function as above to show that $\widehat{Q}(G,2) < 1/4$. Similarly, if $G = \mathbb{M}$ then $H = 13^{1+2}{:}(3 \times 4S_4)$ or 41:40 and once again we can use [12] to verify the bound $\widehat{Q}(G,2) < 1/4$ (here we use `NamesOfFusionSources` in place of `Maxes` to access the character table of H and the fusion maps, since the function `Maxes` is not available for $\mathbb{M}$). ■

4.5.2 Exceptional groups

Next let us turn to the groups in $\mathscr{G}$ where T is an exceptional group of Lie type over $\mathbb{F}_q$ with $q = p^f$ for a prime p. Here we exclude the cases where T is isomorphic to a two-dimensional linear group, since these groups were already handled in Section 4.3, so $T \neq {}^2G_2(3)' \cong \mathrm{L}_2(8)$.

As noted in the proof of [14, Proposition 7.1], the condition $b(G) = 2$ implies that H is a maximal rank subgroup (that is, H contains a maximal torus of G). More precisely, either $H = N_G(R)$ for some maximal torus R of T (see [93, Table 5.2]), or (G,H) is one of the cases recorded in Table 4.5.

Lemma 4.5.6. *The conclusion to Theorem 4.5.1 holds if T is an exceptional group of Lie type and H is the normaliser of a maximal torus.*

	T	Type of H
(a)	$G_2(3)$	$\mathrm{SL}_2(3)^2$
(b)	${}^3D_4(2)$	$3 \times \mathrm{SU}_3(2)$
(c)	${}^2F_4(2)'$	$\mathrm{SU}_3(2)$
(d)	$F_4(2)$	$\mathrm{SU}_3(2)^2$
(e)	${}^2E_6(2)$	$\mathrm{SU}_3(2)^3$
(f)	$E_8(2)$	$\mathrm{SU}_3(2)^4$

Table 4.5: The groups in $\mathscr{G}$, T exceptional, $H \neq N_G(R)$

Proof. The possibilities for H are recorded in [93, Table 5.2] and [31, Proposition 4.2] states that $b(G) = 2$ whenever H is the normaliser of a maximal torus (soluble or otherwise). We proceed by carefully inspecting the proof of [31, Proposition 4.2] in the relevant cases with H soluble.

If $T = E_8(q)$ then one checks that the bound on $\widehat{Q}(G,2)$ in the proof of [31, Lemma 4.3] is sufficient and we note that H is insoluble when $T = E_7(q)$.

Next assume $T = E_6^{\varepsilon}(q)$. Here the proof of [31, Lemma 4.11] yields $\widehat{Q}(G,2) < q^{-1}$ if $q \geqslant 5$, so we may assume $q \leqslant 4$ and

$$N_L(H_0) = (q^2 + \varepsilon q + 1)^3.3^{1+2}.\mathrm{SL}_2(3),$$

where $H_0 = H \cap T$, $L = \mathrm{Inndiag}(T)$ and $(q,\varepsilon) \neq (2,-)$. One checks that the upper bound on $\widehat{Q}(G,2)$ presented in the proof of [31, Lemma 4.11] is sufficient unless $\varepsilon = +$ and $q \leqslant 3$. If $q = 3$ then H does not contain any long root elements (see [31, Corollary 2.13], for example) and by bounding the contribution to $\widehat{Q}(G,2)$ from the remaining elements of prime order, as in the proof of [31, Lemma 4.11], we deduce that $\widehat{Q}(G,2) < 1/4$.

Now suppose $(q,\varepsilon) = (2,+)$. As explained in the proof of [31, Lemma 4.11], we can use MAGMA to construct H as a subgroup of $E_7(8)$ (see [32, Example 1.11] for the details). If $x \in H$ has odd prime order then $|x^G| > 2^{31} = b_1$ and we calculate that $i_3(H) = 11438$ and $i_7(H) = 342$, so Lemma 2.4.1 implies that the contribution to $\widehat{Q}(G,2)$ from elements of odd prime order is less than a_1^2/b_1, where $a_1 = 11780$. Now assume $x \in H$ is an involution. We find that H_0 contains $a_2 = 441$ involutions, so the contribution from these elements is less than a_2^2/b_2, where $b_2 = 2^{21}$. Similarly, there are $a_3 = 406$ involutions in $H_0.2 \setminus H_0$, each of which acts on T as a graph automorphism. Therefore $|x^G| > \frac{1}{3}2^{25} = b_3$ and we conclude that

$$\widehat{Q}(G,2) < \sum_{i=1}^{3} a_i^2/b_i < \frac{1}{4}. \tag{4.5.1}$$

Next assume $T = F_4(q)$, so q is even and G contains graph automorphisms (see [93, Table 5.2]). By applying the bounds on $\widehat{Q}(G,2)$ in the proof of [31, Lemma 4.15] we immediately reduce to the case $q = 2$. Here $G = F_4(2).2$ and $H = 7^2{:}(3 \times 2.S_4)$ is the normaliser of a Sylow 7-subgroup of G. The upper bound on $\widehat{Q}(G,2)$ in the proof of [31, Lemma 4.15] is larger than 1/2, but we can use MAGMA to construct G and H as permutation groups of degree 139776 (more precisely, we use `AutomorphismGroupSimpleGroup` to construct G and we find H by taking the normaliser of a Sylow 7-subgroup). Then by considering the fusion of H-classes in G we calculate that

$$\widehat{Q}(G,2) = \frac{541861}{29328998400}$$

and the result follows.

Now suppose $T = G_2(q)$, so $p = 3$, $q \geqslant 9$ and G contains graph automorphisms (see [93, Table 5.2]). By arguing as in the proof of [31, Lemma 4.21] we reduce to the cases $q \in \{9,27\}$. Suppose $q = 27$ and note that $|H_0| \leqslant 12(q+1)^2 = a_1$. Let $x \in H$ be an element of prime order. If $x \in H_0$ then $|x^G| \geqslant q^3(q^3-1)(q+1) = b_1$ (as noted in the proof of [31, Lemma 4.21]), whereas if x is a field automorphism then $|x^G| > q^{28/3} = b_2$ and H contains at most $a_2 = 24(q+1)^2$ such elements. Similarly, if x is an involutory graph automorphism then $|x^G| = q^3(q^3-1)(q+1) = b_3$ and there are at most $a_3 = 12(q+1)^2$ such elements in H. It is straightforward to check that (4.5.1) holds. Finally, suppose $q = 9$. First we use MAGMA to construct $G = G_2(9).4 = \mathrm{Aut}(T)$ as a permutation group of degree 132860 and we note that $H = N_G(K)$, where K is either a Sylow ℓ-subgroup of T (with $\ell \in \{5,13,73\}$) or $K = C_8 \times C_8$. In each case, it is straightforward to construct H and verify the bound $\widehat{Q}(G,2) < 1/4$.

To complete the proof of the lemma, we may assume T is one of the twisted groups ${}^3D_4(q)$, ${}^2F_4(q)'$, ${}^2G_2(q)$ ($q \geqslant 27$) or ${}^2B_2(q)$. First assume $T = {}^3D_4(q)$, in which case there are three possibilities for H and one checks that the bound on $\widehat{Q}(G,2)$ in the proof of [31, Lemma 4.24] is sufficient if $q \geqslant 9$. Suppose $q = 8$ and let $x \in H$ be an element of prime order, which implies that $x \in H_0.3$. Then $|x^G| > 8^{14} = b_1$ and $3|H_0| \leqslant 383688 = a_1$, whence $\widehat{Q}(G,2) < a_1^2/b_1 < 1/4$. The same conclusion holds when $q = 7$ since $|H| \leqslant 233928$ and $|x^G| > 7^{14}$ for all $x \in H$ of prime order. The remaining groups with $q \leqslant 5$ can be handled using MAGMA. In each case, we can use `AutomorphismGroupSimpleGroup` to construct G and we obtain H as the normaliser in G of an appropriate Sylow ℓ-subgroup of T. For example, if $q = 5$ then the three possibilities for H correspond to the primes $\ell \in \{7,31,601\}$. In every case, it is straightforward to verify the bound $\widetilde{Q}(G,2) < 1/4$ (see (4.2.1)).

Next assume $T = {}^2F_4(q)'$. The case $q = 2$ can be checked using MAGMA and we note that $Q(G,2) > 1/4$ when $H \cap T = 5^2{:}4A_4$ (as recorded in Table 4.3). For $q \geqslant 8$, the upper bound on $\widehat{Q}(G,2)$ in the proof of [31, Lemma 4.26] is sufficient (note that in the upper bound on $|H|$ given in the proof of this lemma, the $2\log q$ factor can be replaced by $|\mathrm{Out}(T)| = \log q$). The case $T = {}^2G_2(q)$ is very similar. Indeed, if $q \geqslant 3^5$ then the upper bound on $\widehat{Q}(G,2)$ in the proof of [28, Lemma 4.37] is good enough, while the case $q = 27$ can be handled using MAGMA, noting that $H = N_G(K)$ with K a Sylow ℓ-subgroup of T for $\ell \in \{7,19,37\}$. Finally, let us assume $T = {}^2B_2(q)$. If $q \geqslant 2^9$ then the bounds in the proof of [28, Lemma 4.39] are good enough. If $q = 2^7$ and $x \in H$ is a field automorphism of order 7 then $|x^G| > q^4$ and by arguing as in the proof of [28, Lemma 4.39] we deduce that $\widehat{Q}(G,2) < 1/4$. The remaining cases with $q \in \{8,32\}$ can be checked using MAGMA and we find that $Q(G,2) < 1/4$ unless $q = 8$ and $H \cap T = 13{:}4$. The latter case is recorded in Table 4.3. ∎

Proposition 4.5.7. *The conclusion to Theorem 4.5.1 holds if T is an exceptional group of Lie type.*

Proof. In view of the previous lemma, we may assume G is one of the groups listed in Table 4.5. In cases (a), (b) and (c) we can use MAGMA to prove the result (we get $Q(G,2) < 1/4$ in cases (b) and (c), while $Q(G,2) \geqslant 1/4$ in (a)). In (d), the upper bound on $\widehat{Q}(G,2)$ in the proof of [31, Lemma 4.16] is insufficient. But as explained in [32, Example 1.4], we can use MAGMA to construct G and H and then it is straightforward to verify the bound $\widehat{Q}(G,2) < 1/4$.

Finally, let us consider cases (e) and (f). In (e) we observe that 2 and 3 are the only prime divisors of $|H|$ and we deduce that $\widehat{Q}(G,2) < 1/4$ by applying the relevant bounds presented in Case 1 in the proof of [31, Lemma 4.12]. Similarly, in case (f) we note that the only prime divisors of $|H|$ are 2 and 3. If x is a long root element, then

$$|x^G \cap H| = 4|y^L| = 36 = a_1,\ |x^G| > 2^{58} = b_1,$$

where y is a long root element in $L = \mathrm{SU}_3(2)$. If not, then $|x^G| > 2^{92} = b_2$ and we note that $|H| = 104485552128 = a_2$. By applying Lemma 2.4.1 we deduce that

$$\widehat{Q}(G,2) < a_1^2/b_1 + a_2^2/b_2 < \frac{1}{4}$$

and the result follows. ■

In order to complete the proof of Theorem 4.5.1, we may assume T is a classical group. It will be convenient to partition the proof into various subsections according to the socle T. The cases that we need to consider are recorded in the following result, which is an immediate consequence of [87] and [14, Theorem 2].

Theorem 4.5.8. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group in $\mathcal{G}$ with socle T classical and point stabiliser H. Suppose $T \not\cong \mathrm{L}_2(q)$. Then (G,H) is one of the cases in Table 4.6.*

4.5.3 Linear groups

In this section we assume $T = \mathrm{L}_n(q)$ for $n \geqslant 3$.

Proposition 4.5.9. *The conclusion to Theorem 4.5.1 holds if $T = \mathrm{L}_n(q)$.*

Proof. First assume n is a prime and H is of type $\mathrm{GL}_1(q^n)$. By applying the upper bound on $\widehat{Q}(G,2)$ in the proof of [14, Lemma 6.4] we immediately reduce to the cases where $(n,q) = (7,2)$, or $n = 5$ and $q \leqslant 5$, or $n = 3$ and $q \leqslant 19$. With the aid of MAGMA, it is straightforward to compute $Q(G,2)$ precisely in each of these cases and the result quickly follows (note that the condition $b(G) = 2$ implies that $G \neq \mathrm{L}_3(3).2$). In particular, we find that $Q(G,2) \geqslant 1/4$ only if $n = 3$ and $q \leqslant 5$ (the precise exceptions are recorded in Table 4.4).

T	Type of H	Conditions
$\mathrm{L}_n(q)$	$\mathrm{GL}_1(q^n)$	$n \geqslant 3$ prime, $G \neq \mathrm{L}_3(3).2$
	$\mathrm{GL}_2(q) \wr S_{n/2}$	$n \in \{6,8\}$, $q = 3$
	$\mathrm{GL}_1(q) \wr S_n$	$n \in \{3,4\}$, $q \geqslant 5$
	$\mathrm{O}_4^+(q)$	$(n,q) = (4,3)$, $G \neq \mathrm{Aut}(T)$
	$\mathrm{O}_3(q)$	$(n,q) = (3,3)$
	$3^{1+2}.\mathrm{Sp}_2(3)$	$n = 3$, $p = q \equiv 1 \pmod 3$
$\mathrm{U}_n(q)$	$\mathrm{GU}_1(q^n)$	$n \geqslant 3$ prime
	$\mathrm{GU}_1(q) \wr S_n$	$n \in \{3,4\}$, $q \geqslant 3$, $(n,q) \neq (3,3)$
	$\mathrm{GU}_2(q) \wr S_{n/2}$	$n \in \{4,6,8\}$, $q = 3$
	$\mathrm{GU}_3(q) \wr S_{n/3}$	$n \in \{9,12\}$, $q = 2$
	$3^{1+2}.\mathrm{Sp}_2(3)$	$n = 3$, $q = p \equiv 2 \pmod 3$
	$\mathrm{GU}_3(2)$	$n = 3$, $q = 2^f$, $f \geqslant 3$ prime
$\mathrm{PSp}_n(q)$	$\mathrm{Sp}_2(q) \wr S_{n/2}$	$n \in \{6,8\}$, $q = 3$
	$\mathrm{O}_2^{\epsilon}(q) \wr S_2$	$(n,p) = (4,2)$, $q \geqslant 4$
	$\mathrm{O}_2^-(q^2)$	$(n,p) = (4,2)$, $q \geqslant 4$
$\mathrm{P\Omega}_n^+(q)$	$\mathrm{O}_4^+(q) \wr S_{n/4}$	$n \in \{12,16\}$, $q = 3$
	$\mathrm{O}_4^+(q) \wr S_2$	$(n,q) = (8,3)$, $\lvert G:T \rvert < 6$
	$\mathrm{O}_2^{\epsilon}(q) \wr S_4$	$n = 8$, $q \geqslant 3$
	$\mathrm{O}_2^-(q) \times \mathrm{GU}_3(q)$	$(n,q) = (8,2)$, $G = T.3$
	$\mathrm{O}_2^-(q^2) \times \mathrm{O}_2^-(q^2)$	$n = 8$
$\Omega_n(q)$	$\mathrm{O}_4^+(q) \perp \mathrm{O}_3(q)$	$(n,q) = (7,3)$

Table 4.6: The groups in $\mathscr{G}$ with $T \not\cong \mathrm{L}_2(q)$ classical

Next assume $n \in \{3,4\}$, $q \geqslant 5$ and H is of type $\mathrm{GL}_1(q) \wr S_n$. First assume $n = 3$. By inspecting the proof of [14, Lemma 6.5] we deduce that $\widehat{Q}(G,2) < 1/4$ if $q \geqslant 43$. If $29 \leqslant q \leqslant 41$ then G does not contain field automorphisms of order 2 or 3, nor graph-field automorphisms of order 2, so we may set $a_8 = a_9 = 0$ in the bound on $\widehat{Q}(G,2)$ presented in the proof of [14, Lemma 6.5]. One checks that this modified bound yields $\widehat{Q}(G,2) < 1/4$. For $7 \leqslant q \leqslant 27$ we can use MAGMA to show that $Q(G,2) < 1/4$ in the usual manner, with the single exception of the case $G = \mathrm{Aut}(T)$ with $q = 9$, where $Q(G,2) = 4093/12285$. Finally, for $q = 5$ we calculate that $Q(G,2) = 199/775$ if $G = T$, otherwise $Q(G,2) = 1379/3875$; both cases are recorded in Table 4.4. Similarly, if $n = 4$ then the result follows by combining explicit MAGMA computations for $q \in \{5,7,8\}$ with the upper bound on $\widehat{Q}(G,2)$ presented in the proof of [14, Lemma 6.6] for $q \geqslant 9$ (in every case we get $Q(G,2) < 1/4$). The case where $n = 3$ and H is of type $3^{1+2}.\mathrm{Sp}_2(3)$ is entirely similar, working with the bound on $\widehat{Q}(G,2)$ in the proof of [14, Lemma 6.11].

There are four remaining cases to consider. If $T = \mathrm{L}_3(3)$ with H of type $\mathrm{O}_3(3)$ then we compute $Q(G,2) = 19/39$ if $G = T$, whereas $Q(G,2) = 23/39$ for $G = T.2$. Next suppose $T = \mathrm{L}_4(3)$ and H is of type $\mathrm{O}_4^+(3)$. Here the condition $b(G) = 2$ implies that $G \neq \mathrm{Aut}(T)$ and using MAGMA one checks that $Q(G,2) > 1/4$ in each case (the precise value of $Q(G,2)$ is recorded in Table 4.4). The case $T = \mathrm{L}_6(3)$ with H of type $\mathrm{GL}_2(3) \wr S_3$ can be handled using MAGMA, working with the function MaximalSubgroups to construct H. Finally, suppose $T = \mathrm{L}_8(3)$ and H is of type $\mathrm{GL}_2(3) \wr S_4$. Here the MaximalSubgroups function is ineffective, but we can construct H by observing that $H = N_G(K)$ with $|K| = 2^{11}$, as noted in the proof of [14, Proposition 6.3] (also see [14, Example 2.4]). It is straightforward to check that $\widehat{Q}(G,2) < 1/4$. ■

4.5.4 Unitary groups

Proposition 4.5.10. *The conclusion to Theorem 4.5.1 holds if $T = \mathrm{U}_n(q)$ with $n \geqslant 3$.*

Proof. First assume n is a prime and H is of type $\mathrm{GU}_1(q^n)$. For $n \geqslant 5$, one checks that the upper bound on $\widehat{Q}(G,2)$ in the proof of [14, Lemma 6.4] is sufficient unless $n = 5$ and $q \leqslant 5$. Suppose $n = 5$, so $q \geqslant 3$ by the maximality of H. If $q = 5$ then it is easy to improve the given bound in [14] in order to show that $\widehat{Q}(G,2) < 1/4$ (for example, we can use the fact that $|H| \leqslant 10(5^5+1)/6$). For $q = 4$ we observe that $H = N_G(P)$, where P is a Sylow 41-subgroup of G, so it is straightforward to construct H in MAGMA and verify the bound $\widehat{Q}(G,2) < 1/4$ (note that it suffices to check this for $G = \mathrm{Aut}(T)$). The case $q = 3$ can also be checked using MAGMA (using MaximalSubgroups to construct H, or noting that H is the normaliser of a Sylow 61-subgroup). Similarly, if $n = 3$ then $q \geqslant 4$ and the bound in the proof of [14, Lemma 6.4] is sufficient for $q \geqslant 23$ (for $q = 32$, we note that $|x^G| \geqslant |T : \mathrm{U}_3(2)|$ if x is a field automorphism of order 5); the remaining cases with $q \leqslant 19$ can be verified using MAGMA.

Next suppose $T = \mathrm{U}_3(q)$ and H is of type $\mathrm{GU}_1(q) \wr S_3$ with $q \geqslant 4$. For $q \geqslant 43$ it is easy to check that the upper bound on $\widehat{Q}(G,2)$ in the proof of [14, Lemma 6.5] is sufficient. The same estimates are also good enough when $29 \leqslant q \leqslant 41$, noting that in each case G does not contain any field or graph-field automorphisms of order 2 or 3. For $11 \leqslant q \leqslant 27$ we can use MAGMA to verify the bound $\widehat{Q}(G,2) < 1/4$. We find that there are examples with $Q(G,2) \geqslant 1/4$ when $q \leqslant 9$; they are easily identified using MAGMA and they are recorded in Table 4.4. The case where $T = \mathrm{U}_4(q)$ and H is of type $\mathrm{GU}_1(q) \wr S_4$ is similar. Here $q \geqslant 3$ and the bound on $\widehat{Q}(G,2)$ in the proof of [14, Lemma 6.5] is good enough for $q \geqslant 9$. If $q \in \{7,8\}$ then one can check that $Q(G,2) < 1/4$ using MAGMA. In the same way, we find that there are exceptions to this bound when $q \in \{3,4,5\}$ and each of these cases is listed in Table 4.4.

Next let us turn to the groups where $n \in \{4,6,8\}$, $q = 3$ and H is of type $\mathrm{GU}_2(q) \wr S_{n/2}$. If $n = 4$ then $G = T$ is the only group with $b(G) = 2$ (see [14, Table 7]) and with the aid of MAGMA we calculate that $Q(G,2) = 187/315$. Next assume $n = 6$. Here $H = N_G(K)$ for some subgroup K of T of order 2^{10} and it is straightforward to check that $\widehat{Q}(G,2) < 1/4$ (see [14, Example 2.4] and the proof of [14, Proposition 6.3]). Similarly, if $n = 8$ then $H = N_G(K)$ with $|K| = 2^{13}$ and once again one checks that $\widehat{Q}(G,2) < 1/4$. (Note that in both cases, it suffices to check the bound for $G = \mathrm{Aut}(T)$.)

Now assume $n \in \{9,12\}$, $q = 2$ and H is of type $\mathrm{GU}_3(q) \wr S_{n/3}$. As noted in the proof of [14, Proposition 6.3], if $n = 9$ then $H = N_G(K)$ with $|K| = 3^8$ and we can use MAGMA to verify the bound $\widehat{Q}(G,2) < 1/4$.

For $n = 12$ we find that the bound presented in the proof of [14, Proposition 6.3] does not give $\widehat{Q}(G,2) < 1/4$ and a more accurate estimate is required. To do this, it suffices to improve the upper bound on the contribution to $\widehat{Q}(G,2)$ from elements of order 3.

As in the proof of [14, Proposition 6.3], we may view H as the stabiliser in G of an orthogonal decomposition

$$V = V_1 \perp V_2 \perp V_3 \perp V_4$$

of the natural module, where each V_i is a nondegenerate 3-space. Suppose $x \in H$ has order 3. If some conjugate of x induces a nontrivial permutation of the V_i, then $|x^G| > 2^{89} = b_1$ and we note that $|H| < 2^{42} = a_1$. Following the argument in [14], the contribution from the remaining elements of order 3 in H with $|x^G| > 2^{69} = b_2$ is less than a_2^2/b_2, where $a_2 = 2^{31}$. As explained in the proof of [14, Proposition 6.3], the contribution from the elements with $|x^G| \leqslant 3.2^{62}$ is less than $2\sum_{i=3}^{7} a_i^2/b_i$, where the integers a_i and b_i are defined as in the proof in [14]. Finally, if $3.2^{62} < |x^G| \leqslant 2^{69}$ then one can check that x is of the form $[I_8, \omega I_4]$, where $\omega \in \mathbb{F}_4$ is a primitive cube root of unity. Here we calculate

$$|x^G \cap H| \leqslant 2\binom{4}{2}m + \binom{4}{2}m^2 + 2\binom{4}{2}m^3 + m^4 = 42480 = a_0$$

where $m = \frac{1}{3}|\mathrm{GU}_3(2):\mathrm{GU}_2(2)| = 12$. Therefore, the contribution to $\widehat{Q}(G,2)$ from elements of order 3 is less than

$$a_1^2/b_1 + a_2^2/b_2 + 2\left(a_0^2/b_0 + \sum_{i=3}^{7} a_i^2/b_i\right) < \frac{1}{20}$$

where $b_0 = 3.2^{62}$. Finally, the estimates in the proof of [14, Proposition 6.3] imply that the contribution to $\widehat{Q}(G,2)$ from involutions is also less than 1/20 and the result follows.

To complete the proof of the proposition, we may assume $n = 3$ and either $q = p \equiv 2 \pmod 3$ and H is of type $3^{1+2}.\mathrm{Sp}_2(3)$, or $q = 2^f$ with $f \geqslant 3$ a prime and H is a subfield subgroup of type $\mathrm{GU}_3(2)$. Suppose H is of type $3^{1+2}.\mathrm{Sp}_2(3)$. Here the proof of [14, Lemma 6.11] gives the result for $q > 29$ and we can use MAGMA to handle the cases with $q \leqslant 29$, noting that there are exceptions to the bound $Q(G,2) < 1/4$ when $q = 5$ (as recorded in Table 4.4). Finally, let us assume H is of type $\mathrm{GU}_3(2)$, so $q = 2^f$ with $f \geqslant 3$ odd. If $f \geqslant 7$ then the bound on $\widehat{Q}(G,2)$ in the proof of [14, Lemma 6.10] is sufficient, while the cases with $f \in \{3,5\}$ can be handled using MAGMA. ■

4.5.5 Symplectic groups

Next assume $T = \mathrm{PSp}_n(q)$ with $n \geqslant 4$. We exclude the groups with $(n,q) = (4,2)$ since $\mathrm{PSp}_4(2)' \cong \mathrm{L}_2(9)$.

Proposition 4.5.11. *The conclusion to Theorem 4.5.1 holds if* $T = \mathrm{PSp}_n(q)$ *with* $n \geqslant 4$.

Proof. First assume $n \in \{6,8\}$, $q = 3$ and H is of type $\mathrm{Sp}_2(q) \wr S_{n/2}$. If $n = 6$ then the condition $b(G) = 2$ implies that $G = T$ and using MAGMA we calculate that $Q(G,2) = 853/1365$, so this case is listed in Table 4.4. For $n = 8$ we use `AutomorphismGroupSimpleGroup` and `MaximalSubgroups` to construct G and H, and we apply `DoubleCosetCanonical` to establish the existence of sufficiently many regular H-orbits in order to force $Q(G,2) < 1/4$ (see (3.1.1)). The details of the MAGMA code here is given in Appendix A.1.2.4. Indeed, for $G = T$ we get $r \geqslant 3113$, while $r \geqslant 1557$ for $G = T.2$.

Finally let us assume $T = \mathrm{Sp}_4(q)$ with $q \geqslant 4$ even and H of type $\mathrm{O}_2^{\epsilon}(q) \wr S_2$ or $\mathrm{O}_2^{-}(q^2)$. Here H is maximal only if G contains graph automorphisms and with the aid of MAGMA one checks that if $q \leqslant 2^5$ then either $\widehat{Q}(G,2) < 1/4$ or $q = 4$, $G = \mathrm{Aut}(T)$ and H is of type $\mathrm{O}_2^{-}(q) \wr S_2$. In the latter case we have $Q(G,2) = 103/153$ as recorded in Table 4.4. For the remainder, we may assume $q \geqslant 2^6$.

Suppose H is of type $\mathrm{O}_2^{\epsilon}(q) \wr S_2$, so $H_0 = (C_{q-\epsilon})^2{:}D_8$. By applying the upper bound in the proof of [14, Lemma 6.9], we deduce that $\widehat{Q}(G,2) < 1/4$ if $q \neq 2^7$. So let us assume $q = 2^7$ and write $\widehat{Q}(G,2) = \alpha_1 + \alpha_2$, where α_1 is the contribution from involutory graph automorphisms. The proof of [14, Lemma 6.9] gives $\alpha_2 < 2^{-6}$, so it remains for us to estimate α_1. If $\varepsilon = -$ then $H \leqslant (C_{129})^2{:}(SD_{16} \times C_7)$ and it follows that every involution in H is contained in $H \cap T = (C_{129})^2{:}D_8$, whence $\alpha_1 = 0$ and the result follows. Now assume $\varepsilon = +$, so $H \leqslant (C_{127})^2{:}(D_{16} \times C_7)$. Since there are exactly 4 involutions in $D_{16} \setminus D_8$, we deduce that $\alpha_1 \leqslant d^2/b$ with $d = 4.127^2$ and $b = |T : {}^2B_2(q)| = 34626060288$. One checks that the resulting bound on $\widehat{Q}(G,2)$ is good enough.

To complete the proof, let us assume $q \geqslant 2^6$ and H is of type $\mathrm{O}_2^{-}(q^2)$, so

$$H_0 = \mathrm{O}_2^{-}(q^2).2 = C_{q^2+1}{:}C_4$$

and we will estimate the contribution to $\widehat{Q}(G,2)$ from the various elements of prime order (the details in this case were omitted in the proof of [14, Lemma 6.9]). First let $x \in H$ be a unipotent involution. Then x embeds in G as an involution of type c_2 (in the notation of Aschbacher and Seitz [4]), whence

$$|x^G \cap H| = i_2(H_0) = q^2 + 1 = a_1, \ |x^G| = (q^2 - 1)(q^4 - 1) = b_1.$$

If x is semisimple, then $|x^G| \geqslant |\mathrm{Sp}_4(q) : \mathrm{GU}_1(q^2)| = q^4(q^2-1)^2 = b_2$ and we note that there are at most $a_2 = q^2 + 1$ such elements in H. Next suppose x is a field automorphism of odd order. Then $|x^G| > q^{20/3} = b_3$ and H contains fewer than $4(q^2+1)\log q = a_3$ such elements. Finally, suppose x is an involutory field or graph automorphism (note that G cannot contain elements of both types). If $\log q$ is even then every involution in H is contained in H_0, so we may assume $\log q$ is odd and x is a graph automorphism. Then $|x^G| = q^2(q+1)(q^2-1) = b_4$ and we note that $|x^G \cap H| \leqslant |H_0| = 4(q^2+1) = a_4$. Therefore, by applying Lemma 2.4.1 we deduce that

$$\widehat{Q}(G,2) < \sum_{i=1}^{3} a_i^2/b_i + \alpha a_4^2/b_4,$$

where $\alpha = 1$ if $\log q$ is odd, otherwise $\alpha = 0$, and we conclude that $\widehat{Q}(G,2) < 1/4$. ■

4.5.6 Orthogonal groups

In order to complete the proof of Theorem 4.5.1, we may assume $T = \mathrm{P}\Omega_n^{\epsilon}(q)$ with $n \geqslant 7$.

Proposition 4.5.12. *The conclusion to Theorem 4.5.1 holds if $T = \mathrm{P}\Omega_n^{\varepsilon}(q)$ with $n \geqslant 7$.*

Proof. By inspecting Table 4.6 we observe that either n is even and $\varepsilon = +$, or $(n,q) = (7,3)$. First assume $n \in \{12,16\}$, $q = 3$ and H is of type $\mathrm{O}_4^+(q) \wr S_{n/4}$. For $n = 16$, the upper bound in the proof of [14, Proposition 6.3] gives $\widehat{Q}(G,2) < 1/4$. On the other hand, if $n = 12$ then we can construct G and H in MAGMA (see [14, Example 2.4]) and it is straightforward to check that $\widehat{Q}(G,2) < 1/4$. The relevant cases with $T = \Omega_7(3)$ or $\Omega_8^+(2)$ can also be handled using MAGMA and the exceptions with $Q(G,2) \geqslant 1/4$ are recorded in Table 4.4.

To complete the proof, we may assume $T = \mathrm{P}\Omega_8^+(q)$ with $q \geqslant 3$. Suppose $q = 3$ and H is of type $\mathrm{O}_4^+(3) \wr S_2$, noting that $|G:T| < 6$ since $b(G) = 2$. Even though $|G:H| = 14926275$ is large, we can still analyse this case in the usual way using MAGMA, working with a set of (H,H) double coset representatives to compute r (and hence $Q(G,2)$). The results are presented in Table 4.4.

Next assume H is of type $\mathrm{O}_2^{\varepsilon'}(q) \wr S_4$. If $q \in \{3,4\}$ then $\varepsilon' = -$ and using MAGMA one can check that either $Q(G,2) < 1/4$, or $q = 3$, $G = \mathrm{Aut}(T)$, $r = 823$ and

$$Q(G,2) = \frac{17810761}{44778825}.$$

For example, if $q = 3$ and $G = T.A_4$ then using `DoubleCosetCanonical` we can verify the bound $r \geqslant 3075$, which forces $Q(G,2) < 1/4$ (see Appendix A.1.2.4). We thank Eamonn O'Brien for his assistance with the precise calculation of r when $G = \mathrm{Aut}(T)$. For $q \geqslant 5$, we seek to apply the upper bound on $\widehat{Q}(G,2)$ presented in the proof of [14, Lemma 6.7]. If $q \geqslant 9$ then

$$\widehat{Q}(G,2) < 2q^{-1} + q^{-2} + q^{-3} + q^{-7} < \frac{1}{4}$$

and the result follows. One can check that the bounds in the proof of [14, Lemma 6.7] are also sufficient when $q \in \{7,8\}$, so we may assume $q = 5$. Here we have $H = N_G(K)$, where $K < T$ has order 2^9 if $\varepsilon' = +$, otherwise $|K| = 3^4$. We now construct H as in [14, Example 2.4] and one checks that $\widehat{Q}(G,2) < 1/4$.

Finally, let us assume H is of type $\mathrm{O}_2^-(q^2) \times \mathrm{O}_2^-(q^2)$ with $q \geqslant 3$. If $q \geqslant 11$ then the upper bound on $\widehat{Q}(G,2)$ in the proof of [14, Lemma 6.8] is sufficient. On the other hand, if $q \leqslant 9$ then we can construct H in MAGMA, noting that $H = N_G(K)$ with K a Sylow ℓ-subgroup of T and ℓ an odd prime divisor of q^2+1. In this way, it is straightforward to check that $\widetilde{Q}(G,2) < 1/4$ (see (4.2.1)) and the result follows. ■

We conclude that the proof of Theorem 4.5.1 is complete via Propositions 4.5.4, 4.5.5, 4.5.7, 4.5.9, 4.5.10, 4.5.11 and 4.5.12.

4.5.7 Proof for base-two groups

4.5.7.1 Common Neighbour Conjecture

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group in $\mathscr{G}$ with socle T and point stabiliser H. Recall that our goal is to show that the Saxl graph $\Sigma(G)$ has the following property:

$(\star)$ *Any two vertices in $\Sigma(G)$ have a common neighbour*

which immediately implies that $\Sigma(G)$ has diameter 2. In view of Theorem 4.2(i) and Lemma 3.1.3(i), we may assume $T \not\cong \mathrm{L}_2(q)$ and $Q(G,2) \geqslant 1/2$, so the relevant groups can be determined by inspecting Tables 4.3 and 4.4 (see Theorem 4.5.1). In every one of these cases, we can verify property $(\star)$ using MAGMA.

To do this, we first construct G and H using the approach in Section 4.2.1. Next we implement the method discussed in Section 4.2.4 by identifying a set R of (H,H) double coset representatives and then for each $x \in R$ we seek an element $y \in G$ (by random search) such that $H \cap H^y = H^x \cap H^y = 1$. Notice that $(\star)$ holds if and only if such an element y exists for each $x \in R$. As demonstrated by the following example, it is easy to implement this approach in MAGMA.

Example 4.5.13. Suppose $T = \Omega_8^+(2)$, $G = T.3$ and H is of type $\mathrm{O}_2^-(2) \times \mathrm{GU}_3(2)$. Here $Q(G,2) = 2071/2800 > 1/2$ and so this is one of the cases we need to consider. We proceed as follows, noting that G has a unique conjugacy class of maximal subgroups of order 11664:

```
G:=AutomorphismGroupSimpleGroup("O+",8,2);
S:=LowIndexSubgroups(G,2);
G:=S[1];
M:=MaximalSubgroups(G:OrderEqual:=11664);
H:=M[1]‘subgroup;
R,T:=DoubleCosetRepresentatives(G,H,H);
z:=0;
for x in R do
  if exists(y){y : y in G | #(H meet H^y) eq 1 and #(H^x meet H^y) eq 1}
    then z:=z+1;
  end if;
end for;
z eq #R;
```

This returns `true` and we conclude that $(\star)$ holds. An entirely similar approach is effective for all of the relevant groups in Tables 4.3 and 4.4.

4.5.7.2 Regular orbits

In this section, we classify the groups $G \in \mathscr{G}$ with $1 \leqslant \mathrm{reg}(G) \leqslant 4$, which will be useful later in our analysis of bases for product type groups in Chapter 6. This gives Theorem 4.5 for base-two groups as an immediate corollary.

Proposition 4.5.14. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive group in $\mathscr{G}$ with socle T and soluble point stabiliser H. Then $1 \leqslant r(G) \leqslant 4$ if and only if (G,H) is one of the cases in Tables 4.7 and 4.8.*

Proof. First assume $T \ncong \mathrm{L}_2(q)$ and $Q(G,2) \geqslant 1/4$. Then G is one of the groups recorded in Tables 4.3 and 4.4, and it is a routine exercise to read off the cases with $r(G) \leqslant 4$, all of which are listed in Tables 4.7 and 4.8.

Next suppose $G \in \mathscr{G}$, $T \ncong \mathrm{L}_2(q)$ and $Q(G,2) < 1/4$, in which case $4|H|^2 r(G) > 3|G|$. We will establish the following claim, which immediately implies that $r(G) \geqslant 5$.

Claim. If $G \in \mathscr{G}$, $T \ncong \mathrm{L}_2(q)$ and $Q(G,2) < 1/4$, then $16|H|^2 \leqslant 3|G|$.

To prove the claim, we consider each possibility for T in turn. First assume $T = A_m$ is an alternating group. With the aid of MAGMA, it is straightforward to verify the claim when $m \leqslant 12$. Now assume $m > 12$. Then by inspecting [87, Table 14] and [14, Table 4], we deduce that m is a prime and $H = \mathrm{AGL}_1(m) \cap G$, which implies that

$$\frac{|H|^2}{|G|} \leqslant \frac{m(m-1)}{(m-2)!} < \frac{3}{16}$$

as required. The sporadic groups are also straightforward. Here the possibilities for H can be read off from [45] and [120], noting that we may exclude the cases in Table 4.3 and [14, Table 4] since we are assuming $Q(G,2) < 1/4$.

Next assume T is an exceptional group of Lie type over $\mathbb{F}_q$. As noted in the proof of [14, Proposition 7.1], either $H = N_G(R)$ for some maximal torus R of T (see [93, Table 5.2]), or (G,H) is one of the cases in Table 4.5. In addition, we may exclude the relevant cases in Table 4.3. The claim now follows by inspection. For example, suppose $T = {}^2B_2(q)$ and $H = N_G(R)$ is the normaliser of a maximal torus, where $q = 2^f$ with $f \geqslant 3$ odd. Here

$$|H| \leqslant 4(q + \sqrt{2q} + 1)\log q, \ |G| \geqslant |T| = q^2(q^2+1)(q-1)$$

and the claim follows if $f \geqslant 5$. On the other hand, if $f = 3$ then the condition $Q(G,2) < 1/4$ implies that $H \cap T = 7{:}2$ or $5{:}4$, whence $|H| \leqslant 60$, $|G| \geqslant 29120$ and once again the desired bound holds.

To complete the proof of the claim, we may assume T is a classical group over $\mathbb{F}_q$ and $T \ncong \mathrm{L}_2(q)$. Here we note that the possibilities for G and H are recorded in Table 4.6. In each case, the precise structure of H is given in [80, Chapter 4] and the claim follows by inspection. For example, suppose $T = \mathrm{L}_3^{\epsilon}(q)$ and H is of type $\mathrm{GL}_1^{\epsilon}(q) \wr S_3$. If $q \geqslant 19$, then the bounds $|G| > \frac{1}{6}q^8$ and $|H| \leqslant 12(q+1)^2 \log q$ are sufficient. For the remaining groups with $q \leqslant 17$, excluding the cases with $Q(G,2) \geqslant 1/4$ recorded in Table 4.3, we can verify the bound by working with the exact orders of G and H. All of the other cases are very similar and we omit the details. This justifies the claim and we have now completed the proof of the proposition for the groups in $\mathscr{G}$ with $T \not\cong \mathrm{L}_2(q)$.

Finally, let us assume $G \in \mathscr{G}$ and $T \cong \mathrm{L}_2(q)$. Write $q = p^f$, where p is a prime. If $q \leqslant 81$ then it is a routine exercise to determine all the groups with $r(G) \leqslant 4$ using MAGMA and one can check that all the relevant cases have been recorded in Tables 4.7 and 4.8. For the remainder, we may assume $q > 81$.

First assume H is of type $\mathrm{GL}_1(q) \wr S_2$. Here [14, Lemma 4.7] implies that $b(G) = 2$ if and only if $\mathrm{PGL}_2(q)$ is not a proper subgroup of G. If $G = \mathrm{PGL}_2(q)$ then $r(G) = 1$ as noted above, and this case is recorded in Table 4.8. Now assume $G \cap \mathrm{PGL}_2(q) = T$ and q is odd. By Lemmas 4.3.11 and 4.3.12, we have $r(G) \leqslant 4$ only if $r(\mathrm{P\Sigma L}_2(q)) \leqslant 4$. By arguing as in the proof of Lemma 4.3.18, we see that $r(\mathrm{P\Sigma L}_2(q)) = m/2f$, where m is the number of non-squares in $\mathbb{F}_q$ that are not contained in any proper subfield of $\mathbb{F}_q$. Since every generator of the multiplicative group $\mathbb{F}_q^\times$ has this property, it follows that $m \geqslant \phi(q-1)$, where ϕ is Euler's totient function. In particular, $r(G) \leqslant 4$ only if $\phi(q-1) \leqslant 8f$. By applying the lower bound on $\phi(q-1)$ in Lemma 4.3.17, we find that $\phi(q-1) > 8f$ for every prime-power q with $q > 81$, whence $r(G) \geqslant 5$ and no additional cases arise.

Next, suppose H is of type $\mathrm{GL}_1(q^2)$, so $b(G) = 2$ if and only if G does not contain $\mathrm{PGL}_2(q)$ (see [14, Lemma 4.8]). Therefore, we may assume q is odd and by combining Lemmas 4.3.20 and 4.3.21, we observe that $r(G) \leqslant 4$ only if $r(\mathrm{P\Sigma L}_2(q)) \leqslant 4$. By arguing as in the proof of Lemma 4.3.26, we deduce that $r(G) \leqslant 4$ only if $\phi(q^2-1) \leqslant 8f(q+1)$. But one can check that the bound in Lemma 4.3.17 yields $\phi(q^2-1) > 8f(q+1)$ for every prime-power q with $q > 81$, and so once again we conclude that $r(G) \geqslant 5$.

Finally, one can deduce from the discussion in Section 4.3 that $Q(G,2) < 1/4$ if H is of any other type, and so $r(G) \geqslant 5$ by arguing as above. ■

Remark 4.5.15. Let us record some additional comments on Tables 4.7 and 4.8.

(i) As before, in the second column of Table 4.7 and the third column of Table 4.8, we record the type of H (see Remark 4.5.3(i)).

(ii) In the first row of Table 4.7 we have $G = \mathrm{PGL}_2(q)$ and $H = D_{2(q-1)}$ is a subgroup of type $\mathrm{GL}_1(q) \wr S_2$. Here we may assume $q \geqslant 7$ and $q \neq 9$ because H is non-maximal when $q = 5$, while the cases $q = 4$ and 9 are recorded as $(G,H) = (A_5, D_6)$ and $(A_6.2, D_{16})$ in Table 4.7. As noted in the proof of [14, Lemma 4.7], we have

$$r(T) = \begin{cases} 1 & q \text{ even} \\ (q+a)/4 & q \text{ odd} \end{cases}$$

where $a = 7$ if $q \equiv 1 \pmod 4$, otherwise $a = 5$.

G	Type of H	$r(T)$	Comments
$\mathrm{PGL}_2(q)$	$\mathrm{GL}_1(q) \wr S_2$	See Remark 4.5.15(ii)	$q \geqslant 7$, $q \neq 9$
$\mathrm{P}\Omega_8^+(3).2^2$	$\mathrm{O}_4^+(3) \wr S_2$	12	Both groups of this shape
$\Omega_8^+(2).3$	$\mathrm{O}_2^-(2) \times \mathrm{GU}_3(2)$	5	
$\mathrm{SO}_7(3)$	$\mathrm{O}_4^+(3) \perp \mathrm{O}_3(3)$	5	
$\mathrm{PSp}_6(3)$	$\mathrm{Sp}_2(3) \wr S_3$	1	
$\mathrm{PGL}_4(3)$	$\mathrm{O}_4^+(3)$	6	
$\mathrm{U}_4(3).[4]$	$\mathrm{GU}_1(3) \wr S_4$	11	$G \neq T.\langle \delta^2, \phi \rangle$
$\mathrm{U}_4(3)$	$\mathrm{GU}_2(3) \wr S_2$	1	
$\mathrm{L}_3(4).D_{12}$	$\mathrm{GL}_1(4^3)$	44	
$\mathrm{L}_3(4).2$	$\mathrm{GU}_3(2)$	3	$G \neq \mathrm{P}\Sigma\mathrm{L}_3(4)$
$\mathrm{U}_3(5).S_3$	$\mathrm{GU}_1(5) \wr S_3$	11	
$\mathrm{U}_3(4)$	$\mathrm{GU}_1(4) \wr S_3$	1	
$\mathrm{PGL}_2(11)$	$2_-^{1+2}.\mathrm{O}_2^-(2)$	3	
$G_2(3).2$	$\mathrm{SL}_2(3)^2$	4	
S_7	$\mathrm{AGL}_1(7)$	4	
$A_6.2$	D_{16}	4	$G = \mathrm{PGL}_2(9)$
$A_6.2$	$5{:}4$	2	$G = \mathrm{M}_{10}$
A_5	D_6	1	
$\mathrm{J}_2.2$	$5^2{:}(4 \times S_3)$	2	
M_{11}	$2.S_4$	1	

Table 4.7: The groups in $\mathcal{G}$ with $r(G) = 1$

4.5.8 Proof for other cases

Finally, we are in a position to prove Theorems 4.2(iii) and 4.5.

First consider the proof of Theorem 4.5, noting that the result for base-two groups can be deduced from Proposition 4.5.14. Here we will establish Proposition 4.5.19 below, which is the analogue of Proposition 4.5.14 for groups with $b(G) > 2$ and this will be useful in Chapter 6.

Throughout this section, set $r = \mathrm{reg}(G)$, $Q = Q(G, b(G))$ and $\widehat{Q} = \widehat{Q}(G, b(G))$. It is straightforward to show that $r \geqslant 5$ if

$$\widehat{Q} < 1 - \frac{4|H|^{b(G)}}{|G|^{b(G)-1}}. \tag{4.5.2}$$

Three special cases arise in the proof of Proposition 4.5.19 below and it is convenient to handle them separately from the main argument. Note that in the following lemma, H is the normaliser of a non-split maximal torus of T.

Lemma 4.5.16. *Suppose $T = \mathrm{L}_2(q)$ and H is of type $\mathrm{GL}_1(q^2)$, where $q \geqslant 11$. Then $b(G) \leqslant 3$, with equality if and only if $\mathrm{PGL}_2(q) \leqslant G$. Moreover, if $b(G) = 3$ then $\mathrm{reg}(G) \geqslant 5$.*

Proof. The base size of G is recorded in Theorem 4.1 and so for the remainder we may assume $\mathrm{PGL}_2(q) \leqslant G$. Write $q = p^f$ with p a prime and note that $H \cap \mathrm{PGL}_2(q) = D_{2(q+1)}$. It suffices to

$r(G)$	G	Type of H	$r(T)$	Comments
2	$\mathrm{P}\Omega_8^+(3).4$	$\mathrm{O}_4^+(3) \wr S_2$	12	
	$\mathrm{L}_4(3).2_2$	$\mathrm{O}_4^+(3)$	6	
	$\mathrm{Sp}_4(4).4$	$\mathrm{O}_2^-(4) \wr S_2$	9	
	$\mathrm{L}_3(3)$	$\mathrm{GL}_1(3^3)$	2	
	$\mathrm{L}_3(3).2$	$\mathrm{O}_3(3)$	5	
	$\mathrm{U}_3(5).S_3$	$3^{1+2}.\mathrm{Sp}_2(3)$	21	
	$\mathrm{L}_2(27).3$	$\mathrm{GL}_1(27) \wr S_2$	8	
		$\mathrm{GL}_1(27^2)$	6	
	$\mathrm{PGL}_2(13)$	$2_-^{1+2}.\mathrm{O}_2^-(2)$	6	
	$\mathrm{L}_2(11)$	$\mathrm{GL}_1(11^2)$	2	
	${}^2B_2(8).3$	$13{:}12$	7	
	A_9	$\mathrm{ASL}_2(3)$	2	
	$A_6.2$	SD_{16}	4	$G = \mathrm{M}_{10}$
	J_2	$5^2{:}D_{12}$	2	
3	$\mathrm{P}\Omega_8^+(3).3$	$\mathrm{O}_4^+(3) \wr S_2$	12	
	$\mathrm{P}\Omega_8^+(3).2$	$\mathrm{O}_4^+(3) \wr S_2$	12	$G = T.\langle\gamma\rangle$
	$\mathrm{L}_4(3).2_3$	$\mathrm{O}_4^+(3)$	6	
	$\mathrm{L}_3(4).S_3$	$\mathrm{GL}_1(4^3)$	44	$G \neq \mathrm{P\Gamma L}_3(4)$
	$\mathrm{PGU}_3(5)$	$\mathrm{GU}_1(5) \wr S_3$	11	
	$\mathrm{L}_2(25).2$	$\mathrm{GL}_1(25) \wr S_2$	8	$G = \mathrm{P\Sigma L}_2(25)$
		$\mathrm{GL}_1(25^2)$	6	$G \neq \mathrm{PGL}_2(25)$
	$\mathrm{L}_2(17)$	$2_-^{1+2}.\mathrm{O}_2^-(2)$	3	
	$\mathrm{L}_2(13)$	$\mathrm{GL}_1(13^2)$	3	
	${}^2F_4(2)$	$5^2{:}4S_4$	6	
	$\mathrm{J}_3.2$	$3^{2+1+2}{:}8.2$	10	
	$\mathrm{HS}.2$	$5^{1+2}.[2^5]$	9	
4	$\mathrm{PSO}_8^+(3)$	$\mathrm{O}_4^+(3) \wr S_2$	12	
	$\mathrm{U}_4(3).2$	$\mathrm{GU}_1(3) \wr S_4$	11	$G \neq T.\langle\delta^2\phi\rangle$
	$\mathrm{L}_2(25).2$	$\mathrm{GL}_1(25) \wr S_2$	8	$G = T.\langle\delta\phi\rangle$
	$\mathrm{L}_2(q)$	$\mathrm{GL}_1(q^2)$	4	$q = 17, 19$
	$G_2(3)$	$\mathrm{SL}_2(3)^2$	4	
	$\mathrm{M}_{12}.2$	$S_4 \times S_3$	13	
	$\mathrm{Suz}.2$	$3^{2+4}{:}2.(S_4 \times D_8)$	16	

Table 4.8: The groups in $\mathcal{G}$ with $2 \leqslant r(G) \leqslant 4$

verify the inequality in (4.5.2) (with $b(G) = 3$), so we need to consider the contributions to $\widehat{Q}$ from the elements $x \in G$ of prime order; the argument below closely follows the proof of [14, Lemma 4.6]. Note that $\mathrm{fpr}(x) = 0$ if $x^G \cap H$ is empty, so we are only interested in the relevant G-classes that meet H. Let $x \in H$ be an element of prime order r.

First assume $r = 2$, so x is either semisimple or unipotent (according to the parity of p) since $\mathrm{fpr}(x) = 0$ if x is an involutory field automorphism. Then

$$|x^G \cap H| \leqslant i_2(D_{2(q+1)}) \leqslant q+2 = a,\ |x^G| \geqslant \frac{1}{2}q(q-1) = b,$$

so the contribution to $\widehat{Q}$ from involutions is at most $\alpha_1 = b(a/b)^3$.

Now suppose r is odd, so either r divides $q+1$ and x is semisimple, or $q = q_0^r$ is an r-th power and x is a field automorphism. If x is semisimple, then $|x^T \cap H| = 2$, $|x^T| = q(q-1)$ and we note that G has $(r-1)/2$ distinct T-classes of such elements. Therefore, the combined contribution to $\widehat{Q}$ from semisimple elements of odd order is at most

$$\sum_{r\in\pi} \frac{1}{2}(r-1)\cdot\frac{8}{q^2(q-1)^2} < \frac{4\log(q+1)}{q(q-1)^2} = \alpha_2,$$

where π is the set of odd prime divisors of $q+1$ (here we are using the fact that $|\pi|$ is at most $\log(q+1)$, recalling that all logarithms in this thesis are in base 2).

Finally, suppose $q = q_0^r$ and x is a field automorphism of order r. Here

$$|x^G \cap H| = \frac{q+1}{q_0+1},\ |x^G| = \frac{q(q^2-1)}{q_0(q_0^2-1)}$$

and we note that there are $r-1$ distinct T-classes of field automorphisms of order r in $\mathrm{Aut}(T)$. If $q_0 = 2$ then $q = 2^r$ and the contribution from field automorphisms is

$$(r-1)\cdot\frac{4(2^r+1)}{3.2^{2r}(2^r-1)^2} < 2^{-r} = q^{-1}.$$

And for $q_0 \geqslant 3$ we get

$$\sum_{r\in\pi'}(r-1)\cdot\frac{q_0^2(q_0-1)^2}{q^2(q-1)^2}\cdot\frac{q+1}{q_0+1} < \sum_{r\in\pi'}(r-1)\cdot 3q^{-3(1-\frac{1}{r})} < q^{-1}\log\log q = \alpha_3,$$

where π' is the set of odd prime divisors of $f = \log_p q$.

By combining the above estimates, we conclude that $\widehat{Q} \leqslant \alpha_1+\alpha_2+\alpha_3$ and it is straightforward to check that the bound in (4.5.2) holds for all $q \geqslant 11$. ■

Lemma 4.5.17. *Suppose $T = {}^2B_2(q)$ and $H \cap T = [q^2]{:}C_{q-1}$ is a Borel subgroup. Then $b(G) = 3$ and either $G = {}^2B_2(8){:}3$ and $\mathrm{reg}(G) = 2$, or $\mathrm{reg}(G) \geqslant 5$.*

Proof. Here $q = 2^f$, $f \geqslant 3$ is odd and $|\Omega| = q^2+1$. In addition, $b(G) = 3$ by [14, Theorem 1.2]. The cases with $q \leqslant 2^7$ can be checked directly using MAGMA (see Section 4.2.4) and so we may assume

$f \geqslant 9$. As before, it suffices to show that the inequality in (4.5.2) is satisfied (with $b(G) = 3$). Set $H_0 = H \cap T$ and let χ be the permutation character $1_{H_0}^T$, which can be expressed as the sum of the trivial and Steinberg characters of T. The character table of T is given in [117].

First let $x \in T$ be an element of prime order r. If $r = 2$ then $\chi(x) = 1$, so $\mathrm{fpr}(x) = 1/(q^2+1)$ and we have $|x^G| = (q^2+1)(q-1)$. Similarly, if r divides $q-1$ then $\chi(x) = 2$, $|x^G| = q^2(q^2+1)$ and we note that there are at most $(q-2)/2$ distinct T-classes of such elements. Therefore, the contribution to $\widehat{Q}$ from unipotent and semisimple elements is at most

$$\alpha_1 = \frac{q-1}{(q^2+1)^2} + \frac{1}{2}(q-2)\cdot\frac{8q^2}{(q^2+1)^2}.$$

Finally, suppose $x \in G$ is a field automorphism of prime order r and note that r is odd since f is odd. Then

$$|x^T| = \frac{q^2(q^2+1)(q-1)}{q^{2/r}(q^{2/r}+1)(q^{1/r}-1)} = f(q,r)$$

and $C_{H_0}(x)$ is a Borel subgroup of $C_T(x) = {}^2B_2(q^{1/r})$, so

$$|x^T \cap H_0x| = \frac{q^2(q-1)}{q^{2/r}(q^{1/r}-1)} = g(q,r).$$

There are $r-1$ distinct T-classes of field automorphisms of order r in $\mathrm{Aut}(T)$, so the combined contribution to $\widehat{Q}$ from field automorphisms is

$$\beta = \sum_{r \in \pi}(r-1)\cdot g(q,r)^3 f(q,r)^{-2}, \tag{4.5.3}$$

where π is the set of prime divisors of $f = \log q$. Set

$$e(q,r) = (r-1)\cdot g(q,r)^3 f(q,r)^{-2}. \tag{4.5.4}$$

If $q = 2^9$ or 2^{11} then it is straightforward to check that $\beta < 1/25$. Now assume $q \geqslant 2^{13}$. If $f = r$ then $\beta = e(q,r)$ and one checks that this is less than $q^{-1/2}$. Now assume f is composite, so $q^{1/r} \geqslant 8$ for each $r \in \pi$. Here $f(q,r) > q^{5(1-1/r)}$ and $g(q,r) < 2q^{3(1-1/r)}$, which implies that $e(q,r) < 8(r-1)q_0^{1-r} < 4q^{-1/2}$. Since $|\pi| < \log\log q$, we deduce that

$$\beta < 4q^{-1/2}\log\log q.$$

By combining the above estimates, we conclude that $\widehat{Q} \leqslant \alpha_1 + \alpha_2$ for $q \geqslant 2^9$, where $\alpha_2 = 1/25$ if $q \in \{2^9, 2^{11}\}$, otherwise $\alpha_2 = 4q^{-1/2}\log\log q$. It is now routine to verify that the bound in (4.5.2) is satisfied for all $q \geqslant 2^9$. ■

Note that in the statement of the next lemma we assume $q \geqslant 27$. Indeed, if $q = 3$ then $T = {}^2G_2(q)' \cong \mathrm{L}_2(8)$ and $H \cap T$ corresponds to a Borel subgroup of $\mathrm{L}_2(8)$ (if $G = T$, then $b(G) = 3$ and $\mathrm{reg}(G) = 1$, otherwise $b(G) = 4$ and $\mathrm{reg}(G) = 2$).

Lemma 4.5.18. *Suppose $T = {}^2G_2(q)$ and $H \cap T = [q^3]{:}C_{q-1}$ is a Borel subgroup, where $q \geqslant 27$. Then $b(G) = 3$ and $\mathrm{reg}(G) \geqslant 5$.*

Proof. Here $q = 3^f$, $f \geqslant 3$ is odd, $|\Omega| = q^3+1$ and $b(G) = 3$ by [14, Theorem 1.2]. The case $q = 27$ can be checked directly using MAGMA and so we may assume $f \geqslant 5$. We now proceed as in the proof of the previous two lemmas, working with fixed point ratio estimates to derive a suitable upper bound on $\widehat{Q}$ which allows us to verify the inequality in (4.5.2) (with $b(G) = 3$). As before, set $H_0 = H \cap T$ and let $\chi = 1_{H_0}^T$ be the permutation character. Once again, χ is the sum of the trivial and Steinberg characters of T (the character table of T is presented in [119]).

First let $x \in T$ be an element of prime order r. If $r = 3$ then $\chi(x) = 1$ and thus $\mathrm{fpr}(x) = 1/(q^3+1)$. In addition, we calculate that there are precisely $(q^3+1)(q^2-1)$ elements in T of order 3 (forming three distinct conjugacy classes). Next assume r divides $q-1$. If $r = 2$ then $|x^G| = q^2(q^2-q+1)$ (there is a unique class of involutions in T) and we have $\chi(x) = q+1$, so $\mathrm{fpr}(x) = 1/(q^2-q+1)$. Now suppose r is an odd prime divisor of $q-1$. Here $\chi(x) = 2$, so $\mathrm{fpr}(x) = 2/(q^3+1)$ and $|x^T| = q^3(q^3+1)$. Since there are at most $(q-3)/2$ distinct T-classes of such elements, we conclude that the contribution to $\widehat{Q}$ from unipotent and semisimple elements is at most

$$\alpha_1 = \frac{q^2-1}{(q^3+1)^2} + \frac{q^2}{(q^2-q+1)^2} + \frac{1}{2}(q-3)\cdot\frac{8q^3}{(q^3+1)^2}.$$

Now assume $x \in G$ is a field automorphism of prime order r, so r is odd and we have

$$|x^T| = \frac{q^3(q^3+1)(q-1)}{q^{3/r}(q^{3/r}+1)(q^{1/r}-1)} = f(q,r)$$

and

$$|x^T \cap H_0x| = \frac{q^3(q-1)}{q^{3/r}(q^{1/r}-1)} = g(q,r).$$

Therefore, the combined contribution to $\widehat{Q}$ from field automorphisms is β, as defined in (4.5.3). Define $e(q,r)$ as in (4.5.4).

If $f = r$ then $\beta = e(q,r) < q^{-1}$ for all $q \geqslant 3^5$. Now assume f is composite, so $q^{1/r} \geqslant 27$ for each $r \in \pi$. Then one checks that $f(q,r) > q^{7(1-1/r)}$ and $g(q,r) < 2q^{4(1-1/r)}$, which implies that $e(q,r) < 8(r-1)q_0^{-2(r-1)} < 4q^{-1}$. Since $|\pi| < \log\log q$, we conclude that $\beta < \alpha_2 = 4q^{-1}\log\log q$ for all $q \geqslant 3^5$.

Therefore, $\widehat{Q} \leqslant \alpha_1 + \alpha_2$ and it is now straightforward to verify the bound in (4.5.2). ■

We are now in a position to prove the following result. Combining with Proposition 4.5.14, this completes the proof of Theorem 4.5.

Proposition 4.5.19. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive group with socle T and soluble point stabiliser H. If $b(G) \geqslant 3$ then $\mathrm{reg}(G) \leqslant 4$ if and only if (G,H) is one of the cases in Table 4.9.*

Proof. Recall that $b(G) \leqslant 5$ by the main theorem of [14]. The proof of [14, Theorem 8.2] gives $r \geqslant 5$ if $b(G) = 5$, so we may assume $b(G) \in \{3,4\}$ and we note that the possibilities for G and H are recorded in [14, Tables 4–7]. Recall that $r \geqslant 5$ if (4.5.2) holds.

For most of the cases appearing in [14, Tables 4–7], an explicit upper bound on $\widehat{Q}$ is given in [14] and we can usually use this to verify the inequality in (4.5.2). However, this approach is not always effective because the given upper bound on $\widehat{Q}$ is either too large, or is not defined. As explained below, in these remaining cases we will typically use MAGMA to directly compute r, implementing the approach described in Section 4.2.4. We divide the remainder of the proof into three cases.

Case 1. $b(G) = 4$.

First assume $b(G) = 4$. By inspecting the relevant tables in [14], we see that $T = \mathrm{L}_2(q)$ with H of type P_1 (a Borel subgroup of G) is the only infinite family that arises. Let us first consider this special case. For $q > 32$, an explicit upper bound on $\widehat{Q}$ is presented as a function of q in the proof of [14, Lemma 4.4] and it is a routine exercise to check that the bound in (4.5.2) is satisfied. The remaining groups with $q \leqslant 32$ can be handled using MAGMA, which allows us to compute r precisely. In particular, the groups with $r \leqslant 4$ are recorded in Table 4.9. We can apply the same computational approach to handle all the remaining groups with $b(G) = 4$ appearing in [14, Tables 4–7], considering each group in turn.

Case 2. $b(G) = 3$*, H non-parabolic.*

To complete the proof, we may assume $b(G) = 3$. We begin by assuming G is not a group of Lie type in a parabolic action, so either

(a) $T = \mathrm{L}_2(q)$ and H is of type $\mathrm{GL}_1(q) \wr S_2$ or $\mathrm{GL}_1(q^2)$; or

(b) (G,H) is one of a finite number of sporadic cases in [14, Tables 4 and 7].

First let us consider the cases in (a), noting that the precise base size of G is recorded in [14, Lemmas 4.7 and 4.8]. The groups with $q \leqslant 37$ can be handled using MAGMA and we find that $r \leqslant 4$ if and only if (G,H,r) is one of the following:

$$(\mathrm{L}_2(4), D_{10}, 2), (\mathrm{L}_2(4).2, 5{:}4, 1), (\mathrm{L}_2(4).2, D_{12}, 4), (\mathrm{PGL}_2(5), D_{12}, 4),$$

all of which are recorded in Table 4.9 with $G = A_5$ or S_5. If H is of type $\mathrm{GL}_1(q) \wr S_2$ and $q > 37$, then the proof of [14, Lemma 4.6] yields the upper bound $\widehat{Q} < 2q^{-1/2}$ and we deduce that (4.5.2) holds. For H of type $\mathrm{GL}_1(q^2)$, we refer the reader to Lemma 4.5.16.

Next let us turn to the groups in (b) above. Here we apply computational methods, after first dividing the groups into two subcollections according to the size of Ω. By inspection, one can check that $|\Omega| \geqslant 5 \times 10^6$ if and only if $T = \mathrm{P}\Omega_8^+(3)$ and H is of type $\mathrm{O}_4^+(3) \wr S_2$, or $T \in \{\mathrm{Fi}_{22}, \mathrm{Fi}_{23}\}$ and H is the 3-local subgroup of G recorded in [14, Table 4]. Here we can use MAGMA to compute

$\widehat{Q}$ precisely, which then allows us to verify the bound in (4.5.2). In each of the remaining cases, we can apply the usual approach to compute r, as explained in Section 4.2.4.

Case 3. $b(G) = 3$, H parabolic.

For the remainder of the proof, we may assume G is a group of Lie type over $\mathbb{F}_q$, H is a maximal parabolic subgroup and $b(G) = 3$. Write $q = p^f$, where p is a prime, and let ϕ be a field automorphism of T of order f.

First assume G is an exceptional group. Here the possibilities for (G,H) are recorded in [14, Table 5] and by inspection we see that one of the following holds:

(a′) $T = G_2(q)$ and $H \cap T = [q^6]{:}C_{q-1}^2$, where $p = 3$ and $G \not\leqslant \langle T, \phi\rangle$.

(b′) $T = {}^2B_2(q)$ and $H \cap T = [q^2]{:}C_{q-1}$.

(c′) $T = {}^2G_2(q)$ and $H \cap T = [q^3]{:}C_{q-1}$, where $q \geqslant 27$.

(d′) (G,H) is one of a finite number of sporadic cases in [14, Table 5] with $q \leqslant 3$.

Consider case (a′). If $q \geqslant 27$, then the explicit upper bound on $\widehat{Q}$ presented in the proof of [14, Lemma 5.9] is sufficient, while the groups with $q \in \{3,9\}$ can be handled directly using MAGMA (note that if $q = 9$ then we can construct H by observing that $H = N_G(K)$ for some subgroup $K < T$ of order 9^6). For (b′) and (c′) we refer the reader to Lemmas 4.5.17 and 4.5.18. The cases in (d′) can all be handled computationally using MAGMA. First assume $G = F_4(2).2$ and $H = [2^{22}].S_3^2.2$, in which case $|\Omega| = 21928725$. Here we construct G as a permutation group of degree 139776 and we use the fact that $H = N_G(K)$ with $|K| = 2^{22}$ to construct H (here the function `MaximalSubgroups` is not effective). We then compute $\widehat{Q}$ and we check that (4.5.2) holds (given the size of Ω, this appears to be the most efficient way to handle this case). We use a similar method in the case where $T = {}^3D_4(3)$ and $T \cap H = [3^{11}]{:}(26 \circ \mathrm{SL}_2(3)).2$. All of the remaining cases in (d′) can be handled in the usual fashion and we can compute r precisely. In this way, we deduce that $r \leqslant 4$ if and only if $G = G_2(3)$ and $H = [3^5]{:}\mathrm{GL}_2(3)$, in which case $r = 4$.

Finally, let us assume G is a classical group and H is a parabolic subgroup. By inspecting [14, Table 6], we see that one of the following holds:

(a″) $T = \mathrm{L}_2(q)$ and H is of type P_1.

(b″) $T = \mathrm{L}_3(q)$ and H is of type $P_{1,2}$.

(c″) $T = \mathrm{U}_3(q)$ and H is of type P_1.

(d″) $T = \mathrm{PSp}_4(q)$ and $H \cap T = [q^4]{:}C_{q-1}^2$, where $q \geqslant 4$ is even and $G \not\leqslant \langle T, \phi\rangle$.

(e″) (G,H) is one of a finite number of sporadic cases in [14, Table 6] with $q \leqslant 3$.

First consider case (a$''$). Here [14, Lemma 4.5] implies that $b(G) = 3$ if and only if $G \leqslant \mathrm{PGL}_2(q)$, or $q = p^f$ is odd, f is even and $G = \langle T, \delta\phi^{f/2}\rangle = T.2$, where $\mathrm{PGL}_2(q) = \langle T, \delta\rangle$. In other words, either G is sharply 3-transitive on Ω and thus $r = 1$, or q is odd, $G = T$ and $r = 2$.

In cases (b$''$), (c$''$) and (d$''$), an explicit upper bound on $\widehat{Q}$ is presented in the proofs of [14, Lemmas 5.6–5.8]. Using this bound, one can check that (4.5.2) holds for $q > 128, 32, 32$, respectively. Consider case (c$''$) for example. For $q > 10^4$, the bound

$$\widehat{Q} < 8q^{-1/2}\log\log q + 4q^{-1} + q^{-3}$$

from the proof of [14, Lemma 5.7] is sufficient. Similarly, for $9 \leqslant q \leqslant 10^4$, we can use a more accurate upper bound on $\widehat{Q}$ in [14] to reduce our analysis to the groups with

$$q \in \{3,4,5,7,8,9,16,27,32\}$$

and at this point, we can use MAGMA to compute r precisely (here it is convenient to note that the standard permutation representation of G in MAGMA corresponds to the action of G on Ω). We find that there are several cases with $r \leqslant 4$, all of which have been listed in Table 4.9. Cases (b$''$) and (d$''$) can be handled in the same way. Similarly, we can use MAGMA to compute r for each group in case (e$''$). ■

Remark 4.5.20. Let us record some additional comments on Table 4.9.

(i) Once again, the we continue using “type of H” as in the previous tables (see Remark 4.5.3(i)).

(ii) Consider the first row in Table 4.9 with $b(G) = 3$. Here $G = \mathrm{L}_2(q).2$, $H = P_1$ is a Borel subgroup and $q = p^f$ is odd, and we may assume $q \neq 5, 9$ (as $\mathrm{L}_2(5) \cong A_5$ and $\mathrm{L}_2(9) \cong A_6$). Then $\mathrm{reg}(G) = 1$ if and only if G is sharply 3-transitive, which means that either $G = \mathrm{PGL}_2(q)$, or f is even and $G = T.\langle\delta\phi^{f/2}\rangle$.

(iii) Up to isomorphism, there are three almost simple groups of the form $\mathrm{L}_4(3).2$, one of which is $\mathrm{PGL}_4(3)$. In addition, we have $\mathrm{L}_4(3).2_2$ and $\mathrm{L}_4(3).2_3$, which contain involutory graph automorphisms x with $C_T(x) = \mathrm{PGSp}_4(3)$ and $\mathrm{PSO}_4^-(3).2$, respectively.

(iv) In the fourth column of Table 4.9 we record $\mathrm{reg}(G)$. In a few cases, this is presented as $r_1, r_2, \ldots$, which means that $\mathrm{reg}(G) = r_i$ when q is contained in the i-th set appearing in the fifth column. For example, if $G = \mathrm{P\Gamma L}_2(q)$ and $H = P_1$, then $\mathrm{reg}(G) = 3$ if $q = 16$ and $\mathrm{reg}(G) = 2$ if $q = 8$.

Finally we prove Theorem 4.2(iii).

$b(G)$	G	Type of H	reg(G)	Comments
4	$\mathrm{L}_3(3)$	P_1, P_2	1	
	$\mathrm{P\Gamma L}_2(q)$	P_1	3,2	$q \in \{16\}, \{8\}$
	$A_6.2^2$	$3^2{:}SD_{16}$	3	
	S_5	S_4	1	
3	$\mathrm{L}_2(q).2$	P_1	1	See Remark 4.5.15(ii)
	$\mathrm{L}_2(q)$	P_1	$2-\delta_{2,p}$	$q \geqslant 7$, $q \neq 9$
	$\mathrm{P\Omega}_8^+(3)$	P_2	3	
	$\Omega_7(3)$	P_2	3	
	$\mathrm{PSp}_6(3)$	P_2	3	
	$\mathrm{L}_4(3).2$	$P_{1,3}$	3	$G \neq \mathrm{PGL}_4(3)$
	$\mathrm{U}_4(3).2$	P_1	1	$G \not< \mathrm{PGU}_4(3)$
	$\mathrm{U}_4(3)$	P_1	3	
	$\mathrm{Aut}(\mathrm{L}_3(q))$	$P_{1,2}$	4,3,1	$q \in \{3,25,27,64\}, \{32\}, \{8,9,16\}$
	$\mathrm{L}_3(16).(2\times 4)$	$P_{1,2}$	4	
	$\mathrm{L}_3(16).D_{12}$	$P_{1,2}$	2	
	$\mathrm{L}_3(16).12$	$P_{1,2}$	3	
	$\mathrm{L}_3(4).2^2$	$P_{1,2}$	4	
	$\mathrm{L}_3(4).6$	$P_{1,2}$	4	
	$\mathrm{Aut}(\mathrm{U}_3(q))$	P_1	4,3,2,1	$q \in \{27\}, \{7,32\}, \{5,9,16\}, \{3,4,8\}$
	$\mathrm{U}_3(16).4$	P_1	4	
	$\mathrm{U}_3(9).2$	P_1	4	
	$\mathrm{U}_3(8).S_3$	P_1	4	
	$\mathrm{U}_3(8).6$	P_1	3	
	$\mathrm{U}_3(8).3^2$	P_1	2	
	$\mathrm{U}_3(4).2$	P_1	2	
	$\mathrm{U}_3(4)$	P_1	4	
	$\mathrm{U}_3(3)$	P_1	3	
	$\mathrm{L}_2(7)$	$2_-^{1+2}.\mathrm{O}_2^-(2)$	1	
	${}^2B_2(8).3$	$[8^2]{:}7.3$	2	
	$G_2(3)$	$[3^5]{:}\mathrm{GL}_2(3)$	4	
	S_7	$S_4 \times S_3$	1	
	$A_6.2$	$3^2{:}Q_8$	1	$G = \mathrm{PGL}_2(9)$
		$\mathrm{AGL}_1(9)$	1	$G = \mathrm{M}_{10}$
	A_6	$(S_3 \wr S_2) \cap G$	2	
	S_5	$S_3 \times S_2$	4	
		$5{:}4$	1	
	A_5	A_4	1	
		D_{10}	2	

Table 4.9: Almost simple primitive groups G with soluble point stabilisers, $b(G) \in \{3,4\}$ and reg$(G) \leqslant 4$

Proof of Theorem 4.2(iii). The precise base size $b(G)$ is computed in [14, Theorem 2]. In particular, we have $b(G) \leqslant 5$ in every case. If $b(G) = 2$ then the result follows from the argument in Section 4.5.7.1. Thus, to complete the proof, we may assume that $3 \leqslant b(G) \leqslant 5$. Hence by [14, Theorem 2], G appears among the infinite families and special cases listed in [14, Tables 4–7].

Note that if $\mathrm{soc}(G) \in \{\mathrm{L}_2(q), \mathrm{U}_3(q), {}^2B_2(q), {}^2G_2(q)\}$ and the point stabiliser is of type P_1, then G is 2-transitive and so $\Sigma(G)$ is complete by Lemma 3.3.8. Upper bounds for $\widehat{Q}(G, b(G))$ in the remaining infinite families with $T \not\cong \mathrm{L}_2(q)$ can be found in [14] and the proof of Lemma 4.5.16. In almost all cases, we deduce that $\widehat{Q}(G, b(G)) < 1/2$, and it follows from Lemma 3.2.6(i) that $(\star)$ holds. Any remaining group in these infinite families with $\widehat{Q}(G, b(G)) \geqslant 1/2$ is one of the following:

(a) $T = \mathrm{L}_3(q)$, H is of type $P_{1,2}$, and either $3 \leqslant q \leqslant 16$, $19 \leqslant q \leqslant 27$, or $q \in \{32, 47, 64\}$; or

(b) $T = \mathrm{Sp}_4(q)$, $H \cap T = [q^4]{:}C_{q-1}^2$, and $q \in \{4, 8, 32\}$.

Combining probabilistic and computational methods (similar to those mentioned in Section 4.2 and the proofs of Proposition 4.4.1 and Theorem 4.4.4), one can check that property $(\star)$ holds for each case in (a) and (b), together with all the special cases appearing in [14, Tables 4–7]. ■

Chapter 5

Diagonal type groups

The majority of the new results in this chapter are taken from the papers

> S.D. Freedman, H.Y. Huang, M. Lee and K. Rekvényi, *On the generalised Saxl graphs of permutation groups*, submitted (2024), arXiv:2410.22613.
>
> H.Y. Huang, *Base sizes of primitive groups of diagonal type*, Forum Math. Sigma **12** (2024), Paper No. e2, 43 pp.

which are [52] and [71], respectively. The work in Sections 5.8 and 5.9 is my own, original and unpublished work.

In this chapter, we will consider the diagonal type primitive groups. Our main goal is to establish Theorem A, which determines the exact base sizes of all these groups. A precise statement of this result is Theorem 5.1 below. We will also classify the groups G such that the generalised Saxl graph $\Sigma(G)$ is G-arc-transitive in this setting (see Theorem 5.3 below), establishing Theorem D. Additionally, we will make progress towards a classification of the semi-Frobenius primitive groups of diagonal type, which is Theorem 5.4. Finally, we will also establish Conjecture II for some base-two diagonal type groups in Theorem 5.6.

With the exception of Theorem 5.6 and the results in Sections 5.8 and 5.9, the majority of the new results in this chapter are taken from my single-authored paper [71], and the results concerning the generalised Saxl graphs come from my joint paper [52] with Freedman, Lee and Rekvényi.

5.1 Introduction

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a diagonal type primitive group (recorded as type III in Table 2.1), so G has socle T^k, where T is a non-abelian simple group and $k \geqslant 2$ is an integer. More precisely, we have $|\Omega| = |T|^{k-1}$ and

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

The primitivity of G implies that the subgroup $P \leqslant S_k$ induced by the conjugation action of G on the set of factors of T^k is either primitive, or $k = 2$ and $P = A_2 = 1$. The group P is called the *top group* of G and we note that

$$T^k \trianglelefteqslant G \leqslant T^k.(\mathrm{Out}(T) \times P). \tag{5.1.1}$$

We will describe the action of G in more detail in Section 5.2.1.

The first systematic study of bases for diagonal type groups was initiated by Fawcett in [51]. Here she shows that $b(G) = 2$ if $P \notin \{A_k, S_k\}$, and in the general case she determines the exact base size of G up to one of two possibilities (see Theorem 5.2.3). One of the key ingredients in [51] is a theorem of Seress [109], which asserts that if $k > 32$ and $P \notin \{A_k, S_k\}$, then there exists a subset of $\{1, \dots, k\}$ with trivial setwise stabiliser in P. However, this does not hold if $P \in \{A_k, S_k\}$, and hence a different approach is required. In this chapter, we extend Fawcett's work by determining the exact base size in all cases. This is the first family of primitive groups arising in the O'Nan-Scott theorem for which the exact base sizes are known.

Theorem 5.1. *Let G be a diagonal type primitive group with socle T^k and top group $P \leqslant S_k$.*

(i) If $P \notin \{A_k, S_k\}$, then $b(G) = 2$.

(ii) If $k = 2$, then $b(G) \in \{3, 4\}$, with $b(G) = 4$ if and only if $T \in \{A_5, A_6\}$ and $G = T^2.(\mathrm{Out}(T) \times S_2)$.

(iii) If $k \geqslant 3$, $P \in \{A_k, S_k\}$ and $|T|^{\ell-1} < k \leqslant |T|^{\ell}$ with $\ell \geqslant 1$, then $b(G) \in \{\ell+1, \ell+2\}$. Moreover, $b(G) = \ell + 2$ if and only if one of the following holds:

(a) $k = |T|$.

(b) $k \in \{|T| - 2, |T|^{\ell} - 1, |T|^{\ell}\}$ and $S_k \leqslant G$.

(c) $k = |T|^2 - 2$, $T \in \{A_5, A_6\}$ and $G = T^k.(\mathrm{Out}(T) \times S_k)$.

As a key step in the proof of Theorem 5.1, we will first classify the base-two diagonal type primitive groups in Section 5.5, stated as below.

Theorem 5.2. *Let G be a diagonal type primitive group with socle T^k and top group $P \leqslant S_k$. Then $b(G) = 2$ if and only if one of the following holds:*

(i) $P \notin \{A_k, S_k\}$.

(ii) $3 \leqslant k \leqslant |T| - 3$.

(iii) $k \in \{|T|-2, |T|-1\}$ *and* G *does not contain* S_k.

We are also able to classify the diagonal type groups G such that $\Sigma(G)$ is G-arc-transitive. Recall that reg(G) is the number of regular G-orbits on $\Omega^{b(G)}$, and $\Sigma(G)$ is G-arc-transitive if reg$(G) = 1$ (see Lemma 3.2.5).

Theorem 5.3. *Let* G *be a diagonal type primitive group. Then* $\Sigma(G)$ *is* G*-arc-transitive if and only if* $G = T^k.(\mathrm{Out}(T) \times S_k)$ *with* $T = A_5$ *and* $k \in \{3, 57\}$*. In particular,* reg$(G) = 1$ *if and only if* G *is one of these base-two groups.*

In addition, we also consider Problem IV for the primitive groups of diagonal type. Recall that G is called *semi-Frobenius* if $\Sigma(G)$ is a complete graph.

Theorem 5.4. *Let* G *be a diagonal type primitive group with socle* T^k *and top group* $P \leqslant S_k$.

(i) If $k = 2$*, then* G *is semi-Frobenius if one of the following holds:*

(a) $P = 1$;

(b) $T = A_n$ *for* $n \geqslant 7$*; or*

(c) T *is a sporadic group.*

(ii) If $k \geqslant 3$*, then the following statements hold:*

(a) If $P \notin \{A_k, S_k\}$ *then* G *is not semi-Frobenius.*

(b) If $|T|^{\ell-1} \leqslant k \leqslant |T|^{\ell}$ *and* $b(G) = \ell + 2$ *with* $\ell \geqslant 1$*, then* G *is semi-Frobenius.*

(c) If $P \in \{A_k, S_k\}$, $|T|^{\ell-1} + 3 \leqslant k \leqslant |T|^{\ell}$ *and* $b(G) = \ell + 1$ *with* $\ell \geqslant 1$*, then* G *is not semi-Frobenius.*

Remark 5.5. The only remaining cases for a complete classification of semi-Frobenius primitive groups of diagonal type are the case where $k \in \{|T|^{\ell-1}+1, |T|^{\ell-1}+2\}$ for $\ell \geqslant 2$, and the case where $P = S_2$. For the former, a partial result is given in Lemma 5.7.16, which shows that G is not semi-Frobenius if $S_k \leqslant G$. And for $P = S_2$, we show that G is not semi-Frobenius if $G = T^2.(\mathrm{Out}(T) \times S_2)$ with $T = \mathrm{L}_2(q)$ and $q \geqslant 11$ (see Proposition 5.6.12).

In Section 5.8 we will consider Conjecture II for the groups with $P \notin \{A_k, S_k\}$, noting from Theorem 5.1 that these groups are base-two.

Theorem 5.6. *Let* G *be a diagonal type primitive group with socle* T^k *and top group* $P \leqslant S_k$*. If* $P \notin \{A_k, S_k\}$ *then* $b(G) = 2$ *and any two vertices in* $\Sigma(G)$ *have a common neighbour.*

Let us briefly discuss the methods we will use to establish our main theorems. Focusing first on Theorem 5.2, recall that the *holomorph* of a non-abelian finite simple group T is the group

$$\mathrm{Hol}(T) = T{:}\mathrm{Aut}(T) = T^2.\mathrm{Out}(T),$$

which can be viewed as a primitive diagonal type group (with $k = 2$ and top group $P = 1$) in terms of its natural action on T (see Section 5.3 for details). We write $\mathrm{Hol}(T,S)$ for the setwise stabiliser of $S \subseteq T$ in $\mathrm{Hol}(T)$. A key observation is Lemma 5.3.1, which implies that

$$b(G) = 2 \text{ if there exists } S \subseteq T \text{ such that } |S| = k \text{ and } \mathrm{Hol}(T,S) = 1.$$

This essentially reduces the proof of Theorem 5.2 to the cases where $3 \leqslant k \leqslant |T|/2$. However, it is rather difficult to directly construct an appropriate subset S of T such that $\mathrm{Hol}(T,S) = 1$.

To overcome this difficulty, we adopt a probabilistic approach for $k \geqslant 5$ in the proof of Theorem 5.2 (see Section 5.4 for more details). More specifically, we estimate the probability that a random k-subset S of T satisfies $\mathrm{Hol}(T,S) = 1$, and we also use fixed point ratios to study the probability that a random pair in Ω is a base for G. The former is a new idea, which involves computing

$$\max\{|C_T(x)| : 1 \neq x \in \mathrm{Aut}(T)\}$$

in Theorem 5.2.10, while the latter is a widely used technique in the study of base sizes introduced by Liebeck and Shalev [96], as described in Section 2.4 (and in view of Lemma 3.1.3(i), this method will also allow us to establish Theorem 5.6).

The cases where $k = 3$ or 4 will be treated separately in Section 5.5.1. Here we use the fact that T is *invariably generated* by two elements (that is, there exist $x, y \in T$ such that $\langle x^g, y^h \rangle = T$ for any $g, h \in T$, which is proved in [65] and [77], independently), and a theorem of Gow [61] on the products of regular semisimple classes in groups of Lie type. We will use a very similar approach to establish Theorem 5.3 for base-two groups.

The proof of Theorem 5.1 will be completed in Section 5.7, and the main step involves constructing a base of size $\ell + 1$ when $|T|^{\ell-1} < k \leqslant |T|^{\ell} - 3$ for some $\ell \geqslant 2$. Once again, our construction requires the existence of a suitable subset S of T such that $\mathrm{Hol}(T,S) = 1$. We will treat the case where $k = 2$ separately, working with a theorem of Leemans and Liebeck [86] on the existence of a generating pair of T with a certain property (see Theorem 5.6.3). Our constructive approach also allows us to complete the proofs of Theorems 5.3 and 5.4.

As described above, a key ingredient in our study of bases for diagonal type groups is the following result, which may be of independent interest. The proof will be given in Section 5.5.

Theorem 5.7. *Let T be a non-abelian finite simple group and suppose $3 \leqslant m \leqslant |T| - 3$. Then there exists a subset $S \subseteq T$ such that $|S| = m$ and $\mathrm{Hol}(T,S) = 1$.*

Remark 5.8. The structure of the proofs of Theorems 5.1, 5.2, 5.3 and 5.4 for the groups with $P \in \{A_k, S_k\}$ are described in Table 5.1. Note that the conclusions to Theorems 5.1, 5.2 and 5.4 for

Theorem(s)	Conditions	Reference(s)
5.2	$k \in \{3, 4, \lvert T\rvert - 4, \lvert T\rvert - 3\}$	5.5.6
	$5 \leqslant k \leqslant \lvert T\rvert - 5$, T sporadic	5.5.10
	$5 \leqslant k \leqslant \lvert T\rvert - 5$, T alternating	5.5.11
	$5 \leqslant k \leqslant \lvert T\rvert - 5$, T exceptional	5.5.14
	$5 \leqslant k \leqslant \lvert T\rvert - 5$, T classical	5.5.17
	$k = \lvert T\rvert - 2$ or $\lvert T\rvert - 1$	5.5.8
	$k = 2$ or $k \geqslant \lvert T\rvert$	5.2.4
5.1, 5.3	$k = 2$	5.6.4
	$3 \leqslant k \leqslant \lvert T\rvert - 3$	5.2 and 5.5.1
	$k = \lvert T\rvert - 2$ or $\lvert T\rvert - 1$	5.5.8 and 5.5.9
	$k = \lvert T\rvert$	5.2.3(iii) and 5.7.4
	$\lvert T\rvert^{\ell-1} < k \leqslant \lvert T\rvert^{\ell} - 3$ with $\ell \geqslant 2$	5.7.9
	$k = \lvert T\rvert^2 - 2$	5.7.13
	$k = \lvert T\rvert^{\ell} - 2$ with $\ell \geqslant 3$	5.7.14
	$k = \lvert T\rvert^{\ell} - 1$ or $\lvert T\rvert^{\ell}$ with $\ell \geqslant 2$	5.7.11
5.4(i)	$k = 2$, $P = 1$	5.6.1
	$P = S_2$, $T = A_n$, $n \geqslant 7$	5.6.8
	$P = S_2$, T sporadic	5.6.11
5.4(ii)(b)	$k = \lvert T\rvert$	5.7.4
	$k = \lvert T\rvert - 2$ or $\lvert T\rvert - 1$	5.5.9
	$k = \lvert T\rvert^{\ell} - 1$ or $\lvert T\rvert^{\ell}$, with $\ell \geqslant 2$	5.7.11
	$k = \lvert T\rvert^2 - 2$, $T \in \{A_5, A_6\}$, $G = T^k.(\mathrm{Out}(T) \times S_k)$	5.7.12
5.4(ii)(c)	$\lvert T\rvert^{\ell-1} + 3 \leqslant k \leqslant \lvert T\rvert^{\ell}$, $\ell \geqslant 1$, $b(G) = \ell + 1$	5.7.15

Table 5.1: A road map for Theorems 5.1, 5.2, 5.3 and 5.4 when $P \in \{A_k, S_k\}$

the groups with $P \notin \{A_k, S_k\}$ follow from Theorem 5.2.3(i) (combining with Lemma 3.1.1(iii) for Theorem 5.4), and we refer to Proposition 5.2.7 and Remark 5.2.8 for the conclusion to Theorem 5.3 for these groups. In view of Lemma 5.3.1, Theorem 5.7 is an immediate corollary of Theorem 5.2. We will prove Theorem 5.6 in Section 5.8. Finally, in Section 5.9, we apply some results from Section 5.8 to establish Conjecture II and resolve Problem III for some primitive twisted wreath products.

5.2 Preliminaries

5.2.1 Diagonal type groups

Here we adopt Fawcett's notation from [51]. Let $k \geqslant 2$ be an integer and let T be a non-abelian finite simple group. Define

$$\begin{aligned}
&W(k,T) := \{(\alpha_1,\dots,\alpha_k)\pi \in \mathrm{Aut}(T) \wr_k S_k : \alpha_1\mathrm{Inn}(T) = \alpha_i\mathrm{Inn}(T) \text{ for all } i\},\\
&D(k,T) := \{(\alpha,\dots,\alpha)\pi \in \mathrm{Aut}(T) \wr_k S_k\},\\
&\Omega(k,T) := [W(k,T) : D(k,T)].
\end{aligned}$$

Then $|\Omega(k,T)| = |T|^{k-1}$ and $W(k,T) = T^k.(\mathrm{Out}(T) \times S_k)$ acts faithfully on $\Omega(k,T)$. We say that a group $G \leqslant \mathrm{Sym}(\Omega)$ with $\Omega = \Omega(k,T)$ is of *diagonal type* if

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

Let P_G denote the subgroup of S_k induced by the conjugation action of G on the set of factors of T^k. That is,

$$P_G = \{\pi \in S_k : (\alpha_1,\dots,\alpha_k)\pi \in G \text{ for some } \alpha_1,\dots,\alpha_k \in \mathrm{Aut}(T)\}.$$

Then $G \leqslant T^k.(\mathrm{Out}(T) \times P_G)$ as in (5.1.1), and G is primitive if and only if either P_G is primitive on $[k] = \{1,\dots,k\}$, or $k = 2$ and $P_G = 1$. From now on, if G is clear from the context, we denote $P = P_G$ and

$$\begin{aligned}
&W := T^k.(\mathrm{Out}(T) \times P),\\
&D := \{(\alpha,\dots,\alpha)\pi : \alpha \in \mathrm{Aut}(T), \pi \in P\},\\
&\Omega := \Omega(k,T) = [W : D].
\end{aligned}$$

We write $\varphi_t \in \mathrm{Inn}(T)$ for the inner automorphism such that $x^{\varphi_t} = t^{-1}xt$ for any $x \in T$. Thus,

$$\Omega = \{D(\varphi_{t_1},\dots,\varphi_{t_k}) : t_1,\dots,t_k \in T\}.$$

The action of G on Ω is given by

$$D(\varphi_{t_1},\dots,\varphi_{t_k})^{(\alpha_1,\dots,\alpha_k)\pi} = D(\varphi_{t_{1^{\pi^{-1}}}}\alpha_{1^{\pi^{-1}}},\dots,\varphi_{t_{k^{\pi^{-1}}}}\alpha_{k^{\pi^{-1}}}),$$

and the stabiliser of $D \in \Omega$ in W is D itself. In particular, for any element $(\alpha,\dots,\alpha)\pi \in D$, we have

$$D(\varphi_{t_1},\dots,\varphi_{t_k})^{(\alpha,\dots,\alpha)\pi} = D(\varphi_{t^{\alpha}_{1^{\pi^{-1}}}},\dots,\varphi_{t^{\alpha}_{k^{\pi^{-1}}}}),$$

noting that $\alpha^{-1}\varphi_t\alpha = \varphi_{t^\alpha}$ for all $t \in T$.

5.2.2 Bases

Now let us record some preliminary results on bases for diagonal type groups from [51]. We start with [51, Lemma 3.4].

Lemma 5.2.1. *Let $t_1,\dots,t_k$ be elements of T such that the following two properties are satisfied:*

(i) At least two of the t_i are trivial and at least one is non-trivial.

(ii) If t_i and t_j are non-trivial and $i \neq j$, then $t_i \neq t_j$.

Then $(\alpha,\dots,\alpha)\pi \in G$ fixes $D(\varphi_{t_1},\dots,\varphi_{t_k})$ only if $t_i^\alpha = t_{i^\pi}$ for all i.

For any $\mathbf{x} = (\varphi_{t_1},\dots,\varphi_{t_k}) \in \mathrm{Inn}(T)^k$, we define an associated partition $\mathscr{P}^{\mathbf{x}} = \{\mathscr{P}_t^{\mathbf{x}} : t \in T\}$ of $[k]$ such that $i \in \mathscr{P}_t^{\mathbf{x}}$ if $t_i = t$. Note that some parts $\mathscr{P}_t^{\mathbf{x}}$ in $\mathscr{P}^{\mathbf{x}}$ might be empty. The following result is an extension of Lemma 5.2.1. Recall that $P_{\{\mathscr{P}^{\mathbf{x}}\}}$ is the setwise stabiliser of the partition $\mathscr{P}^{\mathbf{x}}$ in P. In particular, if $t_{i^\pi} = t_{j^\pi}$ whenever $t_i = t_j$, then we have $\pi \in P_{\{\mathscr{P}^{\mathbf{x}}\}}$.

Lemma 5.2.2. *Let $\mathbf{x} = (\varphi_{t_1},\dots,\varphi_{t_k}) \in \mathrm{Inn}(T)^k$, $\omega = D\mathbf{x} \in \Omega$ and let $\mathscr{P}^{\mathbf{x}} = \{\mathscr{P}_t^{\mathbf{x}} : t \in T\}$ be the associated partition of $[k]$ as above. Suppose $(\alpha,\dots,\alpha)\pi \in G_\omega$. Then the following hold:*

(i) $\pi \in P_{\{\mathscr{P}^{\mathbf{x}}\}}$.

(ii) If $0 < |\mathscr{P}_1^{\mathbf{x}}| \neq |\mathscr{P}_t^{\mathbf{x}}|$ for all $t \neq 1$, then $t_i^\alpha = t_{i^\pi}$ for all i.

(iii) Under the same assumption as (ii), α lies in the setwise stabiliser of $\{g : |\mathscr{P}_g^{\mathbf{x}}| = |\mathscr{P}_t^{\mathbf{x}}|\}$ for any $t \in T$.

Proof. As $(\alpha,\dots,\alpha)\pi$ fixes $\omega = D(\varphi_{t_1},\dots,\varphi_{t_k})$, there exists a unique $g \in T$ such that $t_i^\alpha = g t_{i^\pi}$ for all $i \in [k]$. Suppose $t_i = t_j$ for some $i \neq j$ (so i and j are in the same part of $\mathscr{P}^{\mathbf{x}}$). Then $t_{i^\pi} = g^{-1} t_i^\alpha = g^{-1} t_j^\alpha = t_{j^\pi}$. This gives part (i).

For part (ii), it suffices to show that $g = 1$. If $t_i = 1$, then $t_{i^\pi} = g^{-1}$, and we get $t_{j^\pi} = g^{-1} t_j^\alpha \neq g^{-1}$ if $t_j \neq 1$. This implies that $|\mathscr{P}_{g^{-1}}^{\mathbf{x}}| = |\mathscr{P}_1^{\mathbf{x}}|$, so $g = 1$ by our assumption.

Finally, for part (iii), note that for any $t \in T$, we have $|\mathscr{P}_t^{\mathbf{x}}| = |\mathscr{P}_{t^\alpha}^{\mathbf{x}}|$ by applying (ii). ■

The following theorem combines Fawcett's main results on base sizes of diagonal type groups from [51].

Theorem 5.2.3. *Let G be a diagonal type primitive group with socle T^k and top group $P \leqslant S_k$.*

(i) If $P \notin \{A_k, S_k\}$, then $b(G) = 2$.

(ii) If $k = 2$, then $b(G) = 3$ if $P = 1$, and $b(G) \in \{3,4\}$ if $P = S_2$.

(iii) If $k \geqslant 3$, $P \in \{A_k, S_k\}$ and $|T|^{\ell-1} < k \leqslant |T|^\ell$ with $\ell \geqslant 1$, then $b(G) \in \{\ell+1, \ell+2\}$. Moreover, if either $k = |T|$, or $k \in \{|T|^\ell - 1, |T|^\ell\}$ and $S_k \leqslant G$, then $b(G) = \ell+2$.

Corollary 5.2.4. *If $P \in \{A_k, S_k\}$ and $b(G) = 2$, then $2 < k < |T|$.*

The following is [51, Lemma 3.11].

Lemma 5.2.5. *Suppose $P \in \{A_k, S_k\}$ and there exists an odd integer $3 \leqslant s \leqslant k$ that is relatively prime to the order of every element of* $\mathrm{Out}(T)$*. Then G contains A_k.*

Corollary 5.2.6. *If $P \in \{A_k, S_k\}$ and $k \geqslant |T|-3$, then G contains A_k.*

Proof. We have $|\mathrm{Out}(T)| < |T|^{1/3}$ by Lemma 2.2.5. In particular, $|\mathrm{Out}(T)| < |T|/3$, so there exists a prime s such that $|\mathrm{Out}(T)| < s < k$ (Bertrand's postulate). Now apply Lemma 5.2.5. ■

The following extends [51, Proposition 3.3], which asserts that $b(G) = 2$ if $k > 32$ and $P \notin \{A_k, S_k\}$. As before, $r(G)$ is the number of regular suborbits of G, noting that $r(G) \geqslant 1$ if and only if $b(G) \leqslant 2$, and $r(G) = \mathrm{reg}(G)$ if $b(G) = 2$.

Proposition 5.2.7. *If $k > 32$ and $P \notin \{A_k, S_k\}$, then $r(G) \geqslant 2$.*

Proof. We use the same construction as in the proof of [51, Proposition 3.3]. By [109, Theorem 1], there exists a partition $\mathscr{P} = \{\Pi_1, \Pi_2, \Pi_3\}$ of $[k]$ such that each Π_i is non-empty, $|\Pi_1|$, $|\Pi_2|$ and $|\Pi_3|$ are distinct, and

$$\bigcap_{m=1}^{3} P_{\{\Pi_m\}} = 1. \tag{5.2.1}$$

Let $x_1, x_2 \in T$ be non-trivial elements of distinct orders. By the main theorem of [63], there exist $y_1, y_2 \in T$ such that $\langle x_i, y_i \rangle = T$. Let $\Delta_i = \{D, D(\varphi_{t_{i,1}}, \dots, \varphi_{t_{i,k}})\}$ for $i \in \{1,2\}$, where $t_{i,j} = 1$ if $j \in \Pi_1$, $t_{i,j} = x_i$ if $j \in \Pi_2$, and $t_{i,j} = y_i$ if $j \in \Pi_3$. As explained in the proof of [51, Proposition 3.3], both Δ_1 and Δ_2 are bases for G.

Suppose $\Delta_1^{(\alpha,\dots,\alpha)\pi} = \Delta_2$. Then there exists $g \in T$ such that $t_{1,j}^{\alpha} = g t_{2,j^\pi}$ for all $j \in [k]$. If $t_{1,j} = t_{1,j'}$ for some $j' \in [k]$, then $t_{2,j} = t_{2,j'}$ and

$$t_{2,j^\pi} = g^{-1} t_{1,j}^{\alpha} = g^{-1} t_{1,j'}^{\alpha} = t_{2,(j')^\pi}.$$

Hence, $\pi \in P_{\{\mathscr{P}\}}$, and so $\pi \in P_{\{\Pi_m\}}$ for each $m \in \{1,2,3\}$ as $|\Pi_1|$, $|\Pi_2|$ and $|\Pi_3|$ are distinct. This implies that $\pi = 1$ by (5.2.1), and so $g = 1$. However, it follows that $x_1^{\alpha} = x_2$, which is incompatible with $|x_1| \neq |x_2|$. We conclude that Δ_1 and Δ_2 are in distinct G_D-orbits, and thus $r(G) \geqslant 2$. ■

Remark 5.2.8. In fact, as we will show in Section 5.5, we have $r(G) \geqslant 1$ whenever $3 \leqslant k \leqslant |T|-3$, with equality if and only if $T = A_5$, $k \in \{3, 57\}$ and $G = T^k.(\mathrm{Out}(T) \times S_k)$. In particular, it follows that $r(G) \geqslant 2$ if $k \leqslant 32$ and $P \notin \{A_k, S_k\}$.

5.2.3 Simple groups

We record some properties of finite simple groups that will be used to prove our main results.

Let T be a finite simple group of Lie type over a finite field $\mathbb{F}_q$ of characteristic p, and let K be the algebraic closure of $\mathbb{F}_q$. Recall that a semisimple element $x \in T$ is *regular* if $|C_T(x)|$ is indivisible by p. In particular, if T is a classical group with natural module V, then a semisimple element $x \in T$ is regular if a pre-image $\widehat{x} \in \mathrm{GL}(\overline{V})$ has distinct eigenvalues on $\overline{V} = V \otimes K$. And if T is an orthogonal group, then x is also regular if $\widehat{x}$ has a 2-dimensional (± 1)-eigenspace and all the other eigenvalues are distinct.

We say that a subset $\{t_1,\ldots,t_m\}$ of T is an *invariable* generating set if $\langle t_1^{g_1},\ldots,t_m^{g_m}\rangle = T$ for any $g_1,\ldots,g_m \in T$. It has been proved in [65] and [77], independently, that every non-abelian finite simple group is invariably generated by 2 elements.

Theorem 5.2.9. *Suppose $T \notin \{\mathrm{L}_2(5),\mathrm{L}_2(7),\Omega_8^+(2),\mathrm{P}\Omega_8^+(3)\}$ is a finite simple group of Lie type. Then there exist regular semisimple elements x and y of distinct orders such that T is invariably generated by $\{x,y\}$.*

Proof. If T is an exceptional group, then we take x and y to be t_1 and t_2 in [77, Table 2], respectively, noting that t_1 is a generator of the maximal torus T_1 in that table. It is evident that $|t_1| \neq |t_2|$ in each case, and $\{t_1,t_2\}$ invariably generates T by [77] (see [77, p. 312]). Moreover, we observe that $\langle t_1\rangle$ and $\langle t_2\rangle$ are both maximal tori, which implies that each t_i is regular semisimple.

To complete the proof, we may assume T is a classical group. Here we will work with the corresponding quasisimple group $Q \in \{\mathrm{SL}_n^{\varepsilon}(q),\mathrm{Sp}_n(q),\Omega_n^{\varepsilon}(q)\}$, noting that if Q is invariably generated by $\{t_1,t_2\}$, with t_1 and t_2 regular semisimple, then $T = Q/Z(Q)$ is invariably generated by $\{x,y\}$, where x and y are the images of t_1 and t_2 in T, respectively (so x and y are also regular semisimple). Moreover, $|x| = |t_1|/a$ and $|y| = |t_2|/b$ for some integers a,b dividing $|Z(Q)|$, so $|x| \neq |y|$ if

(5.2.2) $\qquad |t_2||Z(Q)|$ is indivisible by $|t_1|$ and $|t_1||Z(Q)|$ is indivisible by $|t_2|$.

First assume $Q \notin \{\mathrm{SL}_2(q),\Omega_8^+(q)\}$. Here we use the same t_1 and t_2 as presented in [77, Table 1]. In each case, it is clear that t_1 and t_2 are semisimple elements satisfying (5.2.2), and $\{t_1,t_2\}$ invariably generates Q by [77, Lemma 5.3]. Thus, it suffices to show that t_1 and t_2 are regular in every case, which is a straightforward exercise (for instance, we can work with the criterion for regularity in terms of the eigenvalues on $\overline{V}$ as discussed above).

For example, consider the element $t_2 \in Q = \Omega_{4m}^+(q)$. Here, t_2 is of the form

$$t_2 = \begin{pmatrix} A & \\ & B \end{pmatrix}^{\delta}$$

with respect to a decomposition $V = U \perp W$, where $\delta \in \{1,2\}$, U and W are subspaces of minus type of dimensions $4m-4$ and 4, respectively, $A \in \mathrm{SO}_{4m-4}^-(q)$ has order $q^{2m-2}+1$ and $B \in \mathrm{SO}_4^-(q)$ has order q^2+1. Here we note that the block-diagonal matrix $\mathrm{diag}(A,B)$ is in $\mathrm{SO}_{4m}^+(q)$, and δ is chosen so that $t_2 \in \Omega_{4m}^+(q)$. We only deal with the case where $\delta = 1$ since a similar argument holds for $\delta = 2$. Then the eigenvalues of A over the algebraic closure K of $\mathbb{F}_q$ are

$$\lambda,\lambda^q,\ldots,\lambda^{q^{4m-5}}$$

for some $\lambda \in K$ of order $q^{2m-2}+1$. Similarly, the set of eigenvalues of B over K is $\{\mu, \mu^q, \mu^{q^2}, \mu^{q^3}\}$ for some $\mu \in K$ of order q^2+1. If $\mu = \lambda^{q^i}$ for some $i \in \{0,\dots,4m-5\}$, then $\lambda^{q^i(q^2+1)} = 1$ and so $q^{2m-2}+1$ divides $q^i(q^2+1)$, which implies that $q^{2m-2}+1$ divides q^2+1 since $(q^{2m-2}+1, q^i) = 1$. However, since $m \geqslant 3$, this is impossible. It follows that the eigenvalues of t_2 over K are distinct, and so t_2 is a regular semisimple element.

Finally, let us handle the two excluded cases above. If $Q = \mathrm{SL}_2(q)$ with $q \notin \{4,5,7,9\}$, then we take the same t_1 and t_2 as indicated in the proof of [77, Lemma 5.3]. The group $\mathrm{L}_2(4)$ is invariably generated by an element of order 3 and an element of order 5, and if $q = 9$ then we take x and y to be of order 4 and 5, respectively. If $Q = \Omega_8^+(q)$ with $q \notin \{2,3\}$, then we take t_1 as in [77, Table 1], and t_2 an element of order $(q^3-1)/(2,q-1)$ as described in the proof of [77, Lemma 5.4], where it is denoted t_3. ■

It is worth noting that the excluded groups $\mathrm{L}_2(5)$, $\mathrm{L}_2(7)$, $\Omega_8^+(2)$ and $\mathrm{P}\Omega_8^+(3)$ in Theorem 5.2.9 are not invariably generated by any pair of regular semisimple elements of distinct orders. This can be checked using MAGMA [10]. More specifically, we find the set of maximal overgroups of an element $x \in T$ up to T-conjugacy using the method given in [25, Section 1.2], noting that x and y do not invariably generate T if there is a maximal subgroup M of T such that both $|x^T \cap M|$ and $|y^T \cap M|$ are non-empty.

As mentioned in Section 5.1, one of our probabilistic approaches in Section 5.4 relies on computing

$$h(T) := \max\{|C_T(x)| : 1 \neq x \in \mathrm{Aut}(T)\}$$

for every non-abelian finite simple group T.

Theorem 5.2.10. *Let T be a non-abelian finite simple group. Then $h(T)$ is listed in Tables 5.2 and 5.3.*

Remark 5.2.11. Let us briefly comment on the notation we adopt in the third columns of Tables 5.2 and 5.3, where we record an element $x \in \mathrm{Aut}(T)$ with $|C_T(x)| = h(T)$.

(i) We adopt the notation in [123] for labelling conjugacy classes when T is a sporadic group. If T is Lie type, then we write u_α for a long root element.

(ii) When $T = \mathrm{L}_n(q)$, we write ϕ for a field automorphism of order $f = \log_p q$, where p is the characteristic of the field $\mathbb{F}_q$.

(iii) If $T = \mathrm{L}_2(q)$, then let H be the normaliser in $\mathrm{PGL}_2(q)$ of a non-split maximal torus of T, so $H \cong D_{2(q+1)}$. We then define $s \in H$ to be the central involution if q is odd, and an arbitrary element of odd prime order if q is even.

T	$h(T)$	x	Conditions
A_n	$(n-2)!$	$(1,2)$	
$E_8(q)$	$q^{57}\lvert E_7(q)\rvert(2,q-1)$	u_α	
$E_7(q)$	$q^{33}\lvert \mathrm{SO}_{12}^{+}(q)\rvert/(2,q)$	u_α	
$E_6^{\varepsilon}(q)$	$q^{21}\lvert \mathrm{SL}_6^{\varepsilon}(q)\rvert/(3,q-\varepsilon)$	u_α	
$F_4(q)$	$q^{15}\lvert \mathrm{Sp}_6(q)\rvert$	u_α	
$G_2(q)$	$q^{5}\lvert \mathrm{SL}_2(q)\rvert$	u_α	$q \geqslant 3$
${}^3D_4(q)$	$q^{12}(q^6-1)$	u_α	
${}^2F_4(q)$	$q^{10}\lvert {}^2B_2(q)\rvert$	u_α	$q>2$
${}^2F_4(2)'$	10240	u_α	
${}^2G_2(q)$	q^3	u_α	$q \geqslant 27$
${}^2B_2(q)$	q^2	u_α	
$\mathrm{L}_n^{\varepsilon}(q)$	$\lvert \mathrm{PGL}_2(q^{1/2})\rvert$	$\phi^{f/2}$	$n=2$, f is even
	$q+1$	s	$n=2$, f is odd
	$\lvert \mathrm{PGL}_3(q^{1/2})\rvert$	$\phi^{f/2}$	$n=3$, $\varepsilon=+$, f is even, $3 \mid q^{1/2}+1$
	$\lvert \mathrm{PGU}_3(q^{1/2})\rvert$	$\phi^{f/2}\gamma$	$n=3$, $\varepsilon=+$, f is even, $3 \nmid q^{1/2}+1$
	$(2,q-\varepsilon)\lvert \mathrm{PGSp}_4(q)\rvert/(4,q-\varepsilon)$	γ_1	$n=4$
	$\lvert \mathrm{GU}_{n-1}(q)\rvert/(n,q+1)$	$[\omega I_1, I_{n-1}]$	$n \geqslant 6$ is even, $\varepsilon=-$
	$q^{2n-3}\lvert \mathrm{GL}_{n-2}^{\varepsilon}(q)\rvert/(n,q-\varepsilon)$	u_α	$n \geqslant 5$ is odd, or $\varepsilon=+$
$\mathrm{PSp}_n(q)$	$\lvert \mathrm{Sp}_2(q^2)\rvert$	t_1	$n=4$, q is odd
	$q^{n-1}\lvert \mathrm{Sp}_{n-2}(q)\rvert$	u_α	$n \geqslant 6$ or q is even, $(n,q)\neq(4,2)$
$\mathrm{P\Omega}_n^{\varepsilon}(q)$	$\lvert \mathrm{SO}_{n-1}^{-}(q)\rvert$	t_1'	n is odd
	$\lvert \mathrm{Sp}_{n-2}(q)\rvert$	b_1	n is even, q is even
	$\lvert \Omega_{n-1}(q)\rvert$	γ_1	n is even, q is odd

Table 5.2: $h(T)$ in Theorem 5.2.10 for non-sporadic groups

(iv) We adopt the notation in [21, Chapter 3] for elements of classical groups. For example, if $T = \mathrm{P\Omega}_n^{\varepsilon}(q)$, where n is even and q is odd, then a pre-image in $\mathrm{O}_n^{\varepsilon}(q)$ of an element of type γ_1 is an involution of the form $[-I_1, I_{n-1}]$ (see [21, Section 3.5.2.14]).

Proof of Theorem 5.2.10. First observe that we only need to consider prime order elements in $\mathrm{Aut}(T)$, since $C_T(x) \leqslant C_T(x^m)$ for any integer m and $x \in \mathrm{Aut}(T)$.

Assume $T = A_n$ is an alternating group. If $n=5$ or 6, then the result can be checked using MAGMA. Now assume $n \geqslant 7$, so $\mathrm{Aut}(T) = S_n$. It is easy to see that $|C_T(x)|$ is maximal when x is a transposition, in which case $C_{S_n}(x) \cong S_2 \times S_{n-2}$ and thus $|C_T(x)| = (n-2)!$. Hence, $h(T) = (n-2)!$. If T is a sporadic group, then $|C_T(x)|$ for all $x \in \mathrm{Aut}(T)$ can be read off from the character table of T (and also of $\mathrm{Aut}(T) = T.2$ if $|\mathrm{Out}(T)| = 2$), which can be accessed computationally via the GAP Character Table Library [12].

For the remainder, we may assume T is a simple group of Lie type over $\mathbb{F}_q$, where $q = p^f$ with p a prime. As discussed in Section 2.2.4, an element in $\mathrm{Aut}(T)$ of prime order is either contained in the group $\mathrm{Inndiag}(T)$ of inner-diagonal automorphisms (so it is semisimple or unipotent), or is a field, graph or graph-field automorphism. Recall Table 2.3 for the description of $\mathrm{Inndiag}(T)$.

T	$h(T)$	x
M_{11}	48	2A
M_{12}	240	2A
M_{22}	1344	2B
M_{23}	2688	2A
M_{24}	21504	2A
J_1	120	2A
J_2	1920	2A
J_3	2448	2B
J_4	21799895040	2A
HS	40320	2C
McL	40320	2A
Suz	9797760	3A
He	161280	2A
HN	177408000	2A
Ru	245760	2A
Ly	2694384000	3A
Co_1	1345036492800	3A
Co_2	743178240	2A
Co_3	2903040	2A
Th	92897280	2A
O′N	175560	2B
Fi_{22}	18393661440	2A
Fi_{23}	129123503308800	2A
Fi_{24}'	4089470473293004800	2C
$\mathbb{B}$	306129918735099415756800	2A
$\mathbb{M}$	8309562962452852382355161088000000	2A

Table 5.3: $h(T)$ in Theorem 5.2.10 for sporadic groups

Assume T is an exceptional group. Here we assume $T \neq {}^2G_2(3)' \cong \mathrm{L}_2(8)$ and $T \neq G_2(2)' \cong \mathrm{U}_3(3)$ as noted in (2.2.1). By [31, Proposition 2.11], $|C_T(x)|$ is maximal when $x \in T$ is a long root element. So let us assume $x \in T$ is a long root element. If T is not ${}^3D_4(q)$ or ${}^2B_2(q)$, then $|C_T(x)|$ can be read off from the tables in [94, Chapter 22], noting that $x^{\mathrm{Inndiag}(T)} = x^T$ by [94, Corollary 17.10]. If $T = {}^3D_4(q)$ or ${}^2B_2(q)$ then we can find $|C_T(x)|$ in [113, p. 677] and [117], respectively.

For the remainder of the proof, we assume T is a classical group defined over $\mathbb{F}_q$. Let V be the natural module of T and write $\overline{V} = V \otimes K$, where K is the algebraic closure of $\mathbb{F}_q$. For $x \in \mathrm{PGL}(V)$, let $\hat{x}$ be a pre-image of x in $\mathrm{GL}(V)$. Following [16, Definition 3.16], we define

$$\nu(x) = \min\{\dim[\overline{V}, \lambda\hat{x}] : \lambda \in K^\times\},$$

where $[\overline{V}, \lambda\hat{x}] = \{v - \lambda\hat{x}v : v \in \overline{V}\}$. That is, $\nu(x)$ is the codimension of the largest eigenspace of $\hat{x}$ on $\overline{V}$, noting that $\nu(x)$ is independent of the choice of pre-image $\hat{x}$. Upper and lower bounds on $|x^T|$ in terms of n, q and $\nu(x)$ are given in [16, Section 3]. Similarly, if x is a field, graph or graph-field automorphism, then lower bounds for $|x^T|$ can be read off from [16, Table 3.11]. In addition, $|C_{\mathrm{Inndiag}(T)}(x)|$, and a description of the splitting of $x^{\mathrm{Inndiag}(T)}$ into distinct T-classes, can be found in [21, Chapter 3]. In particular, note that if $x \in \mathrm{Inndiag}(T)$ is a semisimple element of prime order, then $x^{\mathrm{Inndiag}(T)} = x^T$ (see [60, Theorem 4.2.2(j)], also recorded as [21, Theorem 3.1.12]).

We start with the case where $T = \mathrm{L}_2(q)$. Let H be the normaliser in $\mathrm{PGL}_2(q)$ of a non-split maximal torus of T, so $H \cong D_{2(q+1)}$. If q is odd, then we let x be the central involution in H, and if q is even, let $x \in H$ be an element of odd prime order. Then $|C_T(x)| = q+1$, so $h(T) \geqslant q+1$. Let $y \in \mathrm{Aut}(T)$ be an element of prime order. Note that if y is unipotent then $|C_T(y)| = q$, whereas $|C_T(y)|$ divides $q+1$ or $q-1$ if y is semisimple. Thus, we only need to consider field automorphisms, noting that $|C_{\mathrm{PGL}_2(q)}(y)| = |\mathrm{PGL}_2(q^{1/r})|$ if y is a field automorphism of prime order r. It follows that $|C_{\mathrm{PGL}_2(q)}(y)| > q+1$ only if $r = 2$ (so f is even). Indeed,

$$|C_T(y)| = |C_{\mathrm{PGL}_2(q)}(y)| = |\mathrm{PGL}_2(q^{1/2})| > q+1$$

if y is an involutory field automorphism, and so we conclude that $h(T) = |\mathrm{PGL}_2(q^{1/2})|$ if f is even, and $h(T) = q+1$ if f is odd.

To complete the proof for linear and unitary groups, we assume $T = \mathrm{L}_n^{\varepsilon}(q)$ with $n \geqslant 3$. Let $x \in T$ be a unipotent element with Jordan form $[J_2, J_1^{n-2}]$ on the natural module, noting that x is a long root element. Then $|C_{\mathrm{PGL}_n^{\varepsilon}(q)}(x)|$ can be read off from [21, Tables B.3 and B.4], and we have $x^{\mathrm{PGL}_n^{\varepsilon}(q)} = x^T$ by [21, Propositions 3.2.7 and 3.3.10]. More specifically,

$$|C_T(x)| = (n, q-\varepsilon)^{-1} q^{2n-3} |\mathrm{GL}_{n-2}^{\varepsilon}(q)|$$

and

$$|x^T| = |x^{\mathrm{PGL}_n^{\varepsilon}(q)}| = \frac{|\mathrm{PGL}_n^{\varepsilon}(q)|}{q^{2n-3}|\mathrm{GL}_{n-2}^{\varepsilon}(q)|} < \frac{2q^{2n-1}}{q-1}.$$

The groups with $n \in \{3,4\}$ require special attention, and we treat them separately.

Assume $T = \mathrm{L}_3^{\varepsilon}(q)$, so $|C_T(x)| = (3, q-\varepsilon)^{-1} q^3 (q-\varepsilon)$, and let y be an element in $\mathrm{Aut}(T)$ of prime order that is not a long root element. If $y \in \mathrm{PGL}_3^{\varepsilon}(q)$ and $\nu(y) = 2$, then either y has Jordan form $[J_3]$ or $|y|$ is odd, so by [16, Propositions 3.22 and 3.36],

$$|y^T| > \frac{1}{2(3, q-\varepsilon)} \left(\frac{q}{q+1}\right) q^6 > (q^2-1)(q^2+\varepsilon q+1) = |x^T|.$$

If $\nu(y) = 1$ and y is semisimple, then a pre-image $\hat{y}$ of y in $\mathrm{GL}(V)$ is $[\omega I_1, I_2]$, so $|C_T(y)| = (3, q-\varepsilon)^{-1} |\mathrm{GL}_2^{\varepsilon}(q)|$. It is easy to see that $|C_T(y)| < |C_T(x)|$. If y is a graph automorphism, then $|C_{\mathrm{PGL}_3^{\varepsilon}(q)}(y)| = |\mathrm{SL}_2(q)|$, so $|C_T(y)| < |C_T(x)|$ evidently. If y is a field automorphism of odd prime order r, then by [21, Propositions 3.2.9 and 3.3.12],

$$|C_{\mathrm{PGL}_3^{\varepsilon}(q)}(y)| = |\mathrm{PGL}_3^{\varepsilon}(q^{1/r})| \leqslant q(q^{2/3}-1)(q-\varepsilon),$$

so $|C_T(y)| \leqslant |C_{\mathrm{PGL}_3^{\varepsilon}(q)}(y)| < |C_T(x)|$. Thus, we only need to consider involutory field or graph-field automorphisms, so we can assume $\varepsilon = +$ and f is even.

Let y_1 be an involutory field automorphism. Then by [21, Proposition 3.2.9],

$$|C_T(y_1)| = \frac{(3,q^{1/2}+1)}{(3,q-1)}|\mathrm{PGL}_3(q^{1/2})|.$$

Similarly, if y_2 is a graph-field automorphism, then

$$|C_T(y_2)| = \frac{(3,q^{1/2}-1)}{(3,q-1)}|\mathrm{PGU}_3(q^{1/2})|$$

by [21, Proposition 3.2.15]. Note that

$$|\mathrm{PGL}_3(q^{1/2})| < q^3(q-1) < |\mathrm{PGU}_3(q^{1/2})| < 3|\mathrm{PGL}_3(q^{1/2})|.$$

Therefore, $h(T) = |C_T(x)|$ if f is odd or $\varepsilon = -$, $h(T) = |C_T(y_1)|$ if $\varepsilon = +$, f is even and $3 \mid q^{1/2}+1$, otherwise $h(T) = |C_T(y_2)|$.

Next, assume $T = \mathrm{L}_4^{\varepsilon}(q)$ and let z be a graph automorphism of type γ_1 (see [21, Sections 3.2.5 and 3.3.5]), so by [21, Propositions 3.2.14 and 3.3.17], we have

$$|C_T(z)| = \frac{(2,q-\varepsilon)}{(4,q-\varepsilon)}|\mathrm{PGSp}_4(q)| > \frac{1}{(4,q-\varepsilon)}q^6(q^2-1)(q-\varepsilon) = |C_T(x)|$$

and we claim that $h(T) = |C_T(z)|$. Note that

$$|z^T| = \frac{q^2(q^3-\varepsilon)}{(2,q-\varepsilon)}.$$

By [16, Propositions 3.22, 3.36, 3.37 and 3.48], we have

$$|y^T| > \frac{1}{2}\left(\frac{q}{q+1}\right)q^6$$

for any unipotent, semisimple, field or graph-field element $y \in \mathrm{Aut}(T)$ of prime order. Hence, $|y^T| > |z^T|$ if $q \geqslant 4$, and for $q \in \{2,3\}$ we can check that $|y^T| > |z^T|$ using MAGMA. Similarly, if y is a graph automorphism, then $|y^T| \geqslant |z^T|$ by inspecting [21, Tables B.3 and B.4].

Finally, assume $T = \mathrm{L}_n^{\varepsilon}(q)$ and $n \geqslant 5$. Then by applying the bounds in [16, Table 3.11] we see that

$$|y^T| > \frac{1}{2}\left(\frac{q}{q+1}\right)^{\frac{1}{2}(1-\varepsilon)} q^{\frac{1}{2}(n^2-n-4)} > \frac{2q^{2n-1}}{q-1} > |x^T|$$

if y is a field, graph or graph-field automorphism, unless $(n,q) = (5,2)$ or $(6,2)$, in which cases one can check that $|y^T| > |x^T|$ with the aid of MAGMA. If y is a unipotent or semisimple element with $\nu(y) \geqslant 2$, then

$$|y^T| > \frac{1}{2}\left(\frac{q}{q+1}\right)q^{4n-8} > \frac{2q^{2n-1}}{q-1} > |x^T|$$

by [16, Proposition 3.36]. Thus, we only need to consider the cases where $\nu(y) = 1$ and y is not $\mathrm{Aut}(T)$-conjugate to x. In this setting, y is semisimple and a pre-image $\widehat{y}$ of y in $\mathrm{GL}(V)$ is $[\omega I_1, I_{n-1}]$, where ω is a non-trivial r-th root of unity in $\mathbb{F}_q$ if $\varepsilon = +$, or $\mathbb{F}_{q^2}$ if $\varepsilon = -$, for some prime r. It follows that

$$|C_T(y)| = (n,q-\varepsilon)^{-1}|\mathrm{GL}_{n-1}^{\varepsilon}(q)|.$$

Note that $|C_T(y)| > |C_T(x)|$ if and only if $\varepsilon = -$ and n is even. This implies that

$$h(T) = (n, q-\varepsilon)^{-1}|\mathrm{GL}^{\varepsilon}_{n-1}(q)|$$

if $\varepsilon = -$ and n is even, otherwise $h(T) = |C_T(x)|$.

This concludes the proof of Theorem 5.2.10 for linear and unitary groups. We can use a very similar approach to handle the symplectic and orthogonal groups and we omit the details. But let us remark that if $T = \mathrm{PSp}_n(q)$ is a symplectic group, then $|C_T(x)|$ is maximal when x is a long root element, unless $n = 4$ and q is odd, where an involution of type t_1 has the largest centraliser order. If $T = \mathrm{P\Omega}^{\varepsilon}_n(q)$, where n is odd or q is even, then $|C_T(x)|$ is maximal when x is an involution of type t'_1 or b_1, respectively. Finally, if $T = \mathrm{P\Omega}^{\varepsilon}_n(q)$ with n even and q odd, then a graph automorphism of type γ_1 has the largest centraliser order. All the relevant information about these elements can be found in [21, Chapter 3]. ∎

An immediate corollary is the following.

Corollary 5.2.12. *We have $h(T) \leqslant |T|/10$ for any non-abelian finite simple group T.*

5.3 Holomorph of simple groups

Recall that $\mathrm{Hol}(T) = T{:}\mathrm{Aut}(T)$ is the *holomorph* of T, which acts faithfully and primitively on T (in fact, $\mathrm{Hol}(T) = T^2.\mathrm{Out}(T)$ is a diagonal type primitive group). Note that every element in $\mathrm{Hol}(T)$ can be uniquely written as $g\alpha$, where $g \in T$ acts on T by left translation and $\alpha \in \mathrm{Aut}(T)$ acts naturally on T. That is,

$$t^{g\alpha} = (g^{-1}t)^{\alpha}$$

for every $t \in T$. Let $\mathrm{Hol}(T,S)$ be the setwise stabiliser of a subset $S \subseteq T$ in $\mathrm{Hol}(T)$. Throughout this section, we assume $P = S_k$, so $W = T^k.(\mathrm{Out}(T) \times S_k)$. The following result is a key observation.

Lemma 5.3.1. *The following statements are equivalent.*

(i) $\{D, D(\varphi_{t_1}, \dots, \varphi_{t_k})\}$ *is a base for W;*

(ii) $t_1, \dots, t_k$ *are distinct and* $\mathrm{Hol}(T, \{t_1, \dots, t_k\}) = 1$.

Proof. First assume (i) holds. If $t_i = t_j$ for some $i \neq j$, then $(i,j) \in W$ stabilises the points D and $D(\varphi_{t_1}, \dots, \varphi_{t_k})$, which is incompatible with (i). Thus, $t_1, \dots, t_k$ are distinct. Suppose $g\alpha \in \mathrm{Hol}(T, \{t_1, \dots, t_k\})$. Then for any i we have

$$t_j = t_i^{g\alpha} = (g^{-1}t_i)^{\alpha} = (g^{-1})^{\alpha} t_i^{\alpha} \tag{5.3.1}$$

for some j. That is, $g\alpha$ induces a permutation $\pi \in S_k$ by $(g^{-1})^{\alpha} t_i^{\alpha} = t_{i^{\pi}}$. Now it is easy to see that $(\alpha, \dots, \alpha)\pi$ fixes $D(\varphi_{t_1}, \dots, \varphi_{t_k})$. Hence, $\alpha = 1$ and $\pi = 1$, which implies that $g = 1$ by (5.3.1), noting that $i = j$ since $\pi = 1$.

Conversely, suppose (ii) holds and $(\alpha,\dots,\alpha)\pi$ fixes D and $D(\varphi_{t_1},\dots,\varphi_{t_k})$. Then there exists $g \in T$ such that $t_{i^\pi} = g^{-1}t_i^\alpha$ for all i. It follows that $g^{\alpha^{-1}}\alpha \in \mathrm{Hol}(T,\{t_1,\dots,t_k\})$, which implies that $g=1$ and $\alpha=1$. As $t_1,\dots,t_k$ are distinct, this gives $\pi=1$ and so (i) holds. ■

Let $\mathscr{P}_k(T)$ (or just $\mathscr{P}_k$ if T is clear from the context) be the set of k-subsets of T. Recall that $r(G)$ is the number of regular suborbits of G.

Lemma 5.3.2. *The number of regular orbits of* $\mathrm{Hol}(T)$ *on* $\mathscr{P}_k$ *or* $\mathscr{P}_{|T|-k}$ *is* $r(W)$. *In particular,* $b(W)=2$ *if and only if* $\mathrm{Hol}(T)$ *has a regular orbit on* $\mathscr{P}_k$ *or* $\mathscr{P}_{|T|-k}$.

Proof. This follows directly from Lemma 5.3.1, noting that $\mathrm{Hol}(T,S)=\mathrm{Hol}(T,T\setminus S)$. ■

Given a subset $S \subseteq T$, it is difficult to determine $\mathrm{Hol}(T,S)$. In particular, it is difficult to construct a subset $S\subseteq T$ such that $\mathrm{Hol}(T,S)=1$. By the transitivity of $\mathrm{Hol}(T)$ on T, we may assume $1\in S$.

Lemma 5.3.3. *Let X_1 and X_2 be subsets of T such that $1\in X_1\cap X_2$ and $X_1^{g\alpha}=X_2$. Then $g\in X_1$.*

Proof. We have $g^{-1}X_1 = X_2^{\alpha^{-1}}$, so $1\in g^{-1}X_1$ and thus $g\in X_1$. ■

Now we give some sufficient conditions that allow us to deduce that $\mathrm{Hol}(T,S)=1$ for a subset $S\subseteq T$ containing 1. Here we write $\mathrm{Aut}(T,R)$ for the setwise stabiliser of $R\subseteq T^\#$ in $\mathrm{Aut}(T)$.

Lemma 5.3.4. *Let $S=\{t_1,\dots,t_k\}\in\mathscr{P}_k$ with $t_1=1$. Then* $\mathrm{Hol}(T,S)=1$ *if the following conditions are satisfied:*

(i) $\mathrm{Aut}(T,\{t_2,\dots,t_k\})=1$*; and*

(ii) For all $2\leqslant i\leqslant k$, $\{|t_i^{-1}t_1|,\dots,|t_i^{-1}t_k|\}\neq\{1,|t_2|,\dots,|t_k|\}$.

Proof. Suppose $g\alpha\in\mathrm{Hol}(T,S)$, where $g\in T$ and $\alpha\in\mathrm{Aut}(T)$. By Lemma 5.3.3, we have $g\in S$. If $g=t_1=1$ then $\alpha\in\mathrm{Aut}(T,\{t_2,\dots,t_k\})$ and condition (i) forces $\alpha=1$. If $g=t_i$ for some $2\leqslant i\leqslant k$ then $t_i^{-1}S=S^{\alpha^{-1}}$, which implies that $\{|t_i^{-1}t_1|,\dots,|t_i^{-1}t_k|\}=\{1,|t_2|,\dots,|t_k|\}$, which is incompatible with the condition (ii). ■

Corollary 5.3.5. *Let $S=\{t_1,\dots,t_k\}\in\mathscr{P}_k$ with $t_1=1$. If* $\mathrm{Out}(T)=1$ *then* $\mathrm{Hol}(T,S)=1$ *if all the following conditions are satisfied:*

(i) $t_2,\dots,t_k$ have distinct orders;

(ii) $M=\langle t_2,\dots,t_k\rangle$ is a maximal subgroup of T such that $Z(M)=1$;

(iii) for all $2\leqslant i\leqslant k$, $\{|t_i^{-1}t_1|,\dots,|t_i^{-1}t_k|\}\neq\{1,|t_2|,\dots,|t_k|\}$.

Proof. In view of Lemma 5.3.4, it suffices to show that conditions (i) and (ii) imply that $\mathrm{Aut}(T,\{t_2,\dots,t_k\})=1$. Suppose $\alpha\in\mathrm{Aut}(T,\{t_2,\dots,t_k\})$. Then $\alpha\in C_{\mathrm{Aut}(T)}(t_i)$ for each i, as $t_2,\dots,t_k$ have distinct orders. It follows that α centralises $\langle t_2,\dots,t_k\rangle=M$ and so $\alpha\in C_{\mathrm{Aut}(T)}(M)$. Since $\mathrm{Out}(T)=1$, this implies that $\alpha\in C_T(M)\leqslant N_T(M)=M$ since M is maximal, so $\alpha\in Z(M)=1$. This completes the proof. ■

Lemma 5.3.6. *Let $X_1=\{t_1,\dots,t_k\}$ and $X_2=\{s_1,\dots,s_k\}$ be k-sets in $\mathscr{P}_k$ such that $1\in X_1\cap X_2$ and* $\mathrm{Hol}(T,X_j)=1$ *for each $j\in\{1,2\}$. Then X_1 and X_2 are in distinct* $\mathrm{Hol}(T)$*-orbits if*

$$\{|t_i^{-1}t_1|,\dots,|t_i^{-1}t_k|\}\neq\{|s_1|,\dots,|s_k|\}$$

for any $i\in[k]$.

Proof. This follows immediately from Lemma 5.3.3. ■

Remark 5.3.7. Let us briefly discuss the main computational techniques we will use to show that $r(W)\geqslant 2$ for some suitable T and k. We refer the reader to Appendix A.1.3 for the relevant MAGMA function `RanHolOrder` to implement this approach.

(i) Let X_1 and X_2 be k-element subsets of T containing 1, and let $O_j=\{|t|:t\in X_j\}$. Assume that $|O_j|=k$, $\langle X_j\rangle=T$ and

$$O_j\neq\{|x^{-1}t|:t\in X_j\}$$

for any $x\in X_j\setminus\{1\}$. Then $\mathrm{Hol}(T,X_j)=1$ by Lemma 5.3.4, noting that the first two conditions imply that $\mathrm{Aut}(T,X_j\setminus\{1\})=1$. Combining Lemmas 5.3.2 and 5.3.6, we have $r(W)\geqslant 2$ if

$$O_2\neq\{|x^{-1}t|:t\in X_1\}$$

for any $x\in X_1$. For suitable T and k, we can construct T in terms of an appropriate permutation representation in MAGMA, and implement this approach to find k-subsets X_1 and X_2 of T with these properties by random search. We will only need to use this method for $k\leqslant 11$.

(ii) In some cases where $\mathrm{Out}(T)=1$, we will work with a centreless maximal subgroup M of T, rather than T itself. More precisely, if X_1 and X_2 are k-element subsets of M containing 1 and $O_j=\{|t|:t\in X_j\}$, then by Corollary 5.3.5, we have $\mathrm{Hol}(T,X_j)=1$ if $|O_j|=k$, $\langle X_j\rangle=M$ and

$$O_j\neq\{|x^{-1}t|:t\in X_j\}$$

for any $x\in X_j\setminus\{1\}$. Again, by Lemmas 5.3.2 and 5.3.6, we have $r(W)\geqslant 2$ if

$$O_2\neq\{|x^{-1}t|:t\in X_1\}$$

for any $x\in X_1$. For example, if $T=\mathbb{M}$ is the Monster sporadic group and $3\leqslant k\leqslant 5$, then we will work with a maximal subgroup M of T isomorphic to $\mathrm{L}_2(71)$ (this case arises in the proofs of Lemma 5.5.2 and Proposition 5.5.10).

5.4 Probabilistic methods

In this section, we assume $G = T^k.(\mathrm{Out}(T) \times S_k)$ with $2 < k < |T|$. By Lemma 5.3.2, we have $r(G) \geqslant 2$ for $k = m$ if and only if $r(G) \geqslant 2$ for $k = |T| - m$, so we will assume $5 \leqslant k \leqslant |T|/2$ throughout this section (we will treat the cases where $k \in \{3,4\}$ separately in Section 5.5).

In Section 5.4.1, we will estimate the probability $\mathrm{Pr}_k(T)$ that a random k-subset of T has non-trivial setwise stabiliser in $\mathrm{Hol}(T)$, noting that

$$\mathrm{Pr}_k(T) = \frac{|\{S \in \mathscr{P}_k : \mathrm{Hol}(T,S) \neq 1\}|}{\binom{|T|}{k}}. \tag{5.4.1}$$

In view of Lemma 5.3.2, we have $r(G) \geqslant 2$ if and only if

$$\mathrm{Pr}_k(T) < 1 - \frac{|\mathrm{Hol}(T)|}{\binom{|T|}{k}}. \tag{5.4.2}$$

To establish this inequality, we will give upper bounds on $\mathrm{Pr}_k(T)$ in Section 5.4.1. In particular, we will show that $r(G) \geqslant 2$ if $4\log|T| < k \leqslant |T|/2$ (see Proposition 5.4.7).

Finally, to handle certain cases where k is small, in Section 5.4.2 we will consider the probability $Q(G,2)$ that a random pair of elements in Ω is not a base for G, which we recall is a widely used method in the study of base sizes (see Section 2.4).

5.4.1 Holomorph and subsets

We first consider $\mathrm{Pr}_k(T)$, as defined in (5.4.1). Let $\mathscr{F} = \{S \in \mathscr{P}_k : \mathrm{Hol}(T,S) \neq 1\}$ and suppose $S \in \mathscr{F}$. Then there exists $\sigma \in \mathrm{Hol}(T,S)$ of prime order. In other words, $S \in \mathrm{fix}(\sigma, \mathscr{P}_k)$, where

$$\mathrm{fix}(\sigma, \mathscr{P}_k) = \{S \in \mathscr{P}_k : \sigma \in \mathrm{Hol}(T,S)\}$$

is the set of fixed points of σ on $\mathscr{P}_k$. It follows that

$$|\mathscr{F}| = \left|\bigcup_{\sigma \in \mathscr{R}} \mathrm{fix}(\sigma, \mathscr{P}_k)\right| \leqslant \sum_{\sigma \in \mathscr{R}} |\mathrm{fix}(\sigma, \mathscr{P}_k)|,$$

where $\mathscr{R}$ is the set of elements of prime order in $\mathrm{Hol}(T)$. Recall that $r(G) \geqslant 2$ if and only if (5.4.2) holds. Thus, $r(G) \geqslant 2$ if

$$\sum_{\sigma \in \mathscr{R}} |\mathrm{fix}(\sigma, \mathscr{P}_k)| < \binom{|T|}{k} - |\mathrm{Hol}(T)|.$$

Moreover, since $5 \leqslant k \leqslant |T|/2$, we note that $|\mathrm{Hol}(T)| < \frac{1}{2}\binom{|T|}{k}$ by Lemma 2.2.5. This observation yields the following result.

Lemma 5.4.1. *We have $r(G) \geqslant 2$, and hence $b(G) = 2$, if*

$$\binom{|T|}{k} > 2 \sum_{\sigma \in \mathscr{R}} |\mathrm{fix}(\sigma, \mathscr{P}_k)|. \tag{5.4.3}$$

In order to apply Lemma 5.4.1, we need to derive a suitable upper bound for the summation appearing on the right-hand side of (5.4.3).

Lemma 5.4.2. *Let $\sigma \in \mathrm{Hol}(T)$ be of prime order r with cycle shape $[r^m, 1^{|T|-mr}]$. Then*

$$|\mathrm{fix}(\sigma, \mathscr{P}_k)| = \sum_{u=0}^{\lfloor k/r \rfloor} \binom{m}{u}\binom{|T|-mr}{k-ru}.$$

Proof. This follows by noting that any subset fixed by σ is a union of some cycles comprising σ. ■

If $\sigma \in \mathrm{Hol}(T)$ is an element as described in Lemma 5.4.2, then $|T| - mr$ is the number of elements in T fixed by σ. It follows that $|T| - mr \leqslant \mathrm{fix}(\mathrm{Hol}(T))$, where $\mathrm{fix}(\mathrm{Hol}(T))$ is the fixity of $\mathrm{Hol}(T)$ (the *fixity* of a permutation group is the maximum number of elements fixed by a non-identity permutation). Recall that

$$h(T) = \max\{|C_T(x)| : 1 \neq x \in \mathrm{Aut}(T)\},$$

which has been determined in Theorem 5.2.10.

Lemma 5.4.3. *We have* $\mathrm{fix}(\mathrm{Hol}(T)) = h(T)$.

Proof. Let $\sigma \in \mathrm{Hol}(T)$ be such that it fixes at least one element in T. We may assume σ fixes $1 \in T$ by the transitivity of $\mathrm{Hol}(T)$. Thus, $\sigma \in \mathrm{Aut}(T)$ and hence $C_T(\sigma)$ is the set of fixed points of σ, which completes the proof. ■

Corollary 5.4.4. *If $\sigma \in \mathrm{Hol}(T)$ has prime order r, then*

$$|\mathrm{fix}(\sigma, \mathscr{P}_k)| \leqslant \sum_{u=0}^{\lfloor k/r \rfloor} \binom{|T|/r}{u}\binom{h(T)}{k-ru}.$$

The following bounds on binomial coefficients come from [114, Theorem 2.6], where e is the exponential constant.

Lemma 5.4.5. *Let ℓ, m, n be positive integers with $n > m$. Then*

$$e^{-\frac{1}{8\ell}} a(\ell, m, n) < \binom{n\ell}{m\ell} < a(\ell, m, n),$$

where

$$a(\ell, m, n) = \frac{1}{\sqrt{2\pi}} \ell^{-\frac{1}{2}} \left(\frac{n}{(n-m)m}\right)^{\frac{1}{2}} \left(\frac{n^n}{(n-m)^{n-m} m^m}\right)^{\ell}.$$

Corollary 5.4.6. *Suppose $n = tm$ for some integer $t \geqslant 2$. Then*

$$e^{-\frac{1}{8}} \left(\frac{t^2}{(t-1)n}\right)^{\frac{1}{2}} \left(\frac{t^t}{(t-1)^{t-1}}\right)^{\frac{n}{t}} < \sqrt{2\pi}\binom{n}{m} < \left(\frac{t^2}{(t-1)n}\right)^{\frac{1}{2}} \left(\frac{t^t}{(t-1)^{t-1}}\right)^{\frac{n}{t}}. \tag{5.4.4}$$

Proof. Put $\ell = 1$ and $m = n/t$ in Lemma 5.4.5. ■

Proposition 5.4.7. *If* $4\log|T| < k \leqslant |T|/2$, *then* $r(G) \geqslant 2$. *In particular,* $b(G) = 2$.

Proof. First, if $T = A_5$, then we construct $\mathrm{Hol}(T)$ as a permutation group on T via the function `Holomorph` in MAGMA. We then find two k-subsets of T lying in distinct regular $\mathrm{Hol}(T)$-orbits by random search (see the function `RanHol` in Appendix A.1.3).

Hence, we may assume $|T| \geqslant 168$ and thus $4\log|T| < |T|/4$. First assume $|T|/4 \leqslant k \leqslant |T|/2$. By Corollary 5.4.4, we have

$$|\mathrm{fix}(\sigma, \mathscr{P}_k)| \leqslant \sum_{u=0}^{\lfloor k/r \rfloor} \binom{|T|/r}{u}\binom{h(T)}{\lfloor h(T)/2 \rfloor} \leqslant 2^{|T|/r}\binom{h(T)}{\lfloor h(T)/2 \rfloor} \leqslant 2^{|T|/2}\binom{h(T)}{\lfloor h(T)/2 \rfloor}$$

for every element $\sigma \in \mathrm{Hol}(T)$ of prime order. Hence, (5.4.3) holds if

$$\binom{|T|}{k} > |\mathrm{Hol}(T)| 2^{|T|/2+1}\binom{h(T)}{\lfloor h(T)/2 \rfloor}, \tag{5.4.5}$$

and it suffices to consider $k = |T|/4$. Now we apply (5.4.4), which gives

$$\binom{|T|}{|T|/4} > \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{8}} \frac{4}{\sqrt{3|T|}} \left(\frac{4}{3^{3/4}}\right)^{|T|}$$

and

$$\binom{h(T)}{\lfloor h(T)/2 \rfloor} < \frac{1}{\sqrt{2\pi}} \cdot \sqrt{\frac{4}{h(T)}} \cdot 2^{h(T)} \leqslant \frac{1}{\sqrt{2\pi}} \cdot \sqrt{\frac{40}{|T|}} \cdot 2^{|T|/10}$$

as $h(T) \leqslant |T|/10$ by Corollary 5.2.12. Combining the inequalities above, we see that (5.4.5) holds for $k = |T|/4$ if

$$\frac{1}{\sqrt{2\pi}} e^{-\frac{1}{8}} \frac{4}{\sqrt{3|T|}} \left(\frac{4}{3^{3/4}}\right)^{|T|} > |\mathrm{Hol}(T)| \cdot 2^{|T|/2+1} \cdot \frac{1}{\sqrt{2\pi}} \cdot \sqrt{\frac{40}{|T|}} \cdot 2^{|T|/10}.$$

Finally, since $|\mathrm{Out}(T)| < |T|^{1/3}$ by Lemma 2.2.5, it suffices to show that

$$t_0^{|T|} > \sqrt{30}\, e^{\frac{1}{8}} |T|^{\frac{7}{3}}, \tag{5.4.6}$$

where

$$t_0 = 4 \cdot 3^{-\frac{3}{4}} \cdot 2^{-\frac{1}{2}-\frac{1}{10}} = 1.1577....$$

and it is easy to check that the inequality in (5.4.6) holds for all $|T| \geqslant 168$.

Now assume $4\log|T| < k < |T|/4$ and let $\sigma \in \mathrm{Hol}(T)$ be of prime order r. Observe that $ru \leqslant k < |T|/4$ for all $u \in \{0, \ldots, \lfloor k/r \rfloor\}$, so

$$\begin{aligned}\sum_{u=0}^{\lfloor k/r \rfloor} \binom{|T|/r}{u}\binom{h(T)}{k-ru} &< \sum_{u=0}^{\lfloor k/r \rfloor} \binom{|T|/2}{u}\binom{h(T)}{k-ru}\\ &< \sum_{u=0}^{\lfloor k/r \rfloor} \binom{|T|/2}{ru}\binom{h(T)}{k-ru}\\ &< \binom{|T|/2+h(T)}{k},\end{aligned}$$

noting that the third inequality follows from Vandermonde's identity. Thus, (5.4.3) holds if

$$\binom{|T|}{k} > 2|\mathrm{Hol}(T)|\binom{|T|/2+h(T)}{k}. \tag{5.4.7}$$

It is easy to see that (5.4.7) is equivalent to

$$\frac{|T|!}{(|T|-k)!} > 2|\mathrm{Hol}(T)|\frac{(|T|/2+h(T))!}{(|T|/2+h(T)-k)!}.$$

Now

$$\frac{|T|-m}{|T|/2+h(T)-m} \geqslant \frac{|T|}{|T|/2+h(T)} =: t$$

for every $m \in \{0,\dots,k-1\}$ and thus (5.4.7) holds if $t^k > 2|\mathrm{Hol}(T)|$. By Corollary 5.2.12, we have $|T|/h(T) \geqslant 10$, and hence $t \geqslant 5/3$. Therefore, (5.4.7) holds if $(5/3)^k > |T|^{8/3}$ (by applying Lemma 2.2.5), which implies the desired result. ■

Now we turn to the cases where $5 \leqslant k \leqslant 4\log|T|$. We start by giving some sufficient conditions for $r(G) \geqslant 2$.

Lemma 5.4.8. *Suppose* $5 \leqslant k \leqslant 4\log|T|$. *Then* $r(G) \geqslant 2$, *and hence* $b(G) = 2$, *if*

$$\binom{|T|}{k} > 2|\mathrm{Hol}(T)|\sum_{u=0}^{\lfloor k/2\rfloor}\binom{|T|/2}{u}\binom{h(T)}{k-2u}. \tag{5.4.8}$$

Proof. If $8\log|T| < h(T)$, then $k < h(T)/2$ and (5.4.3) follows via (5.4.8) and Corollary 5.4.4. By inspecting Table 5.2, we see that $8\log|T| \geqslant h(T)$ only if T is isomorphic to one of the following groups:

$$\mathrm{M}_{11},\ \mathrm{J}_1,\ {}^2B_2(8),\ \mathrm{L}_3(3),\ \mathrm{L}_2(q)\ (q \leqslant 167). \tag{5.4.9}$$

Assume T is one of the groups in (5.4.9) and suppose $\sigma \in \mathrm{Hol}(T)$ has prime order r. We claim that

$$|\mathrm{fix}(\sigma, \mathscr{P}_k)| < \sum_{u=0}^{\lfloor k/2\rfloor}\binom{|T|/2}{u}\binom{h(T)}{k-2u}. \tag{5.4.10}$$

To see this, first assume σ is fixed-point-free on T. Then $|\mathrm{fix}(\sigma, \mathscr{P}_k)| = 0$ if $r \nmid k$, and

$$|\mathrm{fix}(\sigma, \mathscr{P}_k)| = \binom{|T|/r}{k/r}$$

otherwise. In particular, the inequality in (5.4.10) holds. Now assume σ has a fixed point on T. Since σ is conjugate to an element fixing the identity element in T, we may assume $\sigma \in \mathrm{Aut}(T)$. Then with the aid of MAGMA and Corollary 5.4.4, it is easy to check that (5.4.10) holds when T is one of the groups in (5.4.9).

We conclude that the proof is complete by combining (5.4.8) and (5.4.10) with Lemma 5.4.1. ■

Lemma 5.4.9. *The inequality* (5.4.8) *holds if*

$$2^u u^u |T|^{k-u} > 2|\mathrm{Hol}(T)|\lfloor k/2\rfloor k^{2u} e^{k+u} h(T)^{k-2u} \tag{5.4.11}$$

for every $u \in \{0,\dots,\lfloor k/2\rfloor\}$, where we define $u^u = 1$ if $u = 0$.

Proof. First observe that (5.4.8) holds if

$$\binom{|T|}{k} > 2|\mathrm{Hol}(T)|\lfloor k/2\rfloor \binom{|T|/2}{u}\binom{h(T)}{k-2u} \tag{5.4.12}$$

for every $u \in \{0,\dots,\lfloor k/2\rfloor\}$. Now

$$\left(\frac{k}{k-2u}\right)^{k-2u} < e^{2u}$$

for all such u. Therefore, (5.4.12) follows by combining (5.4.11) and the well-known bounds on binomial coefficients

$$\frac{n^m}{m^m} \leqslant \binom{n}{m} \leqslant \frac{(en)^m}{m^m}$$

for any integers $n \geqslant m \geqslant 0$, where we define $m^m = 1$ if $m = 0$. ■

We conclude this section by establishing two more technical lemmas, which will play a key role in Section 5.5.

Lemma 5.4.10. *Suppose $|T| > 4080$ and $5 \leqslant k \leqslant 4\log|T|$. Then* (5.4.8) *holds if there exists an integer k_0 in the range $5 \leqslant k_0 \leqslant k$ such that*

$$|T|^{k_0} > |\mathrm{Hol}(T)|^2 k_0^{2+k_0} e^{3k_0} \tag{5.4.13}$$

and

$$h(T)^2 < k_0|T|. \tag{5.4.14}$$

Proof. We first prove that (5.4.8) holds if $k = k_0$. In view of Lemma 5.4.9, it suffices to verify the inequality in (5.4.11) for all $u \in \{0,\dots,\lfloor k/2\rfloor\}$ and we will do this by induction. First assume $u = \lfloor k/2\rfloor$ and note that (5.4.13) is equivalent to (5.4.11) if k is even. For k odd we have $u = (k-1)/2$ and the inequality in (5.4.11) is as follows:

$$\left(\frac{|T|(k-1)}{k^2e^3}\right)^k |T| > \frac{k-1}{k^2e}\cdot 4|\mathrm{Hol}(T)|^2\left(\frac{k-1}{2}\right)^2 h(T)^2. \tag{5.4.15}$$

In view of (5.4.14), we see that (5.4.15) holds if

$$\left(\frac{|T|}{ke^3}\right)^k\left(\frac{k-1}{k}\right)^{k-1} e > k^2|\mathrm{Hol}(T)|^2,$$

which is implied by (5.4.13) since $(\frac{k-1}{k})^{k-1} > e^{-1}$. Therefore, (5.4.11) holds for $u = \lfloor k/2\rfloor$ and we have established the base case for the induction. Now suppose (5.4.11) holds for $u = u_0$, where

$1 \leqslant u_0 \leqslant \lfloor k/2 \rfloor$. It suffices to show that (5.4.11) holds for $u = u_0 - 1$. Here the desired inequality holds if

$$2^{-1}|T| \cdot \frac{(u_0-1)^{u_0-1}}{u_0^{u_0}} > k^{-2}e^{-1} \cdot h(T)^2,$$

but this is implied by (5.4.14), noting that $(\frac{u_0-1}{u_0})^{u_0-1} > e^{-1}$ and $2u_0 \leqslant k$. In conclusion, if $k = k_0$ then (5.4.11) holds for all $u \in \{0, \dots, \lfloor k/2 \rfloor\}$ and thus (5.4.8) holds by Lemma 5.4.9.

Finally, we need to show that (5.4.8) holds when $k_0 < k$. By (5.4.14) we have $h(T)^2 < k_0|T| < k|T|$, and by arguing as above, it suffices to show that

$$|T|^k > |\mathrm{Hol}(T)|^2 k^{2+k} e^{3k}. \tag{5.4.16}$$

Since $|T| > 4080$ and $5 \leqslant k \leqslant 4\log|T|$, we get

$$|T| > 2e^4(4\log|T|+1) \geqslant 2e^4(k+1) > \left(\frac{k+1}{k}\right)^{k+2} e^3(k+1).$$

Therefore, (5.4.16) holds for all $k_0 \leqslant k \leqslant 4\log|T|$ by induction on k, and the proof is complete. ■

Lemma 5.4.11. *Suppose* $5 \leqslant k \leqslant 4\log|T|$. *Then* (5.4.8) *holds if there exists an integer* k_0 *such that* $5 \leqslant k_0 \leqslant k$,

$$|T|^{k_0} > 2|\mathrm{Hol}(T)|\lfloor k_0/2 \rfloor e^{k_0} h(T)^{k_0} \tag{5.4.17}$$

and

$$2h(T)^2 > (4\log|T|)^2 e|T|. \tag{5.4.18}$$

Proof. This is similar to the proof of Lemma 5.4.10, working with Lemma 5.4.9 to establish the inequality in (5.4.8). First assume $k = k_0$ and note that (5.4.17) is equivalent to (5.4.11) with $u = 0$. We now use induction to show that (5.4.11) holds for all $u \in \{0, \dots, \lfloor k/2 \rfloor\}$. To do this, suppose (5.4.11) holds for $u = u_0$, where $0 \leqslant u_0 \leqslant \lfloor k/2 \rfloor - 1$. Then (5.4.18) implies that

$$2|T|^{-1} \cdot \frac{(u_0+1)^{u_0+1}}{u_0^{u_0}} > k^2 e \cdot h(T)^{-2},$$

and thus (5.4.11) holds for $u = u_0 + 1$ and the result follows.

Finally, let us assume $k_0 < k$. It suffices to show that

$$|T|^k > 2|\mathrm{Hol}(T)|\lfloor k/2 \rfloor e^k h(T)^k$$

for all $k_0 \leqslant k \leqslant 4\log|T|$. This is clear by induction on k, since we have $|T| > 2eh(T)$ for every T by Corollary 5.2.12. ■

5.4.2 Fixed point ratios

Now we turn to the probabilistic approach discussed in Section 2.4 to study $b(G)$, where $G = T^k.(\mathrm{Out}(T)\times S_k)$. Here we will estimate the probability $\mathbb{P}_k(T) := 1-Q(G,2)$ that a random element in Ω is in a regular orbit of $G_D = D$, noting that $b(G) = 2$ if and only if $\mathbb{P}_k(T) > 0$. Equivalently,

$$\mathbb{P}_k(T) = \frac{r(G)|G|}{|T|^{2k-2}}$$

is the probability that a random pair of elements in Ω is a base for G. In view of (2.4.2), we have

$$1-\mathbb{P}_k(T) \leqslant \sum_{x\in R(G)} |x^G|\cdot \mathrm{fpr}(x)^2 = \sum_{x\in R(G)} \frac{|x^G\cap D|^2|C_G(x)|}{|G|},$$

where $R(G)$ is a set of representatives for the G-conjugacy classes of elements in the stabiliser D in G which have prime order. We adopt the notation from [51, Section 4] and define

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

and

$$r_i(G) := \sum_{x\in R_i(G)} \frac{|x^G\cap D|^2|C_G(x)|}{|G|}.$$

It follows that

$$1-\frac{r(G)|G|}{|T|^{2k-2}} = 1-\mathbb{P}_k(T) \leqslant r_1(G)+r_2(G)+r_3(G), \tag{5.4.19}$$

which gives a lower bound on $r(G)$. In particular, $b(G) = 2$ if $r_1(G)+r_2(G)+r_3(G) < 1$. Thus, we need to bound each $r_i(G)$ above.

Lemma 5.4.12. *We have* $r_1(G) < (k!)^2|T|^{8/3-\lceil k/2\rceil}$.

Proof. This is established in the proof of Theorem 1.5 in [51]. ■

Lemma 5.4.13. *We have* $r_2(G) < (|T|/h(T))^{4-k}$.

Proof. Let $f_p(\mathrm{Aut}(T))$ be the number of conjugacy classes of elements of prime order in $\mathrm{Aut}(T)$. It follows from the proof of [51, Lemma 4.2] that

$$r_2(G) \leqslant |\mathrm{Out}(T)|f_p(\mathrm{Aut}(T))\left(\frac{h(T)}{|T|}\right)^{k-2}.$$

Thus, it suffices to show that

$$|\mathrm{Out}(T)|f_p(\mathrm{Aut}(T)) < \left(\frac{|T|}{h(T)}\right)^2. \tag{5.4.20}$$

First assume $T = A_n$ is an alternating group. Then as discussed in the proof of [51, Lemma 4.2], we have $f_p(\mathrm{Aut}(T)) < \frac{n^2}{2}$. This implies (5.4.20) since $h(T) = (n-2)!$ by Theorem 5.2.10.

Next, assume T is a sporadic group. Then $f_p(\mathrm{Aut}(T))$ can be read off from the character table of $\mathrm{Aut}(T)$ and it is easy to check that (5.4.20) holds in every case.

Finally, assume T is a simple group of Lie type over $\mathbb{F}_q$. Let $f(T)$ be the number of conjugacy classes in T. As noted in [55], we have $f_p(\mathrm{Aut}(T)) \leqslant |\mathrm{Out}(T)| f(T)$. Thus, it suffices to show that

$$|\mathrm{Out}(T)|^2 f(T) < \left(\frac{|T|}{h(T)}\right)^2. \tag{5.4.21}$$

We divide the proof into several cases.

Case 1. $T \neq \mathrm{L}_n^{\varepsilon}(q)$.

Here [57, Theorem 1.2] implies that $f(T) < |T|/h(T)$, so in view of (5.4.21) it suffices to show that

$$h(T)|\mathrm{Out}(T)|^2 < |T|. \tag{5.4.22}$$

First assume $T \neq \mathrm{P}\Omega_8^+(q)$. Then $|\mathrm{Out}(T)| \leqslant 8\log q$ and by inspecting Table 5.2, one can see that $|T|/h(T) \geqslant q^3/2$. It is straightforward to check that if $q \geqslant 13$, then $128(\log q)^2 < q^3$, which implies that (5.4.22) holds for $q \geqslant 13$. Then there are only finitely many exceptional groups of Lie type to consider, and in each case we can use the precise value of $h(T)$ in Table 5.2 to verify (5.4.22). Hence, we may assume $q \leqslant 11$ and T is a classical group. By our assumption, $T = \mathrm{PSp}_n(q)$, $\Omega_n(q)$, $\mathrm{P}\Omega_n^-(q)$, or $\mathrm{P}\Omega_n^+(q)$ with $n \geqslant 10$ in the latter case. In each case, we have $|T|/h(T) > q^{n-2}$ by inspecting Table 5.2, so if $n \geqslant 8$ we get

$$|\mathrm{Out}(T)|^2 \leqslant 64(\log q)^2 \leqslant q^6 \leqslant q^{n-2} < |T|/h(T)$$

and thus (5.4.22) holds. There are finitely many groups remaining and we can check that (5.4.22) holds in each case by using precise values of $h(T)$ and $|\mathrm{Out}(T)|$.

Now assume $T = \mathrm{P}\Omega_8^+(q)$. Here $|T|/h(T) > q^6$ and $|\mathrm{Out}(T)| \leqslant 24f \leqslant 24\log q$. This shows that (5.4.22) holds for $q \geqslant 4$ since we have $24^2(\log q)^2 < q^6$. If $q = 2$, then $|\mathrm{Out}(T)|^2 = 36 < 120 = |T|/h(T)$, while for $q = 3$, we have $|\mathrm{Out}(T)|^2 = 576 < 1080 = |T|/h(T)$.

Case 2. $T = \mathrm{U}_n(q)$, $n \geqslant 3$.

In this case, [57, Theorem 1.2] implies that $f(T) < \frac{1}{2}|T|/h(T)$, except when $(n,q) = (3,3)$ or $(4,3)$. In the latter two cases, it is easy to check (5.4.21). In the remaining cases, we have $|T|/h(T) > q^n$ by inspecting Table 5.2, so (5.4.21) holds if

$$|\mathrm{Out}(T)|^2 < 2q^n. \tag{5.4.23}$$

Notice that $|\mathrm{Out}(T)| \leqslant 2(q+1)\log q < q^2$ for $q \geqslant 7$, and for $q \in \{3,5\}$ we still have $|\mathrm{Out}(T)| \leqslant 2(q+1) < q^2$. This implies that if $q \notin \{2,4\}$ and $n \geqslant 4$, then

$$|\mathrm{Out}(T)|^2 < q^4 \leqslant q^n < 2q^n$$

and so (5.4.23) is satisfied. If $q=2$ then $|\mathrm{Out}(T)| \leqslant 6$, so (5.4.23) holds if $n \geqslant 5$; and if $q=4$ then $|\mathrm{Out}(T)| \leqslant 20$, and thus (5.4.23) holds for $n \geqslant 4$. It is straightforward to check (5.4.21) when $T = \mathrm{U}_4(2)$, where we have $f(T)=20$.

Finally, assume $n=3$, so $|\mathrm{Out}(T)| \leqslant 6\log q$. Here (5.4.23) is satisfied for all $q>4$ since $(6\log q)^2 < 2q^3$. By our assumption, the only remaining cases are $T=\mathrm{U}_3(3)$ with $f(T)=14$ and $T=\mathrm{U}_3(4)$ with $f(T)=22$, so the inequality in (5.4.21) holds.

Case 3. $T = \mathrm{L}_n(q)$.

Here we may assume $(n,q) \neq (2,4),(2,5),(2,9),(3,2),(4,2)$ as noted in Remark 2.2.2. If $n=2$ and $q \in \{7,11\}$, then an easy computation using MAGMA shows that (5.4.20) holds, and the result follows.

In each of the remaining cases, we have $|T|/h(T) > q^{n-1}$ by inspecting Table 5.2. Moreover, [54, Corollary 1.2] implies that $f_p(\mathrm{Aut}(T)) < 100|T|/h(T)$, so (5.4.20) holds if

$$100|\mathrm{Out}(T)| < q^{n-1}. \tag{5.4.24}$$

Since $|\mathrm{Out}(T)| \leqslant 2(q-1)\log q < q^2$ for all q, (5.4.24) holds if $n \geqslant 10$. Moreover, if $n \geqslant 4$ then (5.4.24) holds if $q>100$, while for $q<100$ it is easy to check that (5.4.24) still holds in each case, unless $q=2$ and $n \leqslant 8$, or $n \in \{5,6\}$ and $q \leqslant 4$, or $n=4$ and $q \leqslant 9$. But in each of these cases, it is straightforward to check that (5.4.20) is satisfied, so to complete the proof we may assume $n \in \{2,3\}$.

Suppose $n=3$, so $|\mathrm{Out}(T)| \leqslant 6\log q$ and (5.4.24) holds if $600\log q < q^2$. The latter holds if $q>59$. In fact, by working with the precise value of $|\mathrm{Out}(T)|$ we see that (5.4.24) holds if $q>25$. Finally, if $q \leqslant 25$, then we can check (5.4.20) using MAGMA.

To complete the proof, we may assume $T=\mathrm{L}_2(q)$, so $|\mathrm{Out}(T)| \leqslant 2\log q$ and $|T|/h(T) \geqslant (q+1)q^{1/2}/2$. Thus, (5.4.20) holds if

$$800\log q < (q+1)^2$$

since we have $f_p(\mathrm{Aut}(T)) < 100q$ by [54, Corollary 1.2]. In this way, we deduce that (5.4.20) holds if $q \geqslant 71$. And for $q<71$, we can check that (5.4.20) holds with the aid of MAGMA. ■

Lemma 5.4.14. *We have*

$$r_3(G) < \binom{k}{2}\left(\frac{1}{|T|} + \frac{|\mathrm{Out}(T)|h(T)^{k-3}}{|T|^{k-3}}\right) + \frac{k!}{|T|^{\frac{4}{3}}} + |T|^{-\frac{1}{3}}\left(2\binom{k}{3} + \frac{1}{2}\binom{k}{2}\binom{k-2}{2}\right).$$

Proof. First, let

$$R_4(G) = \{(\alpha,\ldots,\alpha)\pi \in R_3(G) : \pi = (1,2)\},$$
$$R_4(T) = \{\alpha \in \mathrm{Aut}(T) : (\alpha,\ldots,\alpha)\pi \in R_4(G)\}$$

as in the proof of [51, Theorem 1.5]. Set $P = S_k$ and

$$r_4(G) := |(1,2)^P| \sum_{\alpha \in R_4(T)} \frac{|\alpha^{\mathrm{Aut}(T)}|}{|T|}\left(\frac{|C_{\mathrm{Inn}(T)}(\alpha)|}{|T|}\right)^{k-3}.$$

Then we have

$$\begin{aligned} r_4(G) &= \binom{k}{2}\left(\frac{1}{|T|} + \sum_{\alpha\in R_4(T)\setminus\{1\}} \frac{|\alpha^{\mathrm{Aut}(T)}|}{|T|}\left(\frac{|C_{\mathrm{Inn}(T)}(\alpha)|}{|T|}\right)^{k-3}\right) \\ &\leqslant \binom{k}{2}\left(\frac{1}{|T|} + |\mathrm{Out}(T)|\left(\frac{h(T)}{|T|}\right)^{k-3}\right). \end{aligned} \tag{5.4.25}$$

As noted in the proof of [51, Theorem 1.5], we have

$$r_3(G) \leqslant r_4(G) + \sum_{\pi\in R\setminus\{(1,2)\}} \frac{|\pi^P|}{|T|^{k-r_\pi-\frac{5}{3}}}, \tag{5.4.26}$$

where R is a set of representatives for the conjugacy classes of elements of prime order in P and r_π is the number of $\langle\pi\rangle$-orbits on $[k]$. Without loss of generality, we may assume $(1,2)\in R$.

Let $x,y\in R$ be representatives of the P-classes $(1,2,3)^P$ and $(1,2)(3,4)^P$, respectively. Note that $r_x = r_y = k-2$ and $r_z \leqslant k-3$ for all $z\in R\setminus\{(1,2),x,y\}$. Then

$$\begin{aligned} \sum_{\pi\in R\setminus\{(1,2)\}} \frac{|\pi^P|}{|T|^{k-r_\pi-\frac{5}{3}}} &= \sum_{\pi\in R\setminus\{(1,2),x,y\}} \frac{|\pi^P|}{|T|^{k-r_\pi-\frac{5}{3}}} + |T|^{-\frac{1}{3}}\left(2\binom{k}{3} + \frac{1}{2}\binom{k}{2}\binom{k-2}{2}\right) \\ &< \frac{k!}{|T|^{\frac{4}{3}}} + |T|^{-\frac{1}{3}}\left(2\binom{k}{3} + \frac{1}{2}\binom{k}{2}\binom{k-2}{2}\right) \end{aligned}$$

and so the lemma follows by combining (5.4.25) and (5.4.26). ■

Now we define

$$Q_1(G) := (k!)^2|T|^{\frac{8}{3}-\frac{k}{2}-\frac{1}{2}\delta_{5,k}} + \frac{k!}{|T|^{\frac{4}{3}}} + \frac{k^4}{2|T|^{\frac{1}{3}}}, \tag{5.4.27}$$

where $\delta_{5,k} = 1$ if $k=5$ and $\delta_{5,k} = 0$ otherwise, and

$$Q_2(G) := \left(\frac{|T|}{h(T)}\right)^{4-k} + \binom{k}{2}|\mathrm{Out}(T)|\left(\frac{|T|}{h(T)}\right)^{3-k}. \tag{5.4.28}$$

By Lemmas 5.4.12, 5.4.13 and 5.4.14, we have

$$r_1(G) + r_2(G) + r_3(G) < Q_1(G) + Q_2(G). \tag{5.4.29}$$

Lemma 5.4.15. *If $Q_1(G)+Q_2(G) < 1/2$ and $5 \leqslant k \leqslant 4\log|T|$, then $r(G)\geqslant 2$. In particular, $b(G)=2$.*

Proof. By (5.4.19) and (5.4.29), we have

$$\frac{1}{2} > Q_1(G)+Q_2(G) > 1 - \frac{r(G)|G|}{|T|^{2k-2}} = 1 - \frac{r(G)|\mathrm{Out}(T)|\cdot k!}{|T|^{k-2}}.$$

It suffices to prove that

$$2|\mathrm{Out}(T)|\cdot k! \leqslant |T|^{k-2},$$

which is clear since $k \leqslant 4\log|T|$. ■

5.5 Proof of Theorem 5.2

In this section, we will establish Theorem 5.2, which determines the base-two diagonal type primitive groups. The same method can be applied to establish Theorem 5.3 for base-two groups G, recalling that $\mathrm{reg}(G) = 1$ if and only if $\Sigma(G)$ is G-arc-transitive (see Lemma 3.1.2). Recall that $r(G)$ is the number of regular suborbits of G, which is positive if and only if $b(G) \leqslant 2$, and it coincides with $\mathrm{reg}(G)$ if $b(G) = 2$.

Theorem 5.5.1. *Let G be a diagonal type primitive group with socle T^k. Then $r(G) = 1$ if and only if $T = A_5$, $k \in \{3,57\}$ and $G = T^k.(\mathrm{Out}(T) \times S_k)$.*

We will consider the following cases in turn:

(a) $P \in \{A_k, S_k\}$ and $k \in \{3,4,|T|-4,|T|-3\}$;

(b) $P \in \{A_k, S_k\}$ and $k \in \{|T|-2,|T|-1\}$;

(c) $P = S_k$, $5 \leqslant k \leqslant |T|/2$ and $G = W$.

More specifically, we will prove that $r(G) \geqslant 2$ (so $b(G) = 2$) for every group in cases (a) and (c), with the exception of the two special cases arising in the statement of Theorem 5.5.1. Then Lemma 5.3.2 shows that $b(G) = 2$ if $P \in \{A_k, S_k\}$ and $3 \leqslant k \leqslant |T|-3$, as in part (ii) of Theorem 5.2, which also establishes Theorem 5.7. In particular, we deduce that $r(G) \geqslant 2$ if $P \notin \{A_k, S_k\}$ and $k \leqslant 32$, as noted in Remark 5.2.8.

As explained in Remark 2.2.2, we will exclude the possibilities for T listed in (2.2.1).

5.5.1 The groups with $k \in \{3,4,|T|-4,|T|-3\}$

We start with case (a).

Lemma 5.5.2. *Suppose $k \in \{3,4\}$, $P = S_k$ and T is a sporadic simple group. Then $r(G) \geqslant 2$.*

Proof. If $T \notin \{\mathrm{Ly}, \mathrm{Th}, \mathrm{J}_4, \mathbb{B}, \mathbb{M}\}$ then we can construct T as a permutation group in MAGMA using the function `AutomorphismGroupSimpleGroup`. Then the result follows by random search (see Remark 5.3.7(i)). If $T \in \{\mathrm{Ly}, \mathrm{Th}, \mathrm{J}_4, \mathbb{B}, \mathbb{M}\}$, then $|\mathrm{Out}(T)| = 1$. Let M be a maximal subgroup of T with

$$(T,M) \in \{(\mathrm{Ly}, G_2(5)),\ (\mathrm{Th}, \mathrm{AGL}_2(5)),\ (\mathrm{J}_4, \mathrm{M}_{22}.2),\ (\mathbb{B}, \mathrm{Fi}_{23}),\ (\mathbb{M}, \mathrm{L}_2(71))\}. \tag{5.5.1}$$

In view of Corollary 5.3.5, the result follows by random search (see Remark 5.3.7(ii)). ∎

We define the following set of finite simple groups of Lie type:

$$\begin{aligned}\mathscr{C} := \{&{}^2B_2(8), {}^2B_2(32), G_2(3), G_2(4), {}^2F_4(2)', {}^3D_4(2), F_4(2), \mathrm{L}_2(7), \mathrm{L}_2(8),\\ &\mathrm{L}_2(11), \mathrm{L}_2(13), \mathrm{L}_2(16), \mathrm{L}_2(27), \mathrm{L}_2(32), \mathrm{L}_3^{\varepsilon}(3), \mathrm{L}_3^{\varepsilon}(4), \mathrm{U}_3(5), \mathrm{U}_3(8), \mathrm{L}_4^{\varepsilon}(3),\\ &\mathrm{PSp}_4(3), \mathrm{Sp}_4(4), \mathrm{L}_5^{\varepsilon}(2), \mathrm{U}_6(2), \mathrm{Sp}_6(2), \mathrm{PSp}_6(3), \mathrm{Sp}_8(2), \Omega_8^{\varepsilon}(2), \mathrm{P}\Omega_8^{+}(3)\}.\end{aligned}$$

Recall that an element x of a simple group of Lie type T defined over a field of characteristic p is regular semisimple if and only if $|C_T(x)|$ is indivisible by p.

Lemma 5.5.3. *Suppose $T \notin \mathscr{C}$ is a finite simple group of Lie type. Then T has at least* 8 *regular semisimple* $\mathrm{Aut}(T)$*-classes.*

Proof. Suppose T is a Lie type group defined over $\mathbb{F}_q$, where $q = p^f$ for some prime p. We will work with a quasisimple group Q with $Q/Z(Q) = T$. Let m be the number of regular semisimple conjugacy classes in Q. Then T has at least $m|T|/|Q|$ regular semisimple T-classes, and thus T has at least 8 regular semisimple $\mathrm{Aut}(T)$-classes if

$$m|T| \geqslant 8|\mathrm{Out}(T)||Q|. \tag{5.5.2}$$

First assume Q is a simply connected quasisimple exceptional group. Then m has been computed by Lübeck [97], and one can see that (5.5.2) holds for every $T \notin \mathscr{C}$ by inspecting [97]. For example, if $T = E_7(q)$ with $p = 3$, then $|Q|/|T| = 2$, $|\mathrm{Out}(T)| = 2f$, and we get

$$m = q^7 + q^6 + 2q^5 + 7q^4 + 17q^3 + 35q^2 + 70q + 99$$

from [97], so (5.5.2) clearly holds.

Next, assume $Q \in \{\mathrm{SL}_n^{\varepsilon}(q), \mathrm{Sp}_n(q)\}$, so m is given in [53]. The result now follows by inspecting [53]. For example, if $Q = \mathrm{SL}_2(q)$ then $|Q|/|T| = (2, q-1)$, $|\mathrm{Out}(T)| = (2, q-1)f$ and

$$m = q - 3 + (2, q)$$

by [53, Theorem 2.4]. Thus, (5.5.2) is valid if

$$q - 3 + (2, q) \geqslant 8(2, q-1)^2 f,$$

which holds for all $q > 81$. For the cases where $q \leqslant 81$ and $T \notin \mathscr{C}$, one can check using MAGMA that there are at least 8 regular semisimple $\mathrm{Aut}(T)$-classes. We use an entirely similar argument to treat all the other cases and we omit the details.

To complete the proof, we assume $Q = \Omega_n^{\varepsilon}(q)$, so Q has index 2 in $\mathrm{SO}_n^{\varepsilon}(q)$. First assume q is even. Here $Q = T$ and every semisimple element in $\mathrm{SO}_n^{\varepsilon}(q)$ has odd order, and so lies in Q. This implies that m is at least the number of regular semisimple $\mathrm{SO}_n^{\varepsilon}(q)$-classes in $\mathrm{SO}_n^{\varepsilon}(q)$, which is computed in [53, Theorem 5.12], and the result follows by arguing as above.

Finally, assume $Q = \Omega_n^\varepsilon(q)$ and q is odd. Write $d = \lceil n/2\rceil - 1$. Let $A \in \mathrm{GL}_d(q)$ be of order $q^d - 1$ and let

$$x = \begin{pmatrix} A & & \\ & (A^{-1})^T & \\ & & I_{n-2d} \end{pmatrix}$$

with respect to a decomposition $V = (U_1 \oplus U_2) \perp W$, where U_i is a totally singular d-space and W is a non-degenerate space of type ε. Then $x \in \mathrm{SO}_n^\varepsilon(q)$, so $y := x^2 \in \Omega_n^\varepsilon(q)$, noting that

$$y = \begin{pmatrix} B & & \\ & (B^{-1})^T & \\ & & I_{n-2d} \end{pmatrix},$$

where $B = A^2$. Let μ be an eigenvalue of B of order $(q^d - 1)/2$ in the algebraic closure K of $\mathbb{F}_q$. Then it is easy to show that $\mu \neq \mu^{\pm q^t}$ for any $1 \leqslant t \leqslant d-1$, and the set of eigenvalues of y is

$$\{\mu, \mu^q, \ldots, \mu^{q^{d-1}}, \mu^{-1}, \mu^{-q}, \ldots, \mu^{-q^{d-1}}, 1\},$$

where 1 has multiplicity $n - 2d \in \{1,2\}$ and every other eigenvalue has multiplicity 1. It follows that y^i is regular semisimple if $(i, (q^d-1)/2) = 1$. This gives at least

$$\frac{\phi\big((q^d-1)/2\big)}{2d}$$

regular semisimple $\mathrm{GO}_n^\varepsilon(q)$-classes in Q, where ϕ is Euler's totient function (note that two semisimple elements in Q are not conjugate in $\mathrm{GL}_n(q)$ if they have distinct sets of eigenvalues in K). By arguing as above, T has at least 8 regular semisimple $\mathrm{Aut}(T)$-classes if

$$\phi\Big((q^d-1)/2\Big) \geqslant 32d \cdot |\mathrm{Aut}(T) : \mathrm{PGO}_n^\varepsilon(q)|, \tag{5.5.3}$$

noting that $|\mathrm{Aut}(T) : \mathrm{PGO}_n^\varepsilon(q)| \leqslant f \leqslant \log q$ if $d \neq 3$, while $|\mathrm{Aut}(T) : \mathrm{PGO}_n^\varepsilon(q)| \leqslant 3f \leqslant 3\log q$ if $d = 3$. It is easy to check that (5.5.3) holds unless

$$(d,q) \in \{(6,3),(5,3),(4,3),(4,5),(4,7),(3,3),(3,5),(3,7)\}.$$

For these remaining cases, one can use MAGMA to compute m and we find that (5.5.2) holds unless $Q \in \{\Omega_{10}^-(3), \Omega_8^+(5), \Omega_8^\varepsilon(3), \Omega_7(3)\}$. In the latter cases, we can directly check that there are at least 8 regular semisimple $\mathrm{Aut}(T)$-classes in T, with the aid of MAGMA. ■

We remark that there are exactly 8 regular semisimple $\mathrm{Aut}(T)$-classes in $T = \mathrm{P}\Omega_8^+(3)$. If $T \in \mathscr{C}$ and $T \neq \mathrm{P}\Omega_8^+(3)$, then one can check that there are at most 7 such classes. But it is convenient to include $\mathrm{P}\Omega_8^+(3)$ in $\mathscr{C}$ in view of Theorem 5.2.9, so that each $T \notin \mathscr{C}$ is invariably generated by a pair of regular semisimple elements of distinct orders.

Lemma 5.5.4. *Suppose $k = 3$, $P = S_k$ and $T \notin \mathscr{C}$ is a simple group of Lie type. Then $r(G) \geqslant 2$.*

Proof. Let x and y be as described in Theorem 5.2.9. Let z_1 and z_2 be semisimple elements in T lying in distinct $\mathrm{Aut}(T)$-classes such that

$$z_1, z_2 \notin x^{\mathrm{Aut}(T)} \cup (x^{-1})^{\mathrm{Aut}(T)} \cup y^{\mathrm{Aut}(T)} \cup (y^{-1})^{\mathrm{Aut}(T)}.$$

Note that the existence of z_1 and z_2 follows from Lemma 5.5.3. Then by applying [61, Theorem 2], which asserts that the product of any two regular semisimple T-classes contains all semisimple elements in T, there exist g_i and h_i in T such that $z_i = x^{g_i}y^{h_i}$, and without loss of generality we may assume $g_i = 1$, so $z_i = xy^{h_i}$.

It is easy to see that $\mathrm{Hol}(T, \{1, x^{-1}, y^{h_i}\}) = 1$, and so $b(G) = 2$. By Lemma 5.3.2, it suffices to show that $X_1 = \{1, x^{-1}, y^{h_1}\}$ and $X_2 = \{1, x^{-1}, y^{h_2}\}$ are in distinct $\mathrm{Hol}(T)$-orbits. Suppose $X_1^{g\alpha} = X_2$ for some $g\alpha \in \mathrm{Hol}(T)$, and note that $g \in X_1$ by Lemma 5.3.3. If $g = 1$ then $(x^{-1})^\alpha = x^{-1}$ and $(y^{h_1})^\alpha = y^{h_2}$. However, this implies that

$$z_1^\alpha = (xy^{h_1})^\alpha = xy^{h_2} = z_2,$$

which is incompatible with our assumption $z_1^{\mathrm{Aut}(T)} \neq z_2^{\mathrm{Aut}(T)}$. If $g = x^{-1}$ then $(y^{h_1})^g = xy^{h_1} = z_1$, which is not $\mathrm{Aut}(T)$-conjugate to any element in X_2, a contradiction. Similarly, if $g = y^{h_1}$ then $(x^{-1})^g = y^{-h_1}x^{-1} = z_1^{-1}$ and once again, this is impossible. Therefore, there is no $g\alpha \in \mathrm{Hol}(T)$ such that $X_1^{g\alpha} = X_2$, which completes the proof. ■

Lemma 5.5.5. *Suppose $k = 4$, $P = S_k$ and $T \notin \mathscr{C}$ is a simple group of Lie type. Then $r(G) \geqslant 2$.*

Proof. Let x and y be as in Theorem 5.2.9. By [61, Theorem 2], every semisimple element in T lies in $x^T y^T$, so we may assume that

$$x^{-1}y \notin x^{\mathrm{Aut}(T)} \cup (x^{-1})^{\mathrm{Aut}(T)} \cup y^{\mathrm{Aut}(T)} \cup (y^{-1})^{\mathrm{Aut}(T)}. \tag{5.5.4}$$

Additionally, using Lemma 5.5.3, we can choose a regular semisimple element $z_0 \in T$ such that

$$z_0 \notin x^{\mathrm{Aut}(T)} \cup (x^{-1})^{\mathrm{Aut}(T)} \cup y^{\mathrm{Aut}(T)} \cup (y^{-1})^{\mathrm{Aut}(T)} \cup (x^{-1}y)^{\mathrm{Aut}(T)} \cup (y^{-1}x)^{\mathrm{Aut}(T)}. \tag{5.5.5}$$

Again, [61, Theorem 2] implies that $x^T z_0^T$ contains all semisimple elements in T. Thus, by Lemma 5.5.3, there exists $z \in z_0^T$ such that

$$z^{-1}x \notin x^{\mathrm{Aut}(T)} \cup (x^{-1})^{\mathrm{Aut}(T)} \cup y^{\mathrm{Aut}(T)} \cup (y^{-1})^{\mathrm{Aut}(T)} \cup (x^{-1}y)^{\mathrm{Aut}(T)} \cup (y^{-1}x)^{\mathrm{Aut}(T)}. \tag{5.5.6}$$

Set $X_1 = \{1, x, y, z\}$ and suppose $g\alpha \in \mathrm{Hol}(T, X_1)$. If $g = 1$ then $\alpha \in \mathrm{Aut}(T, X_1) = 1$ as $\langle x, y\rangle = T$ and x, y, z are in distinct $\mathrm{Aut}(T)$-classes. If $g = x$ then $x^{-1}y \in x^{-1}X_1 = X_1^{\alpha^{-1}}$, which is incompatible with either (5.5.4) or (5.5.5). The case where $g = y$ can be eliminated using the same argument. If $g = z$, then $z^{-1}X_1 = X_1^{\alpha^{-1}}$ and by appealing to (5.5.5) and (5.5.6), we see that both z^{-1} and $z^{-1}x$ are $\mathrm{Aut}(T)$-conjugate to z. But this implies that $z^{-1} = z^\alpha = z^{-1}x$, a contradiction. Thus, we have $b(G) = 2$.

Similarly, Lemma 5.5.3 implies that there exists a regular semisimple element $w \in T$ such that $w \neq z$,

$$w \notin x^{\mathrm{Aut}(T)} \cup (x^{-1})^{\mathrm{Aut}(T)} \cup y^{\mathrm{Aut}(T)} \cup (y^{-1})^{\mathrm{Aut}(T)} \cup (x^{-1}y)^{\mathrm{Aut}(T)} \cup (y^{-1}x)^{\mathrm{Aut}(T)}$$

and

$$w^{-1}x \notin x^{\mathrm{Aut}(T)} \cup (x^{-1})^{\mathrm{Aut}(T)} \cup y^{\mathrm{Aut}(T)} \cup (y^{-1})^{\mathrm{Aut}(T)} \cup (x^{-1}y)^{\mathrm{Aut}(T)} \cup (y^{-1}x)^{\mathrm{Aut}(T)}.$$

Set $X_2 = \{1,x,y,w\}$. By arguing as above, we have $\mathrm{Hol}(T,X_2) = 1$ and it suffices to show that X_1 and X_2 are in distinct $\mathrm{Hol}(T)$-orbits. Suppose $X_1^{g\alpha} = X_2$ and note that $g \in X_1$ by Lemma 5.3.3. If $g = 1$ then $x^\alpha = x$ and $y^\alpha = y$, which implies that $\alpha = 1$. However, this is incompatible with $z \neq w$. If $g = x$ then

$$1^g = x^{-1},\ y^g = x^{-1}y \text{ and } z^g = x^{-1}z.$$

So one of these elements is $\mathrm{Aut}(T)$-conjugate to w, which has to be $z^g = x^{-1}z$ by our assumption. However, this gives a contradiction since $y^g = x^{-1}y$ is not $\mathrm{Aut}(T)$-conjugate to x or y by (5.5.4). The case $g = y$ can be eliminated similarly. Finally, if $g = z$ then

$$x^g = z^{-1}x,\ y^g = z^{-1}y \text{ and } 1^g = z^{-1}.$$

Once again, the only possibility is $x^{g\alpha} = w$ by (5.5.6), but this gives $(z^{-1})^\alpha = 1^{g\alpha} \in \{x,y\}$, which is incompatible with (5.5.5). ■

We can now establish Theorems 5.2 and 5.5.1 for $k \in \{3,4,|T|-4,|T|-3\}$.

Proposition 5.5.6. *If $k \in \{3,4,|T|-4,|T|-3\}$ then $r(G) \geqslant 1$, with equality if and only if $T = A_5$, $k \in \{3,57\}$ and $G = T^k.(\mathrm{Out}(T) \times S_k)$.*

Proof. By Proposition 5.2.7, we may assume $P \in \{A_k, S_k\}$. First assume $k \in \{3,4\}$ and $P = S_k$. The groups where T is sporadic have been treated in Lemma 5.5.2. If $T \notin \mathscr{C}$ is Lie type, then Lemmas 5.5.4 and 5.5.5 imply that $r(G) \geqslant 2$, as desired. The cases where $T \in \mathscr{C}$ can be handled computationally, using random search (see Remark 5.3.7(i)).

Thus, to complete the proof for $k \in \{3,4\}$ and $P = S_k$ we may assume $T = A_n$ is an alternating group. First assume $k = 3$ and $T = A_5$. One can check using MAGMA that $\mathrm{Hol}(T)$ has a unique regular orbit on $\mathscr{P}_k$, so $r(G) = 1$ if $G = W = A_5^3.(2 \times S_3)$. In addition, we find that $r(G) \geqslant 2$ if $G < W$. For the latter, we construct G as a permutation group of degree $|\Omega| = |A_5|^2 = 3600$ via the primitive groups database in MAGMA.

Next, assume $P = S_3$ and $T = A_n$ with $n \geqslant 6$. The groups with $n \leqslant 8$ can be easily handled using MAGMA (see Remark 5.3.7(i)). Now assume $n \geqslant 9$, so by a classical theorem of Miller [102], there exist $x_1, y_1 \in T$ such that $|x_1| = 2$, $|y_1| = 3$ and $\langle x_1, y_1 \rangle = T$. Note that if $|x_1y_1| = 2$ or 3, then $\langle x_1, y_1 \rangle = S_3$ or A_4 respectively, so we must have $|x_1y_1| \geqslant 4$. Hence, $\mathrm{Hol}(T,\{1,x_1,y_1\}) = 1$ by Lemma 5.3.4, and thus $b(G) = 2$. Let $x_2 = (1,2,\dots,n)$ if n is odd, while $x_2 = (1,2)(3,\dots,n)$ if n is even, and let $y_2 = (1,2,3)x_2^{-1}$. Then $\langle x_2,y_2\rangle = T$ and Lemma 5.3.4 implies that $\mathrm{Hol}(T,\{1,x_2,y_2\}) = 1$, so we have $r(G) \geqslant 2$ by Lemma 5.3.6.

Now assume $P = S_4$ and $T = A_n$. The cases where $n \leqslant 11$ can be handled using MAGMA, as noted in Remark 5.3.7(i). Assume $n \geqslant 12$ and let $x = (1,2)(3,4)$. Let $t_1,t_2 \in T$ be of cycle type $[2^4,1^{n-8}]$ and $[2^6,1^{n-12}]$, respectively, and let $C_i = t_i^T$. Note that there exist $y_1 \in C_1$ and $y_2 \in C_2$ such that $xy_i \neq y_ix$. Moreover, by [13, Theorem 1.2], there exist z_1 and z_2 such that

$$T = \langle x,z_1\rangle = \langle y_1,z_1\rangle = \langle x,z_2\rangle = \langle y_2,z_2\rangle.$$

In particular, $2 \notin \{|z_i|,|xz_i|,|y_iz_i|\}$. Set $X_1 = \{1,x,y_1,z_1\}$ and $X_2 = \{1,x,y_2,z_2\}$. We first prove that $\mathrm{Hol}(T,X_i) = 1$. Suppose $g\alpha \in \mathrm{Hol}(T,X_i)$. If $g = 1$ then $\alpha \in \mathrm{Aut}(T,X_i) = 1$ since $\langle x,z_i\rangle = T$ and x,y_i,z_i are in distinct $\mathrm{Aut}(T)$-classes. If $g = x$ then $2 \notin \{|y_i^g|,|z_i^g|\} = \{|xy_i|,|xz_i|\}$, which is impossible. The cases where $g \in \{y_i,z_i\}$ can be eliminated similarly. This implies that $b(G) = 2$. And by applying Lemma 5.3.3, one can show that X_1 and X_2 are in distinct $\mathrm{Hol}(T)$-orbits.

Therefore, we have $r(G) \geqslant 1$ if $k \in \{3,4\}$, with equality if and only if $G = A_5^3.(2\times S_3)$. By Lemma 5.3.2, it suffices to consider the case where $T = A_5$ and $k = |A_5|-3 = 57$. Here $r(G) = 1$ if $G = W = A_5^{57}.(2\times S_{57})$, and G has at least $|W:G|$ regular suborbits if $G < W$. The result follows. ■

5.5.2 The groups with $P \in \{A_k,S_k\}$ and $k \in \{|T|-2,|T|-1\}$

Lemma 5.5.7. *Suppose $m \in \{2,3\}$. Then there exist $X_1,X_2 \subseteq T^\#$ such that $|X_i| = m$, $\mathrm{Aut}(T,X_i) = 1$ and $X_1^{\mathrm{Aut}(T)} \neq X_2^{\mathrm{Aut}(T)}$.*

Proof. First observe that if $X_1 \cup \{1\}$ and $X_2 \cup \{1\}$ are in distinct regular $\mathrm{Hol}(T)$-orbits, then all conditions in the statement of the lemma are satisfied. Hence, the result follows from Lemma 5.3.2 and Proposition 5.5.6, except when $T = A_5$ and $m = 2$. In the latter case, we can verify the lemma using MAGMA. ■

Proposition 5.5.8. *Assume $k = |T|-1$ or $|T|-2$.*

(i) If G contains S_k, then $b(G) = 3$.

(ii) If G does not contain S_k, then $r(G) \geqslant 2$.

Proof. Recall that $b(G) \in \{2,3\}$ by Theorem 5.2.3(iii). First assume G contains S_k. It suffices to show that $b(G) = 3$ if $G = T^k{:}S_k$. Suppose $\{D,D(\varphi_{t_1},\ldots,\varphi_{t_k})\}$ is a base for G. If $t_i = t_j$ for some $i \neq j$, then $(i,j) \in G$ stabilises D and $D(\varphi_{t_1},\ldots,\varphi_{t_k})$ pointwise. Therefore, $t_1,\ldots,t_k$ are distinct. Let $S = T \setminus \{t_1,\ldots,t_k\}$, so $|S| \in \{1,2\}$. Without loss of generality, we may also assume $1 \in S$. Thus, there exists $1 \neq t \in T$ such that $S^{\varphi_t} = S$, and hence $\varphi_t \in \mathrm{Hol}(T,T\setminus S)$, which is incompatible with Lemma 5.3.1.

Now we turn to the case where G does not contain S_k. Recall that $T^k{:}A_k \leqslant G$ by Corollary 5.2.6. From Lemma 5.5.7, there are subsets $X_1, X_2 \subseteq T^\#$ of size $|T|-k+1$ lying in distinct regular $\mathrm{Aut}(T)$-orbits. Write $T^\# \setminus X_i = \{t_{i,1},\dots,t_{i,k-2}\}$ and consider $\Delta_i = \{D, D(\varphi_{t_{i,1}},\dots,\varphi_{t_{i,k}})\}$, where $t_{i,k-1} = t_{i,k} = 1$. Suppose $x = (\alpha,\dots,\alpha)\pi \in G_{(\Delta_i)}$. By Lemma 5.2.1, $t_{i,j}^\alpha = t_{i,j^\pi}$ for all j. It follows that $\alpha \in \mathrm{Aut}(T, X_i)$ and thus $\alpha = 1$. Hence, $x = \pi \in \langle (k-1,k)\rangle$, and so $x = 1$ since G does not contain S_k. This shows that $b(G) = 2$. Finally, if Δ_1 and Δ_2 are in the same G_D-orbit, then

$$D(\varphi_{t_{1,1}},\dots,\varphi_{t_{1,k}})^{(\alpha,\dots,\alpha)\pi} = D(\varphi_{t_{2,1}},\dots,\varphi_{t_{2,k}})$$

for some $\alpha \in \mathrm{Aut}(T)$ and $\pi \in S_k$. This implies that $X_1^\alpha = X_2$, which is incompatible with our assumption. Therefore, $r(G) \geqslant 2$ and the proof is complete. ■

The following lemma will be useful in the proof of Theorem 5.3. Recall that G is called *semi-Frobenius* if the generalised Saxl graph $\Sigma(G)$ is complete (equivalently, any two points in Ω can be extended to a base for G of size $b(G)$). In view of Lemma 3.3.8, if G is semi-Frobenius and G is not 2-transitive, then $\Sigma(G)$ is not G-arc-transitive and so $\mathrm{reg}(G) > 1$ by Lemma 3.2.5.

Lemma 5.5.9. *If $k = |T|-1$ or $|T|-2$ and G contains S_k, then G is semi-Frobenius. In particular, $\Sigma(G)$ is not G-arc-transitive, and* $\mathrm{reg}(G) > 1$.

Proof. By Proposition 5.5.8(i), we see that $b(G) = 3$. Let $\mathbf{x} = (\varphi_{t_1},\dots,\varphi_{t_k}) \in \mathrm{Inn}(T)^k$ be such that $D \neq D\mathbf{x}$. Then there exist $i,j \in [k]$ such that $t_i \neq t_j$, and so $(i,j) \notin G_D \cap G_{D\mathbf{x}}$. Without loss of generality, we may assume $\{i,j\} = \{k-1,k\}$, and let Δ_1 be as in the proof of Proposition 5.5.8. By arguing as in the proof of Proposition 5.5.8, we have $G_{(\Delta_1)} \leqslant \langle (k-1,k)\rangle$, and thus $\Delta_1 \cup \{D\mathbf{x}\}$ is a base for G. It follows that D and $D\mathbf{x}$ are adjacent in $\Sigma(G)$, and we conclude the proof. ■

5.5.3 The groups with $P = S_k$, $5 \leqslant k \leqslant |T|/2$ and $G = W$

Finally, let us turn to case (c) defined at the beginning of Section 5.5. Note that if $r(G) \geqslant 2$ in every case, then the proofs of Theorems 5.2 and 5.5.1 are complete by combining Corollary 5.2.4 with Propositions 5.2.7, 5.5.6 and 5.5.8. By Proposition 5.4.7, it suffices to consider the cases where $5 \leqslant k \leqslant 4\log|T|$. Recall that $r(G) \geqslant 2$ if (5.4.8) holds or $Q_1(G) + Q_2(G) < 1/2$ (see Lemmas 5.4.8 and 5.4.15).

Proposition 5.5.10. *The conclusions to Theorems 5.2 and 5.5.1 hold when T is a sporadic simple group.*

Proof. As noted above, we may assume $5 \leqslant k \leqslant 4\log|T|$. With the aid of MAGMA, it is easy to check that (5.4.8) holds for all k in this range unless T is one of the following groups:

$$\mathrm{Suz},\ \mathrm{Co}_1,\ \mathrm{Co}_2,\ \mathrm{Fi}_{22},\ \mathrm{Fi}_{23},\ \mathrm{Fi}_{24}',\ \mathbb{B},\ \mathbb{M}.$$

Assume $T \in \{\mathrm{Suz}, \mathrm{Co}_1, \mathrm{Co}_2, \mathrm{Fi}_{22}, \mathrm{Fi}_{23}, \mathrm{Fi}_{24}'\}$. Here we can construct T as a permutation group in MAGMA using the function `AutomorphismGroupSimpleGroup`, and we can then check that (5.4.8) holds for $9 \leqslant k \leqslant 4\log|T|$. The cases where $5 \leqslant k \leqslant 8$ can also be handled using MAGMA (see Remark 5.3.7(i)).

Finally, if $T \in \{\mathbb{B}, \mathbb{M}\}$ then (5.4.8) holds unless $k = 5$ or $(T,k) = (\mathbb{B}, 6)$. In each case, we can verify that $r(G) \geqslant 2$ by random search as described in Remark 5.3.7(ii), with the same centreless maximal subgroup M of T defined in (5.5.1). ■

Proposition 5.5.11. *The conclusions to Theorems 5.2 and 5.5.1 hold when $T = A_n$ is an alternating group.*

Proof. Once again, we may assume $5 \leqslant k \leqslant 4\log|T|$. The cases where $n \in \{5,6\}$ can be easily handled using MAGMA, so we also assume $n \geqslant 7$. First assume $n \leqslant k \leqslant 4\log|T|$. With the aid of MAGMA, it is easy to check (5.4.8) holds for all $7 \leqslant n \leqslant 29$. Note that $h(T) = (n-2)!$ and thus (5.4.18) holds. By Lemma 5.4.11, it suffices to establish the inequality in (5.4.17) for $k_0 = n$. Thus, we only need to show that

$$\left(\frac{n(n-1)}{2e}\right)^n > \frac{n(n!)^2}{2},$$

which holds for all $n \geqslant 30$.

Finally, let us assume $5 \leqslant k < n$ and define $Q_1(G)$ and $Q_2(G)$ as in (5.4.27) and (5.4.28), respectively. Then

$$Q_1(G) = (k!)^2|T|^{\frac{8}{3}-\frac{k}{2}-\frac{1}{2}\delta_{5,k}} + \frac{k!}{|T|^{\frac{4}{3}}} + \frac{k^4}{2|T|^{\frac{1}{3}}} < (6!)^2\left(\frac{2}{n!}\right)^{\frac{1}{3}} + \frac{2^{\frac{4}{3}}}{(n!)^{\frac{1}{3}}} + \frac{2^{\frac{1}{3}}n^4}{2(n!)^{\frac{1}{3}}}$$

and

$$Q_2(G) = \left(\frac{|T|}{h(T)}\right)^{4-k} + \binom{k}{2}|\mathrm{Out}(T)|\left(\frac{|T|}{h(T)}\right)^{3-k} < \frac{2}{n(n-1)} + 20\left(\frac{2}{n(n-1)}\right)^2.$$

Given these bounds, it is easy to check that $Q_1(G) + Q_2(G) < 1/2$ for all $n \geqslant 21$. Finally, for the cases where $7 \leqslant n \leqslant 20$ and $5 \leqslant k < n$, one can use MAGMA to check that either (5.4.8) holds, or $Q_1(G) + Q_2(G) < 1/2$, or $\mathrm{Hol}(T)$ has at least 2 regular orbits on $\mathscr{P}_k$ (for the latter, we use the random search approach described in Remark 5.3.7(i)). ■

To complete the proofs of Theorems 5.2 and 5.5.1, we may assume T is a finite simple group of Lie type. First we consider some low rank groups, where $h(T)$ is small and Lemma 5.4.10 can be applied.

Lemma 5.5.12. *Suppose $T = \mathrm{L}_2(q)$ and $5 \leqslant k \leqslant 4\log|T|$. Then $r(G) \geqslant 2$.*

Proof. If $q < 16$ then one can check the result using MAGMA. More precisely, we construct $\mathrm{Hol}(T)$ as a permutation group on T via the function `Holomorph` and we use random search to find two

k-subsets X_1 and X_2 of T lying in distinct regular $\mathrm{Hol}(T)$-orbits (this is a viable approach since $|T|$ is small; see the function `RanHol` in Appendix A.1.3).

Thus, we may assume $q \geqslant 16$. First assume $k \geqslant 6$ and set $k_0 = 6$. For $q \leqslant 733$, one can check (5.4.8) using MAGMA. Assume $q > 733$ and note that $h(T) \leqslant q^{1/2}(q-1)$ by Theorem 5.2.10, so (5.4.14) holds. Moreover, as $|\mathrm{Out}(T)| \leqslant 2\log q$, we can check that (5.4.13) holds if

$$q^2(q^2-1)^2 > 16(\log q)^2 6^8 e^{18},$$

which holds true for all $q > 733$. Now apply Lemma 5.4.10, noting that $|T| > 4080$.

To complete the proof, we assume $k = 5$. By Lemma 5.4.9, $r(G) \geqslant 2$ if (5.4.11) holds for every $u \in \{0,1,2\}$. If $u = 2$, then (5.4.11) holds if

$$q^{1/2}(q+1) > 5^4 e^7 \log q,$$

which is easily checked for all $q > 48449$. With the same method, one can verify that (5.4.11) holds for $u \in \{0,1\}$ if $q > 48449$. With the aid of MAGMA, we see that (5.4.8) holds for all $16 \leqslant q \leqslant 48449$, unless $q \in \{16, 25, 49, 81\}$, and the remaining cases can be handled using MAGMA and random search, utilising the method in Remark 5.3.7(i). ■

Lemma 5.5.13. *Suppose $T \in \{\mathrm{L}_3^{\varepsilon}(q), {}^2B_2(q), {}^2G_2(q)\}$ and $5 \leqslant k \leqslant 4\log|T|$. Then $r(G) \geqslant 2$.*

Proof. Note that $|T| > 4080$ and $h(T)^2 < 5|T|$ by Theorem 5.2.10. Thus, in view of Lemma 5.4.10, we only need to prove (5.4.13) for $k_0 = 5$.

Assume $T = \mathrm{L}_3^{\varepsilon}(q)$, so $|T| \geqslant q^3(q^2-1)(q^3-1)/3$ and $|\mathrm{Out}(T)| \leqslant 6\log q$. Thus, (5.4.13) holds if

$$q^3(q^2-1)(q^3-1) > 3(6\log q)^2 5^7 e^{15},$$

which is true for all $q > 73$. By applying the precise values of $h(T)$ and $|\mathrm{Out}(T)|$, we see that (5.4.8) holds unless $\varepsilon = -$, $k = 5$ and $q \in \{3,5,8\}$, or $\varepsilon = +$ and

$$(q,k) \in \{(3,5),(3,6),(4,5),(13,5)\},$$

all of which cases can be easily handled computationally, as described in Remark 5.3.7(i). We can apply the same method to the cases where $T = {}^2B_2(q)$ or ${}^2G_2(q)$, noting that (5.4.13) holds if $T \neq {}^2G_2(27)$, ${}^2B_2(8)$, ${}^2B_2(32)$ or ${}^2B_2(128)$ (we are excluding the group ${}^2G_2(3)'$, as noted in (2.2.1)). In the remaining four cases, one can check (5.4.8) directly. ■

Proposition 5.5.14. *The conclusions to Theorems 5.2 and 5.5.1 hold when T is an exceptional group of Lie type.*

Proof. Once again, by the previous results, we may assume $5 \leqslant k \leqslant 4\log|T|$. In view of Lemma 5.5.13, we may also assume $T \neq {}^2B_2(q)$ or ${}^2G_2(q)$. Note that

$$\frac{|T|}{h(T)} > 10|\mathrm{Out}(T)| \geqslant 10$$

and $|T| > \frac{1}{6}q^d$, where d is defined in Lemma 2.2.4.

First assume $5 \leqslant k \leqslant 8$. Then

$$Q_2(G) < \frac{h(T)}{|T|} + 10|\mathrm{Out}(T)| \cdot \frac{h(T)^2}{|T|^2} < \frac{1}{10} + \frac{1}{10} = \frac{1}{5}$$

and

$$Q_1(G) < \frac{(6!)^2}{|T|^{\frac{1}{3}}} + \frac{8!}{|T|^{\frac{4}{3}}} + \frac{8^4}{2|T|^{\frac{1}{3}}} < \frac{6^{\frac{1}{3}}(6!)^2}{q^{\frac{d}{3}}} + \frac{6^{\frac{4}{3}} \cdot 8!}{q^{\frac{4d}{3}}} + \frac{6^{\frac{1}{3}}8^4}{2q^{\frac{d}{3}}} < \frac{3}{10}$$

unless $T \in \{{}^2F_4(2)', {}^3D_4(2), {}^3D_4(3), {}^3D_4(4), F_4(2)\}$ or $T = G_2(q)$ for $q \leqslant 23$. In these cases, one can check (5.4.8) with the aid of MAGMA unless $T = {}^3D_4(q)$ and $k = 5$, or $T = F_4(2)$ and $k \in \{5,6\}$. We can resolve the latter cases by random search, explained as in Remark 5.3.7(i).

To complete the proof, we assume $9 \leqslant k \leqslant 4\log|T|$. The groups with $q = 2$ can be handled by verifying (5.4.8) directly, so we now assume $q \geqslant 3$. We first prove (5.4.17) for $k_0 = 9$. By inspecting Table 5.2, we have

$$2^9\left(\frac{|T|}{h(T)}\right)^9 > |T|^2 q^{22}. \tag{5.5.7}$$

For example, if $T = E_8(q)$, then

$$\frac{|T|}{h(T)} = \frac{(q^{30}-1)(q^{24}-1)(q^{20}-1)}{(q^{10}-1)(q^6-1)} > \frac{1}{2}q^{58}$$

and $|T| < q^{248}$ by Lemma 2.2.4, which implies (5.5.7). Since $|\mathrm{Out}(T)| \leqslant 6\log q$, it follows that (5.4.17) holds for $k_0 = 9$ if

$$q^{22} > 48\log q \cdot (2e)^9$$

and one can check that this inequality holds for $q \geqslant 3$.

By Lemma 5.4.11, it suffices to prove (5.4.18). Here we only give a proof for the case where $T = G_2(q)$, as all the other cases are very similar. First note that $|T| = q^6(q^6-1)(q^2-1) < q^{14}$ and $h(T) = q^6(q^2-1) > \frac{1}{2}q^8$. Then (5.4.18) holds if

$$q^2 > 56^2(\log q)^2 e,$$

which holds true for all $q > 907$. One can also check that (5.4.18) holds for all $601 < q \leqslant 907$. If $q \leqslant 601$, then we can use the precise values of $|T|$, $h(T)$ and $|\mathrm{Out}(T)|$ to check (5.4.8) for all $9 \leqslant k \leqslant 4\log|T|$. This completes the proof. ■

Lemma 5.5.15. *Suppose $T = \mathrm{L}_4^{\varepsilon}(q)$ and $5 \leqslant k \leqslant 4\log|T|$. Then $r(G) \geqslant 2$.*

Proof. Recall that $h(T) = (2, q-\varepsilon)|\mathrm{PGSp}_4(q)|/(4, q-\varepsilon)$ by Theorem 5.2.10. First assume that $k \geqslant 7$ and set $k_0 = 7$. For $q \leqslant 89$, one can check (5.4.8) with the aid of MAGMA. Now assume $q > 89$. It is easy to see that

$$q^5 > \max\{48(4e)^7\log q, 4e \cdot 60^2(\log q)^2\},$$

which implies the inequalities in (5.4.17) and (5.4.18).

Now assume $k \in \{5,6\}$. Note that $|T|/h(T) > 10|\mathrm{Out}(T)| \geqslant 10$, so $Q_2(G) < \frac{1}{5}$. Moreover,

$$Q_1(G) < \frac{(6!)^2}{|T|^{\frac{1}{3}}} + \frac{6!}{|T|^{\frac{4}{3}}} + \frac{6^4}{2|T|^{\frac{1}{3}}},$$

so we have $Q_1(G) < \frac{3}{10}$ if $q \geqslant 19$ and thus $Q_1(G)+Q_2(G) < 1/2$. Finally if $q \leqslant 17$ then we can use MAGMA (via random search as in Remark 5.3.7(i)) to check that $r(G) \geqslant 2$. ■

Lemma 5.5.16. *Suppose $T = \mathrm{PSp}_4(q)$ and $5 \leqslant k \leqslant 4\log|T|$. Then $r(G) \geqslant 2$.*

Proof. As noted in (2.2.1), we assume $q \geqslant 3$. First assume $k \geqslant 6$. It can be checked using MAGMA that (5.4.8) holds for $q \leqslant 607$, unless $(k,q) = (6,3)$, in which case we can verify the result using MAGMA and random search as in Remark 5.3.7(i). Now assume $q > 607$. By applying the bounds $|T| < q^{10}$, $h(T) > \frac{1}{2}q^6$ and $\frac{1}{2}q^4 < |T|/h(T) < 2q^4$, we see that (5.4.17) holds for $k_0 = 6$ if

$$q^4 > 6(2e)^6 \log q,$$

while (5.4.18) holds if

$$q^2 > 40^2(\log q)^2 e.$$

It is easy to check that both inequalities hold for all $q > 607$.

Finally, assume $k = 5$. Once again, we have $|T|/h(T) > 10|\mathrm{Out}(T)| \geqslant 10$ and thus $Q_2(G) < \frac{1}{5}$. Additionally,

$$Q_1(G) = \frac{(5!)^2}{|T|^{\frac{1}{3}}} + \frac{5!}{|T|^{\frac{4}{3}}} + \frac{5^4}{2|T|^{\frac{1}{3}}} < \frac{3}{10}$$

for all $q \geqslant 27$. The remaining groups with $q \leqslant 25$ can be handled with the aid of MAGMA via random search (see Remark 5.3.7(i)). ■

Proposition 5.5.17. *The conclusions to Theorems 5.2 and 5.5.1 hold when T is a classical group.*

Proof. Let T be a classical group over $\mathbb{F}_q$ and let n be the dimension of the natural module. Note that $|T| > \frac{1}{8}q^{n(n-1)/2}$ by Lemma 2.2.4. As explained above, we may assume $5 \leqslant k \leqslant 4\log|T|$. In addition, we may also assume $n \geqslant 5$ by Lemmas 5.5.12, 5.5.13, 5.5.15 and 5.5.16. Then

$$\frac{|T|}{h(T)} > 10|\mathrm{Out}(T)| \geqslant 10$$

by inspecting Table 5.2, and thus

$$Q_2(G) < \frac{h(T)}{|T|} + 10|\mathrm{Out}(T)| \cdot \frac{h(T)^2}{|T|^2} < \frac{1}{10} + \frac{1}{10} = \frac{1}{5}.$$

First assume $5 \leqslant k \leqslant n+3$. Then

$$Q_1(G) < \frac{(6!)^2}{|T|^{\frac{1}{3}}} + \frac{(n+3)!}{|T|^{\frac{4}{3}}} + \frac{(n+3)^4}{2|T|^{\frac{1}{3}}} < \frac{8^{\frac{1}{3}}(6!)^2}{q^{\frac{n(n-1)}{6}}} + \frac{8^{\frac{4}{3}}(n+3)!}{q^{\frac{2n(n-1)}{3}}} + \frac{8^{\frac{1}{3}}(n+3)^4}{2q^{\frac{n(n-1)}{6}}} =: Q(n,q).$$

Evidently, $Q(n,q)$ is a decreasing function of q. In addition, if q is fixed, then each summand is a decreasing function of n. Thus, $Q(n,q)$ is also decreasing with n. Note that $Q(n,q) < \frac{3}{10}$ if

$$(n,q) \in \{(12,2),(10,3),(9,4),(8,7),(7,9),(6,23),(5,97)\} =: \mathscr{B}.$$

Hence, we only need to consider the cases where $n < n_0$ or $q < q_0$ for some $(n_0,q_0) \in \mathscr{B}$. For these groups, we can show that $r(G) \geqslant 2$ either by checking $Q_1(G)+Q_2(G) < 1/2$ or (5.4.8), or by random search as explained in Remark 5.3.7(i). This shows that $r(G) \geqslant 2$ if $5 \leqslant k \leqslant n+3$.

To complete the proof, assume $n+4 \leqslant k \leqslant 4\log|T|$ and let $k_0 = n+4$. We first consider the case where $T = \mathrm{L}_n^{\varepsilon}(q)$. Note that $|T| < q^{n^2-1}$ and

$$\frac{|T|}{h(T)} \geqslant \frac{|\mathrm{PGL}_n^{\varepsilon}(q)|}{|\mathrm{GU}_{n-1}(q)|} > \frac{1}{2}q^{2n-2}$$

by Lemma 2.2.4 and Theorem 5.2.10. Hence, (5.4.17) holds if

$$q^{6n-8} > 2(n+4)(2e)^{n+4}$$

since $|\mathrm{Out}(T)| \leqslant 2(q+1)\log q < 2q^2$. This inequality holds if $q \geqslant 3$ or $n \geqslant 7$, while we can check (5.4.17) directly when $(n,q) = (5,2)$ or $(6,2)$. Thus, we have (5.4.17) for all $n \geqslant 5$ and $q \geqslant 2$. By Lemma 5.4.11, it suffices to prove (5.4.18). To do this, first note that

$$h(T) \geqslant q^{2n-3}|\mathrm{PGL}_{n-2}^{\varepsilon}(q)| > \frac{1}{2}q^{2n-3}q^{(n-2)^2-1} = \frac{1}{2}q^{n^2-2n}$$

by Lemma 2.2.4 and Theorem 5.2.10, so (5.4.18) holds if

$$q^{n^2-4n-1} > 32e(n^2-1)^2$$

since $\log q < q$. One can easily check that the above inequality holds for all $n \geqslant 5$ and $q \geqslant 2$, unless $n = 5$ and $q \leqslant 13$, or $(n,q) = (6,2)$, in which cases we can verify (5.4.18) directly. This completes the proof for linear and unitary groups.

Next assume $T = \mathrm{PSp}_n(q)$ with $n \geqslant 6$. Here $|T| < q^{n(n+1)/2}$ by Lemma 2.2.4 and

$$\frac{|T|}{h(T)} = \frac{q^n-1}{(2,q-1)} > q^{n-1}.$$

Since $|\mathrm{Out}(T)| \leqslant 2\log q$, we see that (5.4.17) holds if

$$q^{2n-4} > 2\log q \cdot (n+4)e^{n+4}$$

and one checks that this inequality is valid unless $q = 2$ and $n \leqslant 28$, $n = 6$ and $q \leqslant 5$, or $(n,q) \in \{(8,3),(10,3)\}$. In these remaining cases, one can also check (5.4.17) by applying the precise values of $|T|$, $h(T)$ and $|\mathrm{Out}(T)|$, so as above, it just remains to verify (5.4.18). To do this, first note that

$$h(T) = q^{n-1}|\mathrm{Sp}_{n-2}(q)| > \frac{1}{2}q^{n(n-1)/2},$$

so it suffices to show that

$$q^{n(n-3)/2} > 8en^2(n+1)^2(\log q)^2.$$

The latter holds unless $(n,q) = (6,2)$ or $(6,3)$, in which cases one can directly verify (5.4.18). The result now follows from Lemma 5.4.11.

Finally, assume $T = \mathrm{P}\Omega_n^{\varepsilon}(q)$ is an orthogonal group, so $n \geqslant 7$, and q is odd if n is odd. In this setting, $|T| < q^{n(n-1)/2}$ and

$$\frac{|T|}{h(T)} > \frac{1}{2}q^{n-1}$$

by Lemma 2.2.4 and Theorem 5.2.10. In addition, (5.4.17) holds if

$$q^{4n-4} > 24\log q \cdot (n+4)(2e)^{n+4}$$

since $|\mathrm{Out}(T)| \leqslant 24\log q$, which is valid unless $q = 2$ and $n \leqslant 14$. In the remaining cases, (5.4.17) can be checked directly. Finally, to prove (5.4.18), note that

$$h(T) > \frac{1}{4}q^{(n-1)(n-2)/2}$$

by Lemma 2.2.4 and Theorem 5.2.10, so we only need to show that

$$q^{(n-1)(n-4)/2} > 32en^2(n-1)^2(\log q)^2.$$

This holds unless $(n,q) = (7,3)$ or $(8,2)$, and in these special cases we can verify (5.4.18) directly. We now complete the proof by applying Lemma 5.4.11. ■

As explained in Remark 5.8, we conclude that the proofs of Theorems 5.2 and 5.5.1 are complete by combining Propositions 5.5.10, 5.5.11, 5.5.14 and 5.5.17. And the proof of Theorem 5.7 is also complete.

5.6 The groups with $k = 2$

In this section, we consider the groups with $k = 2$, noting that $b(G) \in \{3,4\}$ by Theorem 5.2.3(ii). We will establish Theorems 5.1, 5.3 and 5.4 for these groups.

First, we consider the case where $P = 1$. Here $G \leqslant \mathrm{Hol}(T)$, and we have $b(G) = 3$ by Theorem 5.2.3(ii).

Lemma 5.6.1. *Suppose that $k = 2$ and $P = 1$. Then G is semi-Frobenius. In particular, $\Sigma(G)$ is not G-arc-transitive.*

Proof. As noted in Example 3.3.10, $\mathrm{Hol}(T)$ is semi-Frobenius, and so the same is true for G (by Lemma 3.2.7). In view of Lemma 3.3.8, $\Sigma(G)$ is not G-arc-transitive. ■

From now on, we focus on the groups with $P = S_2$.

Lemma 5.6.2. *Suppose $G = T^2.(\mathrm{Out}(T) \times S_2)$ and $x, y \in T$. Then $\{D, D(1,\varphi_x), D(1,\varphi_y)\}$ is a base for G if and only if:*

(i) $C_{\mathrm{Aut}(T)}(x) \cap C_{\mathrm{Aut}(T)}(y) = 1$*; and*

(ii) there is no $\alpha \in \mathrm{Aut}(T)$ such that $x^\alpha = x^{-1}$ and $y^\alpha = y^{-1}$.

Proof. This can be deduced from [98, Lemma 3.5]. ■

The following is [86, Theorem 1.1].

Theorem 5.6.3. *Suppose T is not A_7, $\mathrm{L}_2(q)$ or $\mathrm{L}_3^\varepsilon(q)$ for some prime power q. Then there exists a generating pair (x, y) of T such that $|x| = 2$ and there is no $\alpha \in \mathrm{Aut}(T)$ with $x^\alpha = x^{-1}$ and $y^\alpha = y^{-1}$.*

It has recently been proved that each of the excluded groups A_7, $\mathrm{L}_2(q)$ and $\mathrm{L}_3^\varepsilon(q)$ in Theorem 5.6.3 are genuine exceptions (see [74, Theorem 1.3]).

Now we are ready to prove Theorems 5.1 and 5.3 for the groups with $k = 2$.

Proposition 5.6.4. *The conclusions to Theorems 5.1 and 5.3 hold when $k = 2$.*

Proof. The cases where $T \in \{A_5, A_6, A_7\}$ can be easily handled using MAGMA, so we assume $T \notin \{A_5, A_6, A_7\}$ and we are aiming to prove that $b(G) = 3$ and $\Sigma(G)$ is not G-arc-transitive. To do this, it suffices to show that $\{D, D(1,\varphi_x), D(1,\varphi_y)\}$ is a base for some $x, y \in T$ with $|x| \neq |y|$ (note that this condition implies that $(D, D(1,\varphi_x))$ and $(D, D(1,\varphi_y))$ are two arcs in $\Sigma(G)$ in different G-orbits). By Theorem 5.6.3, this condition is satisfied if $T \notin \{\mathrm{L}_2(q), \mathrm{L}_3^\varepsilon(q)\}$, so we may assume $T = \mathrm{L}_2(q)$ or $\mathrm{L}_3^\varepsilon(q)$.

First assume $T = \mathrm{L}_2(q)$. Note that $q \notin \{5, 9\}$ since $T \notin \{A_5, A_6\}$. Let λ be a primitive element of $\mathbb{F}_q^\times$. Additionally, let $x \in T$ be the image of

$$\widehat{x} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \in \mathrm{SL}_2(q),$$

and let $y \in T$ be the image of

$$\widehat{y} = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(q)$$

for some $\mu \in \mathbb{F}_q^\times$. Then $|x| = (q-1)/(2, q-1)$ and $|y| = p$. We claim that conditions (i) and (ii) of Lemma 5.6.2 hold. To see this, first note that $C_{\Gamma\mathrm{L}_2(q)}(\widehat{x}) = C_{\mathrm{GL}_2(q)}(\widehat{x})$, and thus

$$C_{\mathrm{P}\Gamma\mathrm{L}_2(q)}(x) = C_{\mathrm{PGL}_2(q)}(x) \cong C_{q-1}.$$

Moreover, $C_{\mathrm{PGL}_2(q)}(y) \cong C_p^f$, and so

$$C_{\mathrm{Aut}(T)}(x) \cap C_{\mathrm{Aut}(T)}(y) = C_{\mathrm{PGL}_2(q)}(x) \cap C_{\mathrm{PGL}_2(q)}(y) = 1,$$

which gives Lemma 5.6.2(i). Observe next that $\widehat{x}^g = \widehat{x}^{-1}$, where

$$g = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(q).$$

It follows that if $h \in \Gamma\mathrm{L}_2(q)$ and $\widehat{x}^h = \widehat{x}^{-1}$, then h lies in the coset $C_{\Gamma\mathrm{L}_2(q)}(\widehat{x})g = C_{\mathrm{GL}_2(q)}(\widehat{x})g$. Thus

$$h = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}$$

for some $a, b \in \mathbb{F}_q^\times$. However,

$$\widehat{y}^h = \begin{pmatrix} 1 & 0 \\ a^{-1}b\mu & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & -\mu \\ 0 & 1 \end{pmatrix} = \widehat{y}^{-1}.$$

Lemma 5.6.2(ii) now follows, and the proof is complete for $T = \mathrm{L}_2(q)$.

It remains to consider the case $T = \mathrm{L}_3^\varepsilon(q)$, with $\varepsilon \in \{+,-\}$ and $q \geqslant 3$. It suffices to find $x, y \in T$ of distinct orders such that $N_{\mathrm{Aut}(T)}(\langle x\rangle) \cap N_{\mathrm{Aut}(T)}(\langle y\rangle) = 1$. For $q \leqslant 32$, it is routine to find these elements by random search with the aid of MAGMA. Thus, we may assume that $q > 32$. Let H_1 be a maximal subgroup of $\mathrm{Aut}(T)$ of type $\mathrm{GL}_1^\varepsilon(q^3)$, so that $H_1 = N_{\mathrm{Aut}(T)}(\langle x\rangle)$ for some $x \in T$ with $|x| = (q^2+\varepsilon q+1)/(3, q-\varepsilon)$. In addition, let y be an element of T with a pre-image

$$\widehat{y} = \begin{pmatrix} A & \\ & \zeta \end{pmatrix} \in \mathrm{SL}_3^\varepsilon(q),$$

for some $A \in \mathrm{GL}_2(q)$ of order q^2-1, with ζ chosen so that $\det(\widehat{y}) = 1$. Then $|\widehat{y}| = q^2-1$ and $|y| = (q^2-1)/(3, q-\varepsilon)$. Let $H_2 := N_{\mathrm{Aut}(T)}(\langle y\rangle)$. By [72, Satz II.7.3(a)], we have $H_2 \cap T = \langle y\rangle.2$. It suffices to show that $H_1^g \cap H_2 = 1$ for some $g \in \mathrm{Aut}(T)$, or equivalently, that $\mathrm{Aut}(T)$ has a regular orbit on $\Gamma_1 \times \Gamma_2$, where $\Gamma_i := [\mathrm{Aut}(T) : H_i]$. Recall that

$$\mathrm{fpr}(z, \Gamma_i) = \frac{|z^{\mathrm{Aut}(T)} \cap H_i|}{|z^{\mathrm{Aut}(T)}|}$$

is the fixed point ratio of $z \in \mathrm{Aut}(T)$ on Γ_i. Letting $R(\mathrm{Aut}(T))$ be a set of $\mathrm{Aut}(T)$-class representatives of prime order elements in $\mathrm{Aut}(T)$, arguing as in Section 2.4 shows that $\mathrm{Aut}(T)$ has a regular orbit on $\Gamma_1 \times \Gamma_2$ if

$$\begin{aligned} m :&= \sum_{z \in R(\mathrm{Aut}(T))} |z^{\mathrm{Aut}(T)}| \cdot \mathrm{fpr}(z, \Gamma_1) \cdot \mathrm{fpr}(z, \Gamma_2) \\ &= \sum_{z \in R(\mathrm{Aut}(T))} \frac{|z^{\mathrm{Aut}(T)} \cap H_1| \cdot |z^{\mathrm{Aut}(T)} \cap H_2|}{|z^{\mathrm{Aut}(T)}|} < 1. \end{aligned} \tag{5.6.1}$$

Following the proof of [14, Lemma 6.4], let $z \in H_1$ be an element of prime order r. First assume that z is unipotent or semisimple, so the proof of [14, Lemma 6.4] gives

$$|z^{\mathrm{Aut}(T)}| \geqslant \frac{1}{3}q^3(q-1)(q^2-q+1) =: c_1.$$

We note that $|H_1 \cap \mathrm{PGL}_3^{\varepsilon}(q)| \leqslant 3(q^2+q+1) =: a_1$ and $|H_2 \cap \mathrm{PGL}_3^{\varepsilon}(q)| \leqslant 6(q^2-1) =: b_1$.

Now assume that z is a field automorphism with r odd. Here $r \geqslant 5$, as noted in the proof of [14, Lemma 6.4], so we have

$$|z^{\mathrm{Aut}(T)}| \geqslant |z^{\mathrm{PGL}_3^{\varepsilon}(q)}| = \frac{|\mathrm{PGL}_3^{\varepsilon}(q)|}{|\mathrm{PGL}_3^{\varepsilon}(q^{1/r})|} > \frac{1}{2}q^{32/5} =: c_2,$$

and there are at most $3(q^2+q+1)\log_2 q =: a_2$ and $6(q^2-1)\log_2 q =: b_2$ of these elements in H_1 and H_2, respectively.

Assume next that z is an involutory graph automorphism. Then $|C_{\mathrm{PGL}_3^{\varepsilon}(q)}(z)| = |\mathrm{Sp}_2(q)|$ and so $|z^{\mathrm{Aut}(T)}| \geqslant q^2(q^3-1) =: c_3$. Moreover, z inverts the normal subgroup $C_{(q^2+\varepsilon q+1)/(3,q-\varepsilon)}$ of H_1 and the normal subgroup $C_{(q^2-1)/(3,q-\varepsilon)}$ of H_2. This implies that both $C_{(q^2+\varepsilon q+1)/(3,q-\varepsilon)}.\langle z\rangle$ and $C_{(q^2-1)/(3,q-\varepsilon)}.\langle z\rangle$ are dihedral, so H_1 contains at most $a_3 := q^2+q+1$ involutory graph automorphisms, and H_2 contains at most $b_3 := q^2-1$ such elements.

It remains to consider the case where $\varepsilon = +$ and z is an involutory field or graph-field automorphism. Here,

$$|z^{\mathrm{Aut}(T)}| \geqslant |z^{\mathrm{PGL}_3(q)}| \geqslant \frac{|\mathrm{PGL}_3(q)|}{|\mathrm{PGU}_3(q^{1/2})|} = q^{3/2}(q+1)(q^{3/2}-1) =: c_4,$$

and (as noted in the proof of [14, Lemma 6.4]) there are fewer than $a_4 := 2(q+q^{1/2}+1)$ of these elements in H_1. We also set $b_4 := 12(q^2-1) \geqslant |(H_2 \cap \mathrm{PGL}_3^{\varepsilon}(q)).\langle z\rangle|$.

Finally, we conclude that the number m defined in (5.6.1) is less than $\sum_{i=1}^{4} a_i b_i / c_i$, which is less than 1 if $q > 32$. As noted above, this implies that $N_{\mathrm{Aut}(T)}(\langle x^g\rangle) \cap N_{\mathrm{Aut}(T)}(\langle y\rangle) = 1$ for some $g \in G$, which completes the proof. ■

From the proof of Proposition 5.6.4, we deduce the following property of simple groups, which will be useful in Section 5.7.3 when we seek to establish Theorems 5.1 and 5.3 for the groups with $k = |T|^{\ell} - 2$.

Lemma 5.6.5. *Let $O \leqslant \mathrm{Out}(T)$ and $K := \mathrm{Inn}(T).O$, with $O \neq \mathrm{Out}(T)$ if $T \in \{A_5, A_6\}$. Then there exists a pair (x,y) of elements of T such that:*

(a) $|x| \neq |y|$;

(b) $C_K(x) \cap C_K(y) = 1$; *and*

(c) there is no $\alpha \in K$ such that $x^{\alpha} = x^{-1}$ and $y^{\alpha} = y^{-1}$.

Now we determine whether or not G is semi-Frobenius in several special cases.

Lemma 5.6.6. *Let $O \leqslant \mathrm{Out}(T)$. Suppose that $P = S_2$ and $T \in \{A_5, A_6\}$. Then G is not semi-Frobenius if and only if $G = T^2.(O \times S_2)$ with*

$$(T, \mathrm{Inn}(T).O) \in \{(A_5, A_5), (A_6, S_6), (A_6, \mathrm{PGL}_2(9))\}.$$

Proof. This can be obtained with the aid of MAGMA, implementing the approach described in Section 4.2.5. Here we construct the group G via the primitive group database in MAGMA, noting that $|\Omega| = |T| \in \{60, 360\}$. ■

For the remainder of this section, we assume $T \notin \{A_5, A_6\}$, so the conclusion to Theorem 5.1 for these groups implies that $b(G) = 3$. In this setting, Lemma 5.6.2 implies that the group $T^2.(\mathrm{Out}(T) \times S_2)$ is semi-Frobenius if and only if for each non-identity element $x \in T$,

$$(\diamond) \qquad \begin{gathered} \textit{there exists } y \in T \textit{ such that } C_{\mathrm{Aut}(T)}(x) \cap C_{\mathrm{Aut}(T)}(y) = 1 \\ \textit{and there is no } \alpha \in \mathrm{Aut}(T) \textit{ with } (x,y)^\alpha = (x^{-1}, y^{-1}). \end{gathered}$$

We start with two basic observations.

Lemma 5.6.7. *Suppose that $T \notin \{A_5, A_6\}$. Then $T^2.(\mathrm{Out}(T) \times S_2)$ is semi-Frobenius if and only if $(\diamond)$ holds for all $x \in T$ of prime order.*

Proof. Let m be an integer, and let $t \in T$ and $\alpha \in \mathrm{Aut}(T)$. Since $C_{\mathrm{Aut}(T)}(t) \leqslant C_{\mathrm{Aut}(T)}(t^m)$ and $(t^m)^\alpha = (t^\alpha)^m$, the result follows. ■

Now we show that G is semi-Frobenius if $T = A_n$ with $n \geqslant 7$.

Proposition 5.6.8. *Suppose that $k = 2$ and $T = A_n$ for some $n \geqslant 7$. Then G is semi-Frobenius.*

Proof. The cases where $n \in \{7, 8, 9\}$ can be handled using MAGMA, so we will suppose that $n \geqslant 10$. Again, we may assume that $G = T^2.(\mathrm{Out}(T) \times S_2)$. We will appeal to Lemma 5.6.7 and prove the result by showing that $(\diamond)$ holds for all elements $x \in T$ of prime order. Conjugating by an element of S_n if necessary, we may assume that

$$(5.6.2) \qquad x = (1, 2, \ldots, p)(p+1, p+2, \ldots, 2p) \cdots ((\ell-1)p+1, (\ell-1)p+2, \ldots, \ell p)$$

for some prime p and some positive integer ℓ, so that the integers from 1 to ℓp appear in consecutive order.

Let $m := n$ if n is odd and $m := n-1$ if n is even. Suppose first that $x = (1,2)(3,4)$. We claim that $(\diamond)$ holds with $y = (1, 4, 3, 5, 2, 6, 7, \ldots, m)$ (so that all integers from 6 to m appear in consecutive order). To see this, first note that $C_{S_n}(y) = \langle y \rangle$, and that the elements of S_n inverting y by conjugation are precisely the elements of the right coset $\langle y \rangle \sigma$, where

$$\sigma = (4, m)(3, m-1)(5, m-2)(2, m-3)(6, m-4)(7, m-5) \cdots \left(\frac{m+1}{2}, \frac{m+3}{2}\right).$$

It is easy to check that if $g \in S_n \setminus \{1\}$ satisfies $y^g \in \{y, y^{-1}\}$ and $1^g \leqslant 4$, then $2^g > 4$ or $4^g > 4$, and thus $x^g \neq x = x^{-1}$.

To complete the proof, suppose that $x \neq (1,2)(3,4)$. We claim that property $(\diamond)$ holds with $y = (1, 3, 4, 2, 5, 6, \ldots, m)$. By the definition of x in (5.6.2), x cannot lie in $\langle y \rangle$. In what follows, we write ordered pairs using square brackets to avoid confusion with permutations.

First, we will show that $C_{S_n}(x) \cap C_{S_n}(y) = 1$. Note that $C_{S_n}(y) = \langle y \rangle$, so for each non-identity $g \in C_{S_n}(y)$, either

$$[1^g, 2^g] \in \{[2,7],[3,5],[4,6],[m-2,1],[m-1,3],[m,4]\},$$

or $1^g \in \{5,\dots,m-3\}$ and $2^g = 1^g + 3$. Additionally, $3^g = m-1$ if $1^g = m-2$. On the other hand, we see from (5.6.2) that each $h \in C_{S_n}(x)$ maps 1 and 2 to points in a common p-cycle of x, and $2^h = 1^h + 1$, interpreted within that cycle. Moreover, if $[1^h, 2^h] = [m-2,1]$ then $(1,\dots,m-2)$ is a p-cycle of x and $3^h = 2$. It follows that $C_{S_n}(x) \cap C_{S_n}(y) = 1$.

Finally, we will show that no element of S_n inverts both x and y via conjugation. To see this, first observe that the elements of S_n inverting y are precisely the elements of the coset $\langle y \rangle \tau$, where

$$\tau = (3,m)(4,m-1)(2,m-2)(5,m-3)(6,m-4)\cdots\left(\frac{m+1}{2},\frac{m+3}{2}\right).$$

Assume that g lies in this coset. Then either

$$[1^g, 2^g] \in \{[1,m-2],[2,1],[3,m-1],[4,m],[5,3],[6,4],[7,2]\},$$

or $1^g \in \{8,\dots,m\}$ and $2^g = 1^g - 3$. Furthermore, if g fixes 1, then $3^g = m$, and if $[1^g, 2^g] = [2,1]$, then $[3^g, 5^g, 6^g] = [4, m, m-1]$. Now let h be an element of S_n that inverts x. Then h maps 1 and 2 to points in a common p-cycle of x, and $2^h = 1^h - 1$, interpreted within that cycle. In addition, $3^h = m-3$ if $[1^h, 2^h] = [1, m-2]$, and if $[1^h, 2^h] = [2,1]$, then either $p = 2$ or $3^h = p$. Thus, if h also inverts y, then $[1^h, 2^h, 3^h, 5^h, 6^h] = [2,1,4,m,m-1]$, and the fact that p is prime yields $p = 2$. Our assumption that $x \neq (1,2)(3,4)$ now gives $\ell p \geqslant 6$, and $[5^h, 6^h] = [m, m-1]$ implies that $(m-1, m)$ is a cycle of x, so that m must be even. However, m is odd, a contradiction. This completes the proof. ■

To complete the proof of Theorem 5.4(i), it suffices to consider the case where T is a sporadic simple group. To do this, we first present the following result, which will be recorded in my paper [70]. Here we say a conjugacy class C of a group X is a *witness* if for any $g \in X^\#$, there exists $h \in C$ such that $\langle g, h \rangle = X$.

Lemma 5.6.9. *Suppose that there exists $y \in T$ such that y^T is a witness and $y^{-1} \notin y^{\mathrm{Aut}(T)}$. Then $T^2.(\mathrm{Out}(T) \times S_2)$ is semi-Frobenius.*

Proof. Note that the condition in the statement implies that $T \notin \{A_5, A_6\}$. In addition, for any $z \in T^\#$, there exists $x \in z^T$ such that $\langle x, y \rangle = T$, so $C_{\mathrm{Aut}(T)}(x) \cap C_{\mathrm{Aut}(T)}(y) = 1$. This gives ($\diamond$) since $y^{-1} \notin y^{\mathrm{Aut}(T)}$. ■

By a theorem of Guralnick and Kantor [63, Theorem I], every non-abelian finite simple group has a witness. In establishing this result, the probabilistic method introduced in [63, Section 2] played a central role. To be more precise, for elements s and g in a finite group X, let

$$\mathbb{P}_s(g) = \frac{|\{t \in g^X : X = \langle s, t \rangle\}|}{|g^X|}$$

T	M_{11}	M_{12}	M_{22}	M_{23}	M_{24}	HS	Ru	McL	Ly	J_1	J_2	J_3	J_4
m	11	10	7	11	23	11	16	11	11	19	7	19	7

T	Co_1	Co_2	Co_3	HN	He	Suz	Fi_{22}	Fi_{23}	Fi_{24}'	O′N	Th	$\mathbb{B}$	$\mathbb{M}$
m	23	23	11	19	17	13	22	23	23	31	31	47	59

Table 5.4: The integer m in Proposition 5.6.10

be the probability that s and a uniformly random element in g^X generate X. Thus, g^X is a witness if $\mathbb{P}_s(g) > 0$ for all $s \in X^{\#}$ (equivalently, for all $s \in X$ of prime order). The probability $\mathbb{P}_s(g)$ can be estimated as follows. For an element $z \in X$ and a maximal subgroup K of X, we write $\mathrm{fpr}(z,K)$ for the fixed point ratio of z with respect to the action of X on $[X:K]$, recalling that $\mathrm{fpr}(z,K) = |z^X \cap K|/|z^X|$. Then as noted in [63, Section 2],

$$1 - \mathbb{P}_s(g) \leqslant \sum_{K \in \mathcal{M}(g)} \mathrm{fpr}(s,K) =: \widehat{\mathbb{Q}}_s(g),$$

where $\mathcal{M}(g)$ is the set of maximal subgroups of X containing g.

Given this observation, we now prove that the group $G = T^2.(\mathrm{Out}(T) \times S_2)$ is semi-Frobenius if T is a sporadic simple group. Here we establish a stronger result.

Proposition 5.6.10. *Suppose T is a sporadic simple group, and let y be an element of order m, where m is described in Table 5.4. Then for any $z \in T \setminus y^T$ of prime order, there exists $x \in z^T$ such that $\langle x, y \rangle = T$ and there is no $\alpha \in \mathrm{Aut}(T)$ with $(x,y)^\alpha = (x^{-1}, y^{-1})$.*

Proof. First assume

$$T \in \{\mathrm{M}_{11}, \mathrm{M}_{22}, \mathrm{M}_{23}, \mathrm{M}_{24}, \mathrm{McL}, \mathrm{J}_4, \mathrm{Co}_1, \mathrm{Co}_2, \mathrm{Co}_3, \mathrm{Ru}, \mathrm{Fi}_{23}, \mathrm{Fi}_{24}', \mathrm{Th}, \mathrm{Ly}, \mathbb{B}, \mathbb{M}\}.$$

If $T \in \{\mathbb{B}, \mathbb{M}\}$, then y^T is a witness, as noted in [13, Section 4.7], and one can use the GAP function `InverseClasses` on the character table of T to check that $y^{-1} \notin y^{\mathrm{Aut}(T)}$. If instead $T \notin \{\mathbb{B}, \mathbb{M}\}$, one can check with the aid of GAP that $y^{-1} \notin y^{\mathrm{Aut}(T)}$ and $\widehat{\mathbb{Q}}_z(y) < 1$ for all $z \in T^{\#}$ (the latter implies that y^T is a witness). This gives the desired result for these groups. See Appendix A.2.2 for the relevant GAP code.

Next, we assume

$$T \in \{\mathrm{M}_{12}, \mathrm{HS}, \mathrm{Suz}, \mathrm{He}, \mathrm{J}_1, \mathrm{J}_2, \mathrm{J}_3, \mathrm{Fi}_{22}, \mathrm{O'N}\}.$$

For an element $g \in T$, let $I(g) := \{\alpha \in \mathrm{Aut}(T) : g^\alpha \in \{g, g^{-1}\}\} \leqslant \mathrm{Aut}(T)$ be the group of elements in $\mathrm{Aut}(T)$ centralising or inverting g. With the aid of MAGMA, one can check that for each T-class representative $z \in T \setminus y^T$ of prime order (obtained via the function `ConjugacyClasses`), there exists $x \in z^T$ such that $\langle x, y \rangle = T$ and $I(x) \cap I(y) = 1$, noting that the latter condition implies that there is no $\alpha \in \mathrm{Aut}(T)$ with $(x,y)^{\alpha} = (x^{-1},y^{-1})$. The element $x \in z^T$ can be obtained by random search, and we refer the reader to Appendix A.1.4 for the relevant MAGMA code.

To complete the proof, assume $T = \mathrm{HN}$. Here the function `ConjugacyClasses` is expensive since $|T|$ is too large. Thus, we obtain each T-class representative of prime order within an appropriate maximal subgroup. For example, we first construct the maximal subgroup $K = \mathrm{U}_3(8).3$ of T using the generators given in the Web ATLAS [123], and obtain y in the Sylow 19-subgroup within K. Other representatives of prime order can be constructed with the same method. As before, we check that for each representative $z \in T \setminus y^T$ of prime order, there exists $x \in z^T$ such that $\langle x,y\rangle = T$ and $I(x) \cap I(y) = 1$, which gives the desired result. See Appendix A.1.4 for the relevant MAGMA code. ■

Corollary 5.6.11. *If T is a sporadic simple group, then the diagonal type primitive group $T^2.(\mathrm{Out}(T) \times S_2)$ is semi-Frobenius.*

Proof. This is given by combining Lemma 5.6.7 and Proposition 5.6.10. ■

The conclusion to Theorem 5.4(i) follows from Lemma 5.6.1, Proposition 5.6.8 and Corollary 5.6.11 (see Remark 5.8).

Finally, we show that G is not semi-Frobenius if $G = T^2.(\mathrm{Out}(T) \times S_2)$, $T = \mathrm{L}_2(q)$ and $q \geqslant 11$.

Proposition 5.6.12. *Suppose that $G = T^2.(\mathrm{Out}(T) \times S_2)$, where $T = \mathrm{L}_2(q)$ for some $q \geqslant 11$. Then G is not semi-Frobenius.*

Proof. Let $x \in T$ be an element of order $(q+1)/(2,q-1)$. We claim that ($\diamond$) does not hold, which implies the desired result. Setting $R := \mathrm{PGL}_2(q)$, we note that $C_T(x) = \langle x\rangle$, $C_R(x) \cong C_{q+1}$, and $N_R(\langle x\rangle) \cong D_{2(q+1)}$ is a maximal subgroup of R. In particular, each element of $N_R(\langle x\rangle)$ either centralises or inverts x.

Write $q = p^f$ with p prime, and let $y \in T$. Then either $|y| = p$, or y lies in a cyclic subgroup of T of order $(q-1)/(2,q-1)$ or $(q+1)/(2,q-1)$. We shall divide the rest of the proof into four cases, which together account for all possible choices for y; in each case, we will show that y does not satisfy ($\diamond$).

Case 1. $|y| = 2$.

The normaliser $N_T(\langle x\rangle)$ is the unique maximal subgroup of T containing x. Thus if $y \notin N_T(\langle x\rangle)$, then $\langle x,y\rangle = T$. It follows (see [112, Theorem 3] and [86, p. 582]) that there exists $\alpha \in \mathrm{Aut}(T)$ such that $(x,y)^{\alpha} = (x^{-1},y^{-1})$. If instead $y \in N_T(\langle x\rangle) \setminus \langle x\rangle$, then $(x,y)^y = (x^{-1},y^{-1})$, and if $y \in \langle x\rangle$, then $y \in C_{\mathrm{Aut}(T)}(x) \cap C_{\mathrm{Aut}(T)}(y)$. Hence y does not satisfy ($\diamond$).

Case 2. p is odd and $|y| = p$.

Let H be the unique maximal subgroup of R of type P_1 that contains y. Then $H \cong C_p^f{:}C_{q-1}$, and each involution of H inverts y. Since $(q-1,q+1) = 2$ and any subgroup of H of order 4 is cyclic, we see that $J := H \cap N_R(\langle x\rangle)$ has order at most 2. In fact, $|H| \cdot |N_R(\langle x\rangle)| > |R|$, which implies that $|J| = 2$. Let α be the unique involution of J. Now, α is contained in a cyclic subgroup of H of order $q-1$. Hence if α centralises x, then α lies in a proper subgroup of R of order divisible by both $q-1$ and $q+1$. However, no such subgroup exists, and so $(x, y)^\alpha = (x^{-1}, y^{-1})$.

Case 3. $2 \neq |y| \mid (q+1)/(2,q-1)$.

Here, y is contained in a cyclic subgroup of T of order $(q+1)/(2,q-1)$. Since all such subgroups of T are conjugate, we obtain that $y \in \langle x^g\rangle$ for some $g \in T$. It is also clear that the maximal subgroup $N_R(\langle x^g\rangle) \cong D_{2(q+1)}$ of R is equal to $N_R(\langle y\rangle)$. If $y \in \langle x\rangle$, then clearly $C_{\mathrm{Aut}(T)}(x) \cap C_{\mathrm{Aut}(T)}(y) \neq 1$, so we shall assume that $y \notin \langle x\rangle$. By inspecting [49, Table 2], we see that $N := N_R(\langle x\rangle) \cap N_R(\langle y\rangle) \neq 1$. As $\langle x\rangle \cap \langle x^g\rangle = 1$, it follows that there exists $\alpha \in N$ such that $(x, y)^\alpha = (x^{-1}, y^{-1})$.

Case 4. $2 \neq |y| \mid (q-1)/(2,q-1)$.

We shall identify elements of R with corresponding matrices in $\mathrm{GL}_2(q)$. In this case, y lies in a cyclic subgroup of T of order $(q-1)/(2,q-1)$, and so (conjugating x and y by a common element of T if necessary) we may assume without loss of generality that y is a diagonal matrix. Suppose that

$$x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ for } a, b, c, d \in \mathbb{F}_q,$$

noting that $b, c \neq 0$ since $|x| = (q+1)/(2,q-1)$. Then the matrix

$$\begin{pmatrix} 0 & 1 \\ -cb^{-1} & 0 \end{pmatrix}$$

inverts each of x and y, and so $(\diamond)$ does not hold. ■

Remark 5.6.13. In [70], I will present a complete classification of the semi-Frobenius groups with $G \leqslant T^2.(\mathrm{Out}(T) \times S_2)$, following the approach briefly outlined as below.

As in the proof of Proposition 5.6.10, for an element $g \in T$, let

$$I(g) = \{\alpha \in \mathrm{Aut}(T) : g^\alpha = \{g, g^{-1}\}\} \leqslant \mathrm{Aut}(T)$$

be the group of elements in $\mathrm{Aut}(T)$ centralising or inverting g. For elements $x, y \in T$, let $\Gamma_1 := [\mathrm{Aut}(T) : I(x)]$ and $\Gamma_2 := [\mathrm{Aut}(T) : I(y)]$. Then as noted in the proof of Proposition 5.6.4, $\mathrm{Aut}(T)$ has a regular orbit on $\Gamma_1 \times \Gamma_2$ if and only if there exists $g \in \mathrm{Aut}(T)$ such that $I(x) \cap I(y^g) = 1$. The latter implies that both $\{D, D(1,\varphi_x)\}$ and $\{D, D(1,\varphi_y)\}$ are edges in $\Sigma(G)$ if one of x and y has order at least 3, whereas the former condition holds if

$$\sum_{z \in R(\mathrm{Aut}(T))} |z^{\mathrm{Aut}(T)}| \cdot \mathrm{fpr}(z, \Gamma_1) \cdot \mathrm{fpr}(z, \Gamma_2) = \sum_{z \in R(\mathrm{Aut}(T))} \frac{|z^{\mathrm{Aut}(T)} \cap I(x)| \cdot |z^{\mathrm{Aut}(T)} \cap I(y)|}{|z^{\mathrm{Aut}(T)}|} < 1,$$

where $R(\mathrm{Aut}(T))$ is a set of $\mathrm{Aut}(T)$-class representatives of prime order elements.

Let us finish this section by recording the following remark on the groups satisfying property $(\star)$ (see Section 3.3.1).

Remark 5.6.14. Suppose that $G = T^2.(\mathrm{Out}(T) \times S_2)$ with $T \notin \{A_5, A_6\}$ (so that $b(G) = 3$), and let

$$N := \{t \in T : D(1,\varphi_t) \text{ is a neighbour of } D \text{ in } \Sigma(G)\}.$$

Then we claim that $\Sigma(G)$ has diameter at most 2 (equivalently, G satisfies $(\star)$, as noted in Remark 3.3.1) if and only if $N^2 = T$ (that is, any $t \in T$ can be written as $t = x_1x_2$ for some $x_i \in N$).

To see this, note that for $g = (1, x^{-1}) \in T^2 \leqslant G$,

$$(D(1,\varphi_x), D(1,\varphi_y))^g = (D, D(1,\varphi_{yx^{-1}})).$$

In particular, $(D(1,\varphi_x), D(1,\varphi_y))$ is an arc in $\Sigma(G)$ if and only if $(D, D(1,\varphi_{yx^{-1}}))$ is. Hence

$$(D, D(1,\varphi_{x_2}), D(1,\varphi_{x_1x_2}))$$

is a 2-arc from D to $D(1,\varphi_t)$, so $\mathrm{diam}(\Sigma(G)) \leqslant 2$. The converse also holds by a similar argument.

As an example, in the case of $T = \mathrm{L}_2(q)$ with $q = 7$ or $q \geqslant 11$, the elements of T of order $(q-1)/(2,q-1)$ lie in N (as noted in the proof of Proposition 5.6.4). By [56, Theorems 2(i) and 3(i)], for the conjugacy class C of an element of order $(q-1)/(2,q-1)$, we have $C^2 = T$, and so it follows that $N^2 = T$ and $\mathrm{diam}(\Sigma(G)) \leqslant 2$.

5.7 Proofs of Theorems 5.1, 5.3 and 5.4

In this section, we will establish Theorems 5.1, 5.3 and 5.4. Note that the conclusions to these theorems for the groups with $k = 2$ have already been established in Section 5.6. Moreover, Theorems 5.2 and 5.5.1 yield the required results for base-two groups, and one can use Proposition 5.5.8 and Lemma 5.5.9 to handle the groups with $k \in \{|T|-2, |T|-1\}$. With these results in hand, we will assume $k \geqslant |T|$ and $P \in \{A_k, S_k\}$ in this section. Recall that G contains A_k (see Corollary 5.2.6), and recall that $b(G) \in \{\ell+1, \ell+2\}$ if $|T|^{\ell-1} < k \leqslant |T|^\ell$ by Theorem 5.2.3(iii).

Recall that for an element $\mathbf{x} = (\varphi_{t_1}, \ldots, \varphi_{t_k}) \in \mathrm{Inn}(T)^k$, the partition $\mathscr{P}^{\mathbf{x}} = \{\mathscr{P}^{\mathbf{x}}_t : t \in T\}$ of $[k]$ is defined so that $j \in \mathscr{P}^{\mathbf{x}}_t$ if $t_j = t$.

Lemma 5.7.1. *Let $\mathbf{x}, \mathbf{y} \in \mathrm{Inn}(T)^k$ be such that $D\mathbf{x}$ and $D\mathbf{y}$ lie in a common G_D-orbit. Then there exist $g \in T$ and $\alpha \in \mathrm{Aut}(T)$ such that for each integer m,*

$$g\{t \in T : |\mathscr{P}^{\mathbf{x}}_t| = m\}^\alpha = \{t \in T : |\mathscr{P}^{\mathbf{y}}_t| = m\}. \tag{5.7.1}$$

Proof. Write $\mathbf{x} = (\varphi_{x_1}, \ldots, \varphi_{x_k})$ and $\mathbf{y} = (\varphi_{y_1}, \ldots, \varphi_{y_k})$, and let $\alpha \in \mathrm{Aut}(T)$ and $\pi \in S_k$ be such that $D\mathbf{x}^{(\alpha,\ldots,\alpha)\pi} = D\mathbf{y}$. Then

$$D(\varphi_{x_1^\alpha}, \ldots, \varphi_{x_k^\alpha}) = D(\varphi_{y_{1^\pi}}, \ldots, \varphi_{y_{k^\pi}}).$$

It follows that there exists $g \in T$ such that $gx_j^\alpha = y_{j^\pi}$ for all $j \in [k]$, and that $(\mathscr{P}^{\mathbf{x}}_{x_j})^\pi = \mathscr{P}^{\mathbf{y}}_{y_{j^\pi}}$. In particular, $|\mathscr{P}^{\mathbf{x}}_{x_j}| = |\mathscr{P}^{\mathbf{y}}_{y_{j^\pi}}| = |\mathscr{P}^{\mathbf{y}}_{gx_j^\alpha}|$, and thus (5.7.1) holds. ∎

Note from Lemma 3.3.8 that if G is semi-Frobenius, then $\Sigma(G)$ is not G-arc-transitive as G is not 2-transitive. To establish Theorem 5.4(ii)(b), the following lemma will be a key ingredient.

Lemma 5.7.2. *Let $\pi = (j_1,\dots,j_m) \in S_k$ be an m-cycle with $m < k$, and let $\mathbf{x} = (\varphi_{t_1},\dots,\varphi_{t_k}) \in \mathrm{Inn}(T)^k$ such that $t_{j_1},\dots,t_{j_m}$ are not all equal. Then $\pi \notin G_D \cap G_{D\mathbf{x}}$.*

Proof. Suppose for a contradiction that $\pi \in G_D \cap G_{D\mathbf{x}}$. Then there exists $g \in T$ such that $t_j = gt_{j^\pi}$ for all $j \in [k]$. Since $m < k$, there exists $j_0 \in [k] \setminus \{j_1,\dots,j_m\}$, so by taking $j = j_0$ we see that $g = 1$. However, this yields $t_{j_1} = \cdots = t_{j_m}$, which is incompatible with our assumption. ■

Corollary 5.7.3. *The group G is semi-Frobenius if there exists a subset $\Delta \subseteq \Omega$ of size $b(G)-1$ such that $G_{(\Delta)}$ is generated by a transposition.*

5.7.1 The groups with $k = |T|$

We start with the case where $k = |T|$ and $P \in \{A_k, S_k\}$.

Proposition 5.7.4. *Suppose $k = |T|$ and $P \in \{A_k, S_k\}$. Then G is semi-Frobenius. In particular, $\Sigma(G)$ is not G-arc-transitive.*

Proof. First note that $b(G) = 3$ by Theorem 5.2.3(iii). Write $\mathbf{x} = (\varphi_{x_1},\dots,\varphi_{x_k}) \in \mathrm{Inn}(T)^k$. We consider the following two cases in turn and show that $\{D, D\mathbf{x}\}$ can be extended to a base for G of size 3 in each case.

Case 1. There are at least three distinct entries in $\mathbf{x}$.

Without loss of generality, we may assume that x_1, x_2, x_3 are distinct. In view of Lemma 5.7.2, it suffices to find $\mathbf{a} = (\varphi_{t_1},\dots,\varphi_{t_k}) \in \mathrm{Inn}(T)^k$ such that $G_D \cap G_{D\mathbf{a}} \leqslant \langle (1,2,3),(1,2) \rangle$. Theorem 5.7 (proved in Section 5.5) implies that there exists a subset $S \subseteq T^\#$ of size $|T|-3$ with trivial setwise stabiliser in $\mathrm{Aut}(T)$. Let $\{t_4,\dots,t_k\} = S$ and let $t_1 = t_2 = t_3 = 1$. Suppose $(\alpha,\dots,\alpha)\pi \in G_{D\mathbf{a}}$. Then by Lemma 5.2.2(iii) we have $S^\alpha = S$, which forces $\alpha = 1$. Thus, $G_D \cap G_{D\mathbf{a}} \leqslant \langle (1,2,3),(1,2) \rangle$ as desired.

Case 2. There are exactly two distinct entries in $\mathbf{x}$.

We may assume that $\mathbf{x} = (1,\dots,1,\varphi_x,\dots,\varphi_x)$ for some non-trivial $x \in T$, with 1 appearing exactly m times for some $m \leqslant |T|/2$ (that is, $|\mathscr{P}_1^{\mathbf{x}}| = m$). By the main theorem of [63], there exists $y \in T$ such that $\langle x, y \rangle = T$. Define $\mathbf{a} = (\varphi_{t_1},\dots,\varphi_{t_k}) \in \mathrm{Inn}(T)^k$ such that the following conditions hold:

(a) $t_m = t_{m+1} = 1$;

(b) $\{t_1,\dots,t_k\} \setminus \{t_m, t_{m+1}\} = T \setminus \{1, y\}$; and

(c) if $m = |T|/2$, then some $\mathrm{Aut}(T)$-conjugacy class C is equal to $\{t_1,\dots,t_{|C|}\}$ (note that $|C| < m$).

Note that since $k = |T|$, each element of $T\setminus\{1, y\}$ is equal to t_j for exactly one j. By Lemma 5.2.2(iii), if $(\alpha,\dots,\alpha)\pi \in G_{D\mathbf{a}}$, then $\alpha \in C_{\mathrm{Aut}(T)}(y)$.

Suppose now that $(\alpha,\dots,\alpha)\pi$ also lies in $G_{D\mathbf{x}}$. We claim that $\alpha \in C_{\mathrm{Aut}(T)}(x)$. If $m < |T|/2$, then this is immediate from Lemma 5.2.2(iii). Otherwise, the same lemma yields $t_j^\alpha = t_{j^\pi}$ for all $j \in [k]$ and

$$\{1,\dots,m\}^\pi = \{1,\dots,m\} \text{ or } \{m+1,\dots,k\}.$$

If the latter holds, then for each $j < m$, there exists $j' \geqslant m+1$ such that $t_j^\alpha = t_{j'}$, contradicting condition (c). Hence, $\{1,\dots,m\}$ is fixed by π, and $x_j^\alpha = x_{j^\pi}$ for all $j \in [k]$. This implies that $\alpha \in C_{\mathrm{Aut}(T)}(x)$, as claimed.

It now follows that $\alpha \in C_{\mathrm{Aut}(T)}(\langle x, y\rangle) = C_{\mathrm{Aut}(T)}(T) = 1$. Moreover, if $x_j = x_{j'}$, then $t_j \neq t_{j'}$, and therefore $\pi = 1$. Thus $\{D, D\mathbf{x}, D\mathbf{a}\}$ is a base for G. ■

5.7.2 The groups with $|T|^{\ell-1} < k \leqslant |T|^\ell - 3$

Next, assume $|T|^{\ell-1} < k \leqslant |T|^\ell - 3$ for $\ell \geqslant 2$. Our aim is to show that $b(G) = \ell + 1$ and the generalised Saxl graph $\Sigma(G)$ is not G-arc-transitive.

Lemma 5.7.5. *Suppose that $P \in \{A_k, S_k\}$, and that $|T|^{\ell-1} < k \leqslant |T|^\ell - 3$ for some $\ell \geqslant 2$. Then there exists $\mathbf{x} \in \mathrm{Inn}(T)^k$ such that the partition $\mathscr{P}^{\mathbf{x}} = \{\mathscr{P}_t^{\mathbf{x}} : t \in T\}$ of $[k]$ satisfies the following properties.*

(P1) $|\mathscr{P}_t^{\mathbf{x}}| \leqslant |T|^{\ell-1}$ for all $t \in T$.

(P2) $|\mathscr{P}_1^{\mathbf{x}}| \neq 0$ and $\mathrm{Hol}(T, S) = 1$, where $S = \{t \in T : |\mathscr{P}_t^{\mathbf{x}}| = |\mathscr{P}_1^{\mathbf{x}}|\}$.

(P3) There exists $x \in T^\#$ such that $|\mathscr{P}_x^{\mathbf{x}}| \in \{1, |T|^{\ell-1} - 1\}$.

(P4) If $k \neq |T|^\ell - 3$, then there exist $t_1, t_2 \in T \setminus S$ with $|\mathscr{P}_{t_1}^{\mathbf{x}}| \neq |\mathscr{P}_{t_2}^{\mathbf{x}}|$.

Proof. First assume $|T|^\ell - 2|T|^{\ell-1} < k \leqslant |T|^\ell - 3$. In view of Theorem 5.7, let S be a subset of T containing 1 with $|S| = |T| - 3$ and $\mathrm{Hol}(T, S) = 1$, and let $\{x_1, x_2, x_3\} = T \setminus S$. Now define $\mathbf{x} \in \mathrm{Inn}(T)^k$ with $|\mathscr{P}_t^{\mathbf{x}}| = |T|^{\ell-1}$ if $t \in S$, and $|\mathscr{P}_{x_i}^{\mathbf{x}}| \leqslant |T|^{\ell-1} - 1$ with

$$|\mathscr{P}_{x_1}^{\mathbf{x}}| = |T|^{\ell-1} - 1 \text{ and } |\mathscr{P}_{x_2}^{\mathbf{x}}| + |\mathscr{P}_{x_3}^{\mathbf{x}}| = k - (|T| - 2)|T|^{\ell-1} + 1.$$

Note that such a partition exists since

$$2 \leqslant k - (|T| - 2)|T|^{\ell-1} + 1 \leqslant 2|T|^{\ell-1} - 2.$$

It is then easy to check that $\mathscr{P}^{\mathbf{x}}$ satisfies the conditions (P1)–(P4).

Now assume $3|T|^{\ell-1} < k \leqslant |T|^\ell - 2|T|^{\ell-1}$. Then there exists an integer m such that $3 \leqslant m \leqslant |T| - 3$ and $m|T|^{\ell-1} < k \leqslant (m+1)|T|^{\ell-1}$. By Theorem 5.7, there exists a subset $S \subseteq T$ containing 1 with $|S| = m$ and $\mathrm{Hol}(T, S) = 1$. Let $x_1, x_2 \in T \setminus S$ and define $\mathbf{x} \in \mathrm{Inn}(T)^k$ with $|\mathscr{P}_t^{\mathbf{x}}| = |T|^{\ell-1}$ if

$t \in S$, $|\mathscr{P}^{\mathbf{x}}_{x_1}| = 1$ and $|\mathscr{P}^{\mathbf{x}}_{x_2}| = k - m|T|^{\ell-1} - 1$, noting that $0 \leqslant k - m|T|^{\ell-1} - 1 < |T|^{\ell-1}$. One can check (P1)–(P4) easily.

To complete the proof, we assume $|T|^{\ell-1} < k \leqslant 3|T|^{\ell-1}$ and let $S = \{t_1, t_2, t_3\} \subseteq T$ be such that $t_1 = 1$ and $\mathrm{Hol}(T,S) = 1$. In this setting, let $x_1, x_2, x_3 \in T \setminus S$ and define $\mathbf{x} \in \mathrm{Inn}(T)$ with $|\mathscr{P}^{\mathbf{x}}_{t_i}| = 1$, and $|\mathscr{P}^{\mathbf{x}}_{x_i}| \leqslant |T|^{\ell-1}$ with $|\mathscr{P}^{\mathbf{x}}_{x_i}| \neq 1$ and $|\mathscr{P}^{\mathbf{x}}_{x_1}| + |\mathscr{P}^{\mathbf{x}}_{x_2}| + |\mathscr{P}^{\mathbf{x}}_{x_3}| = k - 3$. We conclude the proof by noting that $\mathscr{P}^{\mathbf{x}}$ satisfies the conditions (P1)–(P4). ■

For the remainder of this subsection, we fix an element $\mathbf{x} = (\varphi_{t_{0,1}}, \dots, \varphi_{t_{0,k}}) \in \mathrm{Inn}(T)^k$ such that the associated partition $\mathscr{P}^{\mathbf{x}}$ of $[k]$ satisfies the conditions in Lemma 5.7.5, where $S \subseteq T$ and $x \in T^{\#}$ are as described in (P2) and (P3), respectively.

Lemma 5.7.6. *Suppose $(\alpha, \dots, \alpha)\pi \in G_{D\mathbf{x}}$. Then $\alpha = 1$ and $\pi \in P_{(\mathscr{P}^{\mathbf{x}})}$.*

Proof. First note that there exists a unique $g \in T$ such that $t_{0,j}^{\alpha} = g t_{0,j^{\pi}}$ for all $j \in [k]$, and we have $\pi \in P_{\{\mathscr{P}^{\mathbf{x}}\}}$ by Lemma 5.2.2(i). This implies that π fixes the set $\{\mathscr{P}^{\mathbf{x}}_t : t \in S\}$, and thus $g^{-1}t^{\alpha} \in S$ if $t \in S$, whence $g^{\alpha^{-1}}\alpha \in \mathrm{Hol}(T,S) = 1$. It follows that $g = 1$ and $\alpha = 1$, so $t_{0,j} = t_{0,j^{\pi}}$ for all $j \in [k]$, which concludes the proof. ■

Write $T^{\ell-1} = \{\mathbf{b}_1, \dots, \mathbf{b}_{|T|^{\ell-1}}\}$, where $\mathbf{b}_h = (a_{1,h}, \dots, a_{\ell-1,h})$. If $|\mathscr{P}^{\mathbf{x}}_x| = 1$, then we may assume $\mathbf{b}_1 = (1, \dots, 1)$, and if $|\mathscr{P}^{\mathbf{x}}_x| = |T|^{\ell-1} - 1$, we assume $\mathbf{b}_{|T|^{\ell-1}} = (1, \dots, 1)$. Let $1 \leqslant i \leqslant \ell - 1$ and define $\mathbf{a}_i = (\varphi_{t_{i,1}}, \dots, \varphi_{t_{i,k}}) \in \mathrm{Inn}(T)^k$, where $t_{i,j} = a_{i,h}$ if j is the h-th smallest number in $\mathscr{P}^{\mathbf{x}}_t$. Define $X_{i,t} := \{j \in \mathscr{P}^{\mathbf{x}}_x : t_{i,j} = t\}$.

Lemma 5.7.7. *For any $t \in T^{\#}$ and $i \in \{1, \dots, \ell - 1\}$, we have $|X_{i,t}| \neq |X_{i,1}|$.*

Proof. If $|\mathscr{P}^{\mathbf{x}}_x| = 1$, then $\mathbf{b}_1 = (1, \dots, 1)$, so $|X_{i,1}| = 1$ and $|X_{i,t}| = 0$ for all $t \in T^{\#}$. And if $|\mathscr{P}^{\mathbf{x}}_x| = |T|^{\ell-1}$, then $\mathbf{b}_{|T|^{\ell-1}} = (1, \dots, 1)$, which implies that $|X_{i,1}| = |T|^{\ell-1} - 1$ and $|X_{i,t}| = |T|^{\ell-1}$ for all $t \in T^{\#}$. ■

Lemma 5.7.8. *The set $\Delta = \{D, D\mathbf{x}, D\mathbf{a}_1, \dots, D\mathbf{a}_{\ell-1}\}$ is a base for G.*

Proof. Suppose $(\alpha, \dots, \alpha)\pi \in G_{(\Delta)}$. By Lemma 5.7.6, we have $\alpha = 1$ and $\pi \in P_{(\mathscr{P}^{\mathbf{x}})}$. Note that for any $i \in \{1, \dots, \ell - 1\}$, there exists a unique $g_i \in T$ such that $t_{i,j} = g_i t_{i,j^{\pi}}$ for any $j \in [k]$. Now $j \in X_{i,1}$ if and only if $j^{\pi} \in X_{i,g_i^{-1}}$. This implies that $g_i = 1$ by Lemma 5.7.7, and hence $t_{i,j} = t_{i,j^{\pi}}$ for all $i \in \{1, \dots, \ell - 1\}$ and $j \in [k]$.

From the definition of $\mathbf{a}_i$, we see that if $j, j' \in \mathscr{P}^{\mathbf{x}}_t$ and $j \neq j'$, then there exists $i \in \{1, \dots, \ell - 1\}$ such that $t_{i,j} \neq t_{i,j'}$. This yields $j^{\pi} \neq j'$, so $j^{\pi} = j$ since $\pi \in P_{\{\mathscr{P}^{\mathbf{x}}_t\}}$. That is, $\pi \in P_{(\mathscr{P}^{\mathbf{x}}_t)}$ for all $t \in T$, whence $\pi = 1$. ■

Proposition 5.7.9. *Suppose $\ell \geqslant 2$, $P \in \{A_k, S_k\}$ and $|T|^{\ell-1} < k \leqslant |T|^{\ell} - 3$. Then $b(G) = \ell + 1$ and $\Sigma(G)$ is not G-arc-transitive.*

Proof. We see that $b(G) = \ell+1$ by combining Theorem 5.2.3(iii) and Lemma 5.7.8, so it suffices to show that $\Sigma(G)$ is not G-arc-transitive.

First assume $k = |T|^\ell - 3$. Then $|\mathscr{P}_t^{\mathbf{x}}| \in \{|T|^{\ell-1}-1, |T|^{\ell-1}\}$ for all $t \in T$, whereas $|\mathscr{P}_1^{\mathbf{a}_1}| = |T|^{\ell-1}-3$. Hence by Lemma 5.7.1, $(D, D\mathbf{x})$ and $(D, D\mathbf{a}_1)$ are arcs of $\Sigma(G)$ lying in distinct G-orbits.

Now assume $k \neq |T|^\ell - 3$, and let $t_1, t_2 \in T \setminus S$ be as in (P4) of Lemma 5.7.5. Define $\mathbf{y} \in \mathrm{Inn}(T)^k$ by setting

$$\mathscr{P}_{t_1}^{\mathbf{y}} = \mathscr{P}_{t_2}^{\mathbf{x}},\ \mathscr{P}_{t_2}^{\mathbf{y}} = \mathscr{P}_{t_1}^{\mathbf{x}},\ \text{and } \mathscr{P}_t^{\mathbf{y}} = \mathscr{P}_t^{\mathbf{x}} \text{ for } t \in T \setminus \{t_1, t_2\}.$$

By repeating the above argument, we see that D and $D\mathbf{y}$ are adjacent in $\Sigma(G)$. Suppose that $D\mathbf{x}$ and $D\mathbf{y}$ lie in a common G_D-orbit. Then Lemma 5.7.1 implies that $|\mathscr{P}_t^{\mathbf{x}}| = |\mathscr{P}_t^{\mathbf{y}}|$ for all $t \in T$, which is incompatible with (P4). This gives $|\mathscr{P}_{t_1}^{\mathbf{x}}| \neq |\mathscr{P}_{t_2}^{\mathbf{x}}| = |\mathscr{P}_{t_1}^{\mathbf{y}}|$. ■

5.7.3 The groups with $|T|^\ell - 2 \leqslant k \leqslant |T|^\ell$

Lemma 5.7.10. *Suppose $\ell \geqslant 2$, $|T|^\ell - 2 \leqslant k \leqslant |T|^\ell$, $P \in \{A_k, S_k\}$ and $S_k \not\leqslant G$. Then $b(G) = \ell+1$ and $\Sigma(G)$ is not G-arc-transitive.*

Proof. First note by [13, Theorem 1.2] that T has a conjugacy class C such that for any $x, y \in T^\#$, there exists $z \in C$ with $\langle x, z\rangle = \langle y, z\rangle = T$. Let $x_1, y_1 \in T^\#$ be such that $|x_1|, |y_1|$ and $|z|$ for $z \in C$ are distinct, and let $x_2, y_2 \in C$ be such that $\langle x_1, x_2\rangle = \langle y_1, y_2\rangle = T$. In particular, the setwise stabilisers of $\{x_1, x_2\}$ and $\{y_1, y_2\}$ in $\mathrm{Aut}(T)$ are trivial, and $\{x_1, x_2\}^\alpha \neq \{y_1, y_2\}$ for any $\alpha \in \mathrm{Aut}(T)$.

Let $k = |T|^\ell - m$ with $m \in \{0,1,2\}$ and define $\mathbf{x} = (\varphi_{t_{0,1}}, \ldots, \varphi_{t_{0,k}}) \in \mathrm{Inn}(T)^k$ by setting $|\mathscr{P}_1^{\mathbf{x}}| = |T|^{\ell-1}+1$, $|\mathscr{P}_{x_1}^{\mathbf{x}}| = |T|^{\ell-1}-1$, $|\mathscr{P}_{x_2}^{\mathbf{x}}| = |T|^{\ell-1}-m$, and $|\mathscr{P}_t^{\mathbf{x}}| = |T|^{\ell-1}$ for $t \in T \setminus \{1, x_1, x_2\}$. We also write $T^{\ell-1} = \{\mathbf{b}_1, \ldots, \mathbf{b}_{|T|^{\ell-1}}\}$, where $\mathbf{b}_h = (a_{1,h}, \ldots, a_{\ell-1,h})$, and we may assume $\mathbf{b}_{|T|^{\ell-1}} = (y, \ldots, y)$. Define $\mathbf{a}_i = (\varphi_{t_{i,1}}, \ldots, \varphi_{t_{i,k}}) \in \mathrm{Inn}(T)^k$ for $i \in \{1, \ldots, \ell-1\}$, where

$$t_{i,j} = \begin{cases} a_{i,h} & \text{if } j \text{ is the } h\text{-th smallest number in } \mathscr{P}_t^{\mathbf{x}}; \\ 1 & \text{if } j \text{ is the largest number in } \mathscr{P}_1^{\mathbf{x}}. \end{cases}$$

We claim that $\Delta = \{D, D\mathbf{x}, D\mathbf{a}_1, \ldots, D\mathbf{a}_{\ell-1}\}$ is a base for G.

Suppose $(\alpha, \ldots, \alpha)\pi \in G_{(\Delta)}$. By Lemma 5.2.2, we have $\pi \in P_{\{\mathscr{P}^{\mathbf{x}}\}}$ and $t_{0,j}^\alpha = t_{0,j^\pi}$ for all $j \in [k]$. We first prove that $\alpha = 1$. To see this, note that if $k \in \{|T|^\ell - 2, |T|^\ell - 1\}$, then $\pi \in P_{\{\mathscr{P}_{x_1}^{\mathbf{x}} \cup \mathscr{P}_{x_2}^{\mathbf{x}}\}}$, which implies that $\alpha \in \mathrm{Aut}(T, \{x_1, x_2\})$, and thus $\alpha = 1$ since $\mathrm{Aut}(T, \{x_1, x_2\}) = 1$. Now assume $k = |T|^\ell$. Then $\pi \in P_{\{\mathscr{P}_{x_1}^{\mathbf{x}}\}}$ and thus $\alpha \in C_{\mathrm{Aut}(T)}(x_1)$. Note that for each $i \in \{1, \ldots, \ell-1\}$, we have $|\mathscr{P}_1^{\mathbf{a}_i}| = |T|^{\ell-1}+1$, $|\mathscr{P}_{x_2}^{\mathbf{a}_i}| = |T|^{\ell-1}-1$ and $|\mathscr{P}_t^{\mathbf{a}_i}| = |T|^{\ell-1}$ for $t \in T \setminus \{1, x_2\}$. By arguing as above, we have $t_{i,j}^\alpha = t_{i,j^\pi}$ for all $i \in \{1, \ldots, \ell-1\}$, which implies that $\alpha \in C_{\mathrm{Aut}(T)}(x_2)$, and so $\alpha = 1$ since $\mathrm{Aut}(T, \{x_1, x_2\}) = 1$.

Observe that there exists a unique pair $\{j_1, j_2\}$ of elements in $[k]$ such that $j_1 \neq j_2$ and $t_{i,j_1} = t_{i,j_2}$ for all $i \in \{0, \ldots, \ell-1\}$, where we have $t_{i,j_1} = t_{i,j_2} = 1$. For each i, there exists a unique element $g_i \in T$ such that $t_{i,j} = g_i t_{i,j^\pi}$ for all $j \in [k]$, so $t_{i,j_1^\pi} = t_{i,j_2^\pi} = g_i^{-1}$. Since $\pi \in P_{\{\mathscr{P}_1^{\mathbf{x}}\}}$, it follows that $g_i = 1$ and so $t_{i,j} = t_{i,j^\pi}$ for all $j \in [k]$. It is then easy to see that $\pi \in \langle (j_1, j_2) \rangle$, and thus $\pi = 1$ as G does not contain any transpositions in S_k.

Therefore, Δ is a base for G, and so $b(G) = \ell + 1$. In particular, $(D, D\mathbf{x})$ is an arc in $\Sigma(G)$. Similarly, if $y \in \mathrm{Inn}(T)^k$ is such that $|\mathscr{P}_1^{\mathbf{y}}| = |T|^{\ell-1} + 1$, $|\mathscr{P}_{y_1}^{\mathbf{y}}| = |T|^{\ell-1} - 1$, $|\mathscr{P}_{y_2}^{\mathbf{y}}| = |T|^{\ell-1} - m$, and $|\mathscr{P}_t^{\mathbf{y}}| = |T|^{\ell-1}$ for $t \in T \setminus \{1, y_1, y_2\}$, then $D\mathbf{y}$ is adjacent to D in $\Sigma(G)$. Suppose $(D, D\mathbf{x})$ and $(D, D\mathbf{y})$ are in a common G-orbit and note that

$$\{t : |\mathscr{P}_t^{\mathbf{x}}| = |T|^{\ell-1} + 1\} = \{1\} = \{t : |\mathscr{P}_t^{\mathbf{y}}| = |T|^{\ell-1} + 1\}.$$

Hence, the element $g \in T$ described in Lemma 5.7.1 is the identity, and we have $x_1^\alpha = y_1$ for some $\alpha \in \mathrm{Aut}(T)$, which is incompatible with the assumption $|x_1| \neq |y_1|$. This shows that $(D, D\mathbf{x})$ and $(D, D\mathbf{y})$ are arcs lying in distinct G-orbits. ■

Proposition 5.7.11. *Suppose $\ell \geqslant 2$ and $k \in \{|T|^\ell - 1, |T|^\ell\}$. Then*

$$b(G) = \begin{cases} \ell + 2 & \text{if } S_k \leqslant G; \\ \ell + 1 & \text{otherwise,} \end{cases}$$

and $\Sigma(G)$ is not G-arc-transitive. In addition, if $S_k \leqslant G$ then G is semi-Frobenius.

Proof. The result on base sizes is a combination of Theorem 5.2.3(iii) and Lemma 5.7.10, and so it suffices to show that G is semi-Frobenius if $S_k \leqslant G$. In this setting, the construction in the proof of Lemma 5.7.10 shows that there exists a subset Δ of Ω of size $\ell + 1 = b(G) - 1$ such that $G_{(\Delta)}$ is generated by a transposition. Now apply Corollary 5.7.3. ■

Finally, we consider the case where $k = |T|^\ell - 2$ and $S_k \leqslant G$. The case $\ell = 2$ requires special attention.

Lemma 5.7.12. *Suppose $k = |T|^2 - 2$, $T \in \{A_5, A_6\}$ and $G = T^k.(\mathrm{Out}(T) \times S_k)$. Then $b(G) = 4$ and G is semi-Frobenius. In particular, $\Sigma(G)$ is not G-arc-transitive.*

Proof. From the proof of Lemma 5.7.10, we see that there exists a subset $\Delta \subseteq \Omega$ of size 3 whose pointwise stabiliser in G is generated by a transposition. Hence, in view of Corollary 5.7.3, we only need to show that $b(G) = 4$. By Theorem 5.2.3(iii), it suffices to prove that there is no base for G of size 3.

We argue by contradiction and suppose $\Delta = \{D, D\mathbf{a}_0, D\mathbf{a}_1\}$ is a base for G, where $\mathbf{a}_i = (\varphi_{t_{i,1}}, \ldots, \varphi_{t_{i,k}}) \in \mathrm{Inn}(T)^k$. If $|\mathscr{P}_t^{\mathbf{a}_0}| \geqslant |T| + 1$ for some t, then there exist $j, j' \in \mathscr{P}_t^{\mathbf{a}_0}$ such that $j \neq j'$, $t_{0,j} = t_{0,j'} = t$ and $t_{1,j} = t_{1,j'}$, which implies that $G_{(\Delta)}$ contains the transposition (j, j'). Thus, we may assume that $|\mathscr{P}_t^{\mathbf{a}_0}| \leqslant |T|$ for all $t \in T$. The same argument holds for $\mathbf{a}_1$. It follows that the set

$$X_i = \{t \in T : |\mathscr{P}_t^{\mathbf{a}_i}| = |T|\}$$

has size at least $|T| - 2$, so $|X_i| \in \{|T| - 2, |T| - 1\}$.

First, assume either $|S_0|$ or $|X_1|$ is equal to $|T|-1$, say $|S_0| = |T|-1$ and $1 \notin S_0$. For the same reason as above, for any j, j' such that $j \neq j'$ and $t_{0,j} = t_{0,j'}$, we have $t_{1,j} \neq t_{1,j'}$, otherwise $(j,j') \in G_{(\Delta)}$. This implies that $|X_1| = |T|-2$, and we may assume $T \setminus X_1 = \{1,x\}$ for some $x \neq 1$. Write $\mathbf{c}_j = (t_{0,j}, t_{1,j})$ for $j \in [k]$, noting that

$$\{\mathbf{c}_j : j \in [k]\} = T^2 \setminus \{(1,1),(1,x)\}.$$

That is, $\{\mathbf{c}_j : j \in [k]\}$ is fixed by φ_x setwise, with the componentwise action. This induces a permutation $\pi \in S_k$, where

$$j^\pi = m \text{ if } \mathbf{c}_j^{\varphi_x} = \mathbf{c}_m.$$

In particular, $t_{i,j}^{\varphi_x} = t_{i,j^\pi}$ for each $i \in \{0,1\}$. Then

$$D\mathbf{a}_i^{(\varphi_x,\ldots,\varphi_x)\pi} = D(\varphi_{t^{\varphi_x}_{i,1^{\pi^{-1}}}},\ldots,\varphi_{t^{\varphi_x}_{i,k^{\pi^{-1}}}}) = D(\varphi_{t_{i,1}},\ldots,\varphi_{t_{i,k}}) = D\mathbf{a}_i$$

for each $i \in \{0,1\}$, and so $(\varphi_x,\ldots,\varphi_x)\pi \in G_{(\Delta)}$.

To complete the proof, we may assume $|S_0| = |X_1| = |T|-2$, say $T \setminus S_0 = \{1,x\}$ and $T \setminus X_1 = \{1,y\}$. Write $\mathbf{c}_j = (t_{0,j}, t_{1,j})$ for $j \in [k]$ as above, and observe that

$$T^2 \setminus \{\mathbf{c}_j : j \in [k]\} = \{(1,1),(x,y)\} \text{ or } \{(1,y),(x,1)\}.$$

It is easy to check with the aid of MAGMA that there exists an automorphism $\alpha \in \mathrm{Aut}(T)$ such that $1 \neq \alpha \in C_{\mathrm{Aut}(T)}(x) \cap C_{\mathrm{Aut}(T)}(y)$, or $(x,y)^\alpha = (x^{-1}, y^{-1})$.

Assume $\alpha \neq 1$ and $(x,y)^\alpha = (x,y)$. Then $\{\mathbf{c}_j : j \in [k]\}$ is fixed by α setwise, with the componentwise action. Once again, α induces a permutation $\pi \in S_k$, where

$$j^\pi = m \text{ if } \mathbf{c}_j^\alpha = \mathbf{c}_m.$$

Then by arguing as above, we deduce that $(\alpha,\ldots,\alpha)\pi \in G_{(\Delta)}$.

Finally, assume $(x,y)^\alpha = (x^{-1},y^{-1})$ and note that

$$\{\mathbf{c}_j : j \in [k]\}^\alpha = \{(x^{-1},y^{-1})\mathbf{c}_j : j \in [k]\}.$$

Here α also induces a permutation $\pi \in S_k$, where

$$j^\pi = m \text{ if } \mathbf{c}_j^\alpha = (x^{-1},y^{-1})\mathbf{c}_m,$$

and thus $t_{0,j}^\alpha = x^{-1}t_{0,j^\pi}$ and $t_{1,j}^\alpha = y^{-1}t_{1,j^\pi}$ for all $j \in [k]$, noting that $\pi \neq 1$ if $\alpha = 1$. Now we have

$$D\mathbf{a}_0^{(\alpha,\ldots,\alpha)\pi} = D(\varphi_{t^{\alpha}_{i,1^{\pi^{-1}}}},\ldots,\varphi_{t^{\alpha}_{i,k^{\pi^{-1}}}}) = D(\varphi_{x^{-1}}\varphi_{t_{i,1}},\ldots,\varphi_{x^{-1}}\varphi_{t_{i,k}}) = D\mathbf{a}_0$$

and similarly, $D\mathbf{a}_1^{(\alpha,\ldots,\alpha)\pi} = D\mathbf{a}_1$. This completes the proof. ■

Proposition 5.7.13. *If $P \in \{A_k, S_k\}$ and $k = |T|^2 - 2$, then*

$$b(G) = \begin{cases} 4 & \text{if } T \in \{A_5, A_6\} \text{ and } G = T^k.(\mathrm{Out}(T) \times S_k); \\ 3 & \text{otherwise.} \end{cases}$$

Moreover, $\Sigma(G)$ is not G-arc-transitive.

Proof. By Lemmas 5.7.10 and 5.7.12, we may assume that $S_k \leqslant G$, and G is not $T^k.(\mathrm{Out}(T) \times S_k)$ if $T \in \{A_5, A_6\}$. That is, $G = T^k.(O \times S_k)$ for some $O \leqslant \mathrm{Out}(T)$, with $O \neq \mathrm{Out}(T)$ if $T \in \{A_5, A_6\}$. We will prove the result by construction.

Write $K = \mathrm{Inn}(T).O \leqslant \mathrm{Aut}(T)$. In view of Lemma 5.6.5, there exist $x, y \in T$ such that $|x| \neq |y|$, $C_K(x) \cap C_K(y) = 1$ and there is no $\alpha \in K$ with $(x,y)^\alpha = (x^{-1}, y^{-1})$. Define $\mathbf{x} = (\varphi_{t_{0,1}}, \dots, \varphi_{t_{0,k}}) \in \mathrm{Inn}(T)^k$ by setting $|\mathscr{P}_1^{\mathbf{x}}| = |\mathscr{P}_x^{\mathbf{x}}| = |T| - 1$, and $|\mathscr{P}_t^{\mathbf{x}}| = |T|$ if $t \in T \setminus \{1, x\}$. And we label the elements in T by $T = \{g_1, \dots, g_{|T|}\}$, where $g_1 = 1$ and $g_{|T|} = y$. Now define $\mathbf{y} = (\varphi_{t_{1,1}}, \dots, \varphi_{t_{1,k}}) \in \mathrm{Inn}(T)^k$ by setting

$$t_{1,j} = \begin{cases} g_h & \text{if } t \neq 1 \text{ and } j \text{ is the } h\text{-th smallest number in } \mathscr{P}_t^{\mathbf{x}}; \\ g_{h+1} & \text{if } j \text{ is the } h\text{-th smallest number in } \mathscr{P}_1^{\mathbf{x}}. \end{cases}$$

Note by Lemma 5.7.1 that $(D, D\mathbf{x})$ and $(D, D\mathbf{y})$ are in distinct G-orbits (as $|x| \neq |y|$), so it suffices to show that $\Delta = \{D, D\mathbf{x}, D\mathbf{y}\}$ is a base for G.

Suppose $(\alpha, \dots, \alpha)\pi \in G_{(\Delta)}$, noting that $\alpha \in K$. By Lemma 5.2.2(i), we have $\pi \in P_{\{\mathscr{P}^{\mathbf{x}}\}}$, so either $\pi \in P_{\{\mathscr{P}_1^{\mathbf{x}}\}} \cap P_{\{\mathscr{P}_x^{\mathbf{x}}\}}$, or $(\mathscr{P}_1^{\mathbf{x}})^\pi = \mathscr{P}_x^{\mathbf{x}}$, hence there are two cases to consider.

First assume that $(\mathscr{P}_1^{\mathbf{x}})^\pi = \mathscr{P}_x^{\mathbf{x}}$. There exists a unique $g \in T$ such that $t_{0,j}^\alpha = g t_{0,j^\pi}$ for all $j \in [k]$, and by taking $j \in \mathscr{P}_1^{\mathbf{x}}$ we have $g = x^{-1}$. This implies that $x^\alpha = x^{-1}$ by taking $j \in \mathscr{P}_x^{\mathbf{x}}$. Note that $|\mathscr{P}_1^{\mathbf{y}}| = |\mathscr{P}_y^{\mathbf{y}}| = |T| - 1$, and $|\mathscr{P}_t^{\mathbf{y}}| = |T|$ if $t \notin \{1, y\}$. By arguing as above, either $\pi \in P_{\{\mathscr{P}_1^{\mathbf{y}}\}} \cap P_{\{\mathscr{P}_y^{\mathbf{y}}\}}$ or $(\mathscr{P}_1^{\mathbf{y}})^\pi = \mathscr{P}_y^{\mathbf{y}}$. If the former holds, then

$$(\mathscr{P}_1^{\mathbf{x}} \cap \mathscr{P}_1^{\mathbf{y}})^\pi = \mathscr{P}_x^{\mathbf{x}} \cap \mathscr{P}_1^{\mathbf{y}}.$$

However, as can be seen from the definitions of $\mathbf{x}$ and $\mathbf{y}$, we have $|\mathscr{P}_1^{\mathbf{x}} \cap \mathscr{P}_1^{\mathbf{y}}| = 0$, while $|\mathscr{P}_x^{\mathbf{x}} \cap \mathscr{P}_1^{\mathbf{y}}| = 1$. This implies that $(\mathscr{P}_1^{\mathbf{y}})^\pi = \mathscr{P}_y^{\mathbf{y}}$, so $y^\alpha = y^{-1}$ as above. By our assumptions on x and y, there is no $\alpha \in K$ with $(x,y)^\alpha = (x^{-1}, y^{-1})$, which gives a contradiction.

Finally, suppose that $\pi \in P_{\{\mathscr{P}_1^{\mathbf{x}}\}} \cap P_{\{\mathscr{P}_x^{\mathbf{x}}\}}$. First note that $t_{0,j}^\alpha = t_{0,j^\pi}$ for all $j \in [k]$, so $x^\alpha = x$. Similarly, we have $\pi \in P_{\{\mathscr{P}_1^{\mathbf{y}}\}} \cap P_{\{\mathscr{P}_y^{\mathbf{y}}\}}$ and $y^\alpha = y$. This implies that $\alpha \in C_K(x) \cap C_K(y) = 1$, and thus $t_{i,j} = t_{i,j^\pi}$ for all $i \in \{0,1\}$ and $j \in [k]$, which yields $\pi = 1$ and completes the proof. ■

Proposition 5.7.14. *If $\ell \geqslant 3$, $k = |T|^\ell - 2$ and $P \in \{A_k, S_k\}$, then $b(G) = \ell + 1$ and $\Sigma(G)$ is not G-arc-transitive.*

Proof. First note that there exist $x, y, z \in T$ such that $|x| \neq |y|$,

$$C_{\mathrm{Aut}(T)}(x) \cap C_{\mathrm{Aut}(T)}(y) \cap C_{\mathrm{Aut}(T)}(z) = 1$$

and there is no $\alpha \in \mathrm{Aut}(T)$ with

$$(x,y,z)^{\alpha} = (x^{-1},y^{-1},z^{-1}).$$

To see this, if $T \notin \{A_5,A_6\}$ then we apply Lemma 5.6.5, and if $T \in \{A_5,A_6\}$ then it can be checked using MAGMA. Define $\mathbf{x} = (\varphi_{t_{0,1}},\dots,\varphi_{t_{0,k}}) \in \mathrm{Inn}(T)^k$ by setting $|\mathscr{P}_1^{\mathbf{x}}| = |\mathscr{P}_x^{\mathbf{x}}| = |T|^{\ell-1}-1$ and $|\mathscr{P}_t^{\mathbf{x}}| = |T|^{\ell-1}$ if $t \notin \{1,x\}$. Write $T^{\ell-1} = \{\mathbf{b}_1,\dots,\mathbf{b}_{|T|^{\ell-1}}\}$, where $\mathbf{b}_h = (a_{1,h},\dots,a_{\ell-1,h})$, and we may assume $\mathbf{b}_1 = (1,\dots,1)$ and $\mathbf{b}_{|T|^{\ell-1}} = (y,z,\dots,z)$. Now define $\mathbf{a}_i = (\varphi_{t_{i,1}},\dots,\varphi_{t_{i,k}})$ for $i \in \{1,\dots,\ell-1\}$, where

$$t_{i,j} = \begin{cases} a_{i,h} & \text{if } t \neq 1 \text{ and } j \text{ is the } h\text{-th smallest number in } \mathscr{P}_t^{\mathbf{x}}; \\ a_{i,h+1} & \text{if } j \text{ is the } h\text{-th smallest number in } \mathscr{P}_1^{\mathbf{x}}. \end{cases}$$

We claim that $\Delta = \{D,D\mathbf{x},D\mathbf{a}_1,\dots,D\mathbf{a}_{\ell-1}\}$ is a base for G.

We argue as in the proof of Proposition 5.7.13. Suppose $(\alpha,\dots,\alpha)\pi \in G_{(\Delta)}$, noting that $\pi \in P_{\{\mathscr{P}^{\mathbf{x}}\}}$ by Lemma 5.2.2(i). It follows that either $\pi \in P_{\{\mathscr{P}_1^{\mathbf{x}}\}} \cap P_{\{\mathscr{P}_x^{\mathbf{x}}\}}$ or $(\mathscr{P}_1^{\mathbf{x}})^{\pi} = \mathscr{P}_x^{\mathbf{x}}$.

First assume that $(\mathscr{P}_1^{\mathbf{x}})^{\pi} = \mathscr{P}_x^{\mathbf{x}}$. Note that there exists a unique $g \in T$ such that $t_{0,j}^{\alpha} = gt_{0,j^{\pi}}$ for all $j \in [k]$. Now $g = x^{-1}$ by taking $j \in \mathscr{P}_1^{\mathbf{x}}$, and thus $x^{\alpha} = x^{-1}$ by taking $j \in \mathscr{P}_x^{\mathbf{x}}$. Note that $|\mathscr{P}_1^{\mathbf{a}_1}| = |\mathscr{P}_y^{\mathbf{a}_1}| = |T|^{\ell-1}-1$, and $|\mathscr{P}_t^{\mathbf{a}_1}| = |T|^{\ell-1}$ if $t \notin \{1,y\}$. By applying Lemma 5.2.2(i) again, we have either $\pi \in P_{\{\mathscr{P}_1^{\mathbf{a}_1}\}} \cap P_{\{\mathscr{P}_y^{\mathbf{a}_1}\}}$ or $(\mathscr{P}_1^{\mathbf{a}_1})^{\pi} = \mathscr{P}_y^{\mathbf{a}_1}$. If $\pi \in P_{\{\mathscr{P}_1^{\mathbf{a}_1}\}} \cap P_{\{\mathscr{P}_y^{\mathbf{a}_1}\}}$, then

$$(\mathscr{P}_1^{\mathbf{x}} \cap \mathscr{P}_1^{\mathbf{a}_1})^{\pi} = \mathscr{P}_x^{\mathbf{x}} \cap \mathscr{P}_1^{\mathbf{a}_1},$$

which is impossible since $|\mathscr{P}_1^{\mathbf{x}} \cap \mathscr{P}_1^{\mathbf{a}_1}| = |T|^{\ell-2}-1$, while $|\mathscr{P}_x^{\mathbf{x}} \cap \mathscr{P}_1^{\mathbf{a}_1}| = |T|^{\ell-2}$. Hence, we have $(\mathscr{P}_1^{\mathbf{a}_1})^{\pi} = \mathscr{P}_y^{\mathbf{a}_1}$, and thus $y^{\alpha} = y^{-1}$ with the same argument as above. Now suppose $m \geqslant 2$, noting that $|\mathscr{P}_1^{\mathbf{a}_m}| = |\mathscr{P}_z^{\mathbf{a}_m}| = |T|^{\ell-1}-1$, and $|\mathscr{P}_t^{\mathbf{a}_i}| = |T|^{\ell-1}$ if $t \notin \{1,z\}$. By arguing as above, we have $z^{\alpha} = z^{-1}$. However, by our assumptions on x, y and z, there is no automorphism of T simultaneously inverting all three elements, which gives a contradiction.

It follows that $\pi \in P_{\{\mathscr{P}_1^{\mathbf{x}}\}} \cap P_{\{\mathscr{P}_x^{\mathbf{x}}\}}$, and with a similar argument we deduce that $\pi \in P_{\{\mathscr{P}_1^{\mathbf{a}_1}\}}$ and $\pi \in P_{\{\mathscr{P}_1^{\mathbf{a}_m}\}}$. Hence, $t_{i,j}^{\alpha} = t_{i,j^{\pi}}$ for all $i \in \{0,\dots,\ell-1\}$ and $j \in [k]$. This implies that

$$\alpha \in C_{\mathrm{Aut}(T)}(x) \cap C_{\mathrm{Aut}(T)}(y) \cap C_{\mathrm{Aut}(T)}(z),$$

so $\alpha = 1$. Moreover, note that if $j,j' \in \mathscr{P}_t^{\mathbf{x}}$ for some $t \in T$ and $j \neq j'$, then there exists $i \in \{1,\dots,\ell-1\}$ such that $t_{i,j} \neq t_{i,j'}$. Hence, $\pi = 1$ and so Δ is a base for G. Therefore, $b(G) = \ell+1$, as desired.

Finally, we see that $(D,D\mathbf{x})$ and $(D,D\mathbf{a}_1)$ are in distinct G-orbits by Lemma 5.7.1 since $|x| \neq |y|$. This shows that $\Sigma(G)$ is not G-arc-transitive and completes the proof. ■

5.7.4 Concluding remarks

As explained in Remark 5.8, we conclude that the proofs of Theorems 5.1 and 5.3 are complete, which are obtained by combining Theorems 5.2.3(i) and 5.5.1 for the groups with $P \notin \{A_k,S_k\}$, and the relevant results for the groups with $P \in \{A_k,S_k\}$ as recorded in Table 5.1, noting that Theorem 5.2 has been proved in Section 5.5.

To complete the proof of Theorem 5.4 (see Remark 5.8), we establish the following lemma.

Lemma 5.7.15. *Suppose $P \in \{A_k, S_k\}$, $|T|^{\ell-1}+3 \leqslant k \leqslant |T|^{\ell}$ for some $\ell \geqslant 1$ and $b(G)=\ell+1$. Then G is not semi-Frobenius.*

Proof. If $\ell = 1$ then $b(G)=2$ and so G is not semi-Frobenius (see Lemma 3.1.1(iii)). Hence, we assume $\ell \geqslant 2$, and so $A_k \leqslant G$ by Corollary 5.2.6. Let $\mathbf{x} := (1,\dots,1,\varphi_x) \in \mathrm{Inn}(T)^k$ for some $x \in T^{\#}$. It suffices to show that $\Delta := \{D, D\mathbf{x}, D\mathbf{a}_1, \dots, D\mathbf{a}_{\ell-1}\}$ is not a base for any choices of $\mathbf{a}_i := (\varphi_{t_{i,1}},\dots,\varphi_{t_{i,k}}) \in \mathrm{Inn}(T)^k$.

For each $j \in [k]$, let $\mathbf{c}_j := (t_{1,j},\dots,t_{\ell-1,j}) \in T^{\ell-1}$. Note that $k-1 \geqslant |T|^{\ell-1}+2$. This implies that either there exist $j_1,j_2,j_3 \in [k-1]$ such that $\mathbf{c}_{j_1} = \mathbf{c}_{j_2} = \mathbf{c}_{j_3}$, or there exist distinct $j_1,j_2 \in [k-1]$ and distinct $j_1',j_2' \in [k-1]$ such that $\mathbf{c}_{j_1} = \mathbf{c}_{j_2} \neq \mathbf{c}_{j_1'} = \mathbf{c}_{j_2'}$. In the former case, $(j_1,j_2,j_3) \in G_{(\Delta)}$, while $(j_1,j_2)(j_1',j_2') \in G_{(\Delta)}$ in the latter case. ■

However, as one may observe, the method in the above proof cannot be extended to the groups with $k = |T|^{\ell-1}+1$ or $|T|^{\ell-1}+2$. Although we are not able to handle these cases in general, we obtain partial results.

Lemma 5.7.16. *Suppose that $S_k \leqslant G$ and $k \in \{|T|^{\ell-1}+1, |T|^{\ell-1}+2\}$ for some $\ell \geqslant 2$. Then G is not semi-Frobenius.*

Proof. Note that $b(G) = \ell+1$ by Proposition 5.7.9. Let $\mathbf{x} := (1,\dots,1,\varphi_x) \in \mathrm{Inn}(T)^k$ for some $x \in T^{\#}$. Again, it suffices to show that $\Delta := \{D, D\mathbf{x}, D\mathbf{a}_1, \dots, D\mathbf{a}_{\ell-1}\}$ is not a base for any choices of $\mathbf{a}_i := (\varphi_{t_{i,1}},\dots,\varphi_{t_{i,k}}) \in \mathrm{Inn}(T)^k$, and without loss of generality, we may assume that $t_{i,k} = 1$ for all i. As before, let $\mathbf{c}_j := (t_{1,j},\dots,t_{\ell-1,j}) \in T^{\ell-1}$ for each $j \in [k]$.

It is easy to see that if $k = |T|^{\ell-1}+2$, then there exist distinct $j,j' \in [k-1]$ such that $\mathbf{c}_j = \mathbf{c}_{j'}$. Thus $(j,j') \in G_{(\Delta)}$, and Δ is not a base for G.

To complete the proof, we assume that $k = |T|^{\ell-1}+1$. Arguing as above, we may also assume that $\mathbf{c}_1,\dots,\mathbf{c}_{k-1}$ are all distinct, otherwise there is a transposition in $G_{(\Delta)}$. In particular, for each $j \in [k-1]$, we have $\mathbf{c}_j^{\varphi_x} = \mathbf{c}_m$ (acting componentwise) for some $1 \leqslant m \leqslant k-1$, and clearly $\mathbf{c}_k^{\varphi_x} = \mathbf{c}_k$ as $\mathbf{c}_k = (1,\dots,1)$ by our assumption above. Thus φ_x induces a permutation $\pi \in S_k$, where

$$j^{\pi} = m \text{ if } \mathbf{c}_j^{\varphi_x} = \mathbf{c}_m.$$

That is, $t_{i,j}^{\varphi_x} = t_{i,j^{\pi}}$ for each $i \in \{1,\dots,\ell-1\}$ and $j \in [k]$. Now

$$\begin{aligned} D\mathbf{a}_i^{(\varphi_x,\dots,\varphi_x)\pi} &= D(\varphi_{t_{i,1}},\dots,\varphi_{t_{i,k}})^{(\varphi_x,\dots,\varphi_x)\pi} \\ &= D(\varphi_{t_{i,1}^{\varphi_x}},\dots,\varphi_{t_{i,k}^{\varphi_x}})^{\pi} \\ &= D(\varphi_{t_{i,1^{\pi}}},\dots,\varphi_{t_{i,k^{\pi}}})^{\pi} \\ &= D(\varphi_{t_{i,1}},\dots,\varphi_{t_{i,k}}) = D\mathbf{a}_i. \end{aligned}$$

Therefore, $(\varphi_x,\dots,\varphi_x)\pi \in G_{(\Delta)}$, which concludes the proof. ■

5.8 Proof of Theorem 5.6

Although it seems difficult to verify Conjecture II for diagonal type groups in full generality, we consider the case where $P \notin \{A_k, S_k\}$ in this section, which establishes Theorem 5.6. Recall that $b(G) = 2$ in this setting, and we may assume $G = T^k.(\mathrm{Out}(T) \times P)$.

Here we adopt the notation from Section 5.4.2, recalling that $R(G)$ is a set of representatives for the G-conjugacy classes of elements in the stabiliser D in G which have prime order, and defining

$$R_1(G) := \{(\alpha,\dots,\alpha)\pi \in R(G) : \pi \text{ is fixed-point-free on } [k]\},$$
$$R_2(G) := \{(\alpha,\dots,\alpha)\pi \in R(G) : \pi = 1\},$$
$$R_3(G) := \{(\alpha,\dots,\alpha)\pi \in R(G) : \pi \neq 1 \text{ and } \pi \text{ has a fixed point on } [k]\},$$

and

$$r_i(G) := \sum_{x \in R_i(G)} \frac{|x^G \cap D|^2 |C_G(x)|}{|G|}.$$

Recall (2.4.2) that

$$Q(G,2) \leqslant \widehat{Q}(G,2) = r_1(G) + r_2(G) + r_3(G).$$

Thus, in view of Lemma 3.1.3(i), it suffices to show that $r_1(G) + r_2(G) + r_3(G) < 1/2$.

The following lemma is [51, Lemma 4.5].

Lemma 5.8.1. *If $x = (\alpha,\dots,\alpha)\pi$, then*

$$|x^G \cap D| = |\alpha^{\mathrm{Aut}(T)}||\pi^P|.$$

Note that if $(\alpha,\dots,\alpha)\pi$ has prime order and $\pi \neq 1$, then $|\pi|$ is a prime and either $|\alpha| = |\pi|$ or $\alpha = 1$. Define $X_1(G) := \bigcup_{x \in R_1(G)} (x^G \cap D)$. That is (recall that a fixed-point-free permutation is called a *derangement*),

$$X_1(G) = \{(\alpha,\dots,\alpha)\pi \in G : \pi \in P \text{ is a derangement of prime order and } |\alpha| = |\pi| \text{ or } \alpha = 1\}.$$

Then

$$r_1(G) = \sum_{x \in R_1(G)} \frac{|x^G \cap D|^2 |C_G(x)|}{|G|} = \sum_{x \in X_1(G)} \frac{|x^G \cap D||C_G(x)|}{|G|},$$

and by Lemma 5.8.1 we get

$$r_1(G) = \sum_{(\alpha,\dots,\alpha)\pi \in X_1(G)} \frac{|\alpha^{\mathrm{Aut}(T)}||\pi^P||C_G((\alpha,\dots,\alpha)\pi)|}{|G|}. \tag{5.8.1}$$

Now we can apply [51, Lemma 4.6], where it is proved that

$$|C_G((\alpha,\dots,\alpha)\pi)| = |C_P(\pi)||C_{\mathrm{Out}(T)}(\overline{\alpha})||T|^{\frac{k}{|\pi|}}, \tag{5.8.2}$$

where $\overline{\alpha}$ is the image of α in $\mathrm{Out}(T)$. Note that $|C_{\mathrm{Out}(T)}(\overline{\alpha})| \leqslant |\mathrm{Out}(T)|$. Combining (5.8.1) and (5.8.2), we have

$$r_1(G) \leqslant \sum_{\pi \in \Delta(P)} |T|^{\frac{k}{|\pi|}-k} \left(1 + \sum_{\substack{\alpha \in \mathrm{Aut}(T) \\ |\alpha| = |\pi|}} |\alpha^{\mathrm{Aut}(T)}| \right), \tag{5.8.3}$$

where $\Delta(P)$ is the set of derangements in P of prime order. We are now ready to bound $r_1(G)$ from above.

Lemma 5.8.2. *If $(P,k) \neq (S_5,6)$, then $r_1(G) < |T|^{-1}$, and we have $r_1(G) < |T|^{-\frac{1}{6}}$ if $(P,k) = (S_5,6)$.*

Proof. First, let us assume $k > 24$. As noted in the proof of [51, Lemma 4.1], we have

$$r_1(G) \leqslant \frac{|\mathrm{Out}(T)|^2 |P|^2}{|T|^{\lceil \frac{k}{2} \rceil - 2}}$$

and we also note that $|P| < 2^k$ by [100, Corollary 1.2]. By applying the bounds $|T| \geqslant 60$ and $|\mathrm{Out}(T)|^3 < |T|$ (see Lemma 2.2.5), we get

$$r_1(G) \leqslant \frac{|\mathrm{Out}(T)|^2 |P|^2}{|T|^{\lceil \frac{k}{2} \rceil - 2}} < \frac{4^k}{60^{\lceil \frac{k}{2} \rceil - \frac{10}{3}} |T|} < |T|^{-1}.$$

Now assume $k \leqslant 24$. Here we will use the bound given in (5.8.3), which gives

$$\begin{aligned} r_1(G) &\leqslant |T|^{-1} \sum_{\pi \in \Delta(P)} |T|^{\frac{k}{|\pi|}-k+1} \left(1 + \sum_{\substack{\alpha \in \mathrm{Aut}(T) \\ |\alpha| = |\pi|}} |\alpha^{\mathrm{Aut}(T)}| \right) =: |T|^{-1} \varphi(P,T) \\ &< |T|^{-1} \sum_{\pi \in \Delta(P)} |\mathrm{Aut}(T)|^2 |T|^{\frac{k}{|\pi|}-k+1} \\ &< |T|^{-1} \sum_{\pi \in \Delta(P)} |T|^{\frac{k}{|\pi|}-k+\frac{11}{3}} =: |T|^{-1} \phi(P,|T|). \end{aligned} \tag{5.8.4}$$

Assume $(P,k) \neq (S_5,6)$. We have $\frac{11}{3} + k(\frac{1}{p} - 1) < \frac{11}{3} - \frac{k}{2} < 0$ if $k > 7$. For $k \leqslant 7$, one can check using MAGMA that the inequality $\frac{11}{3} + k(\frac{1}{p} - 1) < 0$ is still valid. Thus, $\phi(P,|T|)$ is an increasing function of $|T|$. With the aid of MAGMA, it is routine to check that if $|T| \geqslant 126000 = |\mathrm{U}_3(5)|$, then $\phi(P,|T|) < 1$. For each simple group T with $|T| < 126000$, we use MAGMA to check that $\varphi(P,T) < 1$ and the result follows.

To complete the proof, it suffices to consider the case where $(P,k) = (S_5,6)$. Here there are 30 derangements of prime order in P, 10 of which have order 2, and the remainder have order 3. Then (5.8.4) implies that

$$r_1(G) < 10|T|^{-\frac{1}{3}} + 20|T|^{-\frac{4}{3}} < 10|T|^{-\frac{1}{3}} + \frac{1}{3}|T||T|^{-\frac{4}{3}} < \frac{11}{3}|T|^{-\frac{1}{3}}.$$

In particular, when $|T| \geqslant 1285608 = |\mathrm{L}_2(137)|$, we have $r_1(G) < \frac{11}{3}|T|^{-\frac{1}{3}} < |T|^{-\frac{1}{6}}$. For each simple group T with $|T| < 1285608$, we can use MAGMA to check that $\varphi(P,T) < |T|^{\frac{5}{6}}$, so the result follows. ■

By combining Corollary 5.2.12 and Lemma 5.4.13, we obtain the following upper bound on $r_2(G)$.

Lemma 5.8.3. *We have* $r_2(G) < 10^{4-k}$.

Finally, we obtain a bound on $r_3(G)$. To do this, we first extend [51, Lemma 4.4] with the following technical result.

Lemma 5.8.4. *Suppose* $k \geqslant 11$*, or* $5 \leqslant k \leqslant 10$ *and* $|T| \geqslant |\mathrm{L}_2(431)| = 40031280$*. Then*

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

where $R(P)$ *is a set of representatives for the conjugacy classes of prime order elements in* P*, and* r_π *denotes the number of orbits of* π *on* $[k]$*.*

Proof. Note that if $k - r_\pi \leqslant \frac{5}{3}$ then $k - r_\pi = 1$, so π is a transposition, which forces $P = S_k$ by a classical result of Jordan [75] (that is, a primitive group of degree k that contains a transposition is always S_k) and is incompatible with our assumption. Thus, $k - r_\pi \geqslant 2$, and hence it is easy to check the desired result holds if $5 \leqslant k \leqslant 10$ and $|T| \geqslant |\mathrm{L}_2(431)| = 40031280$.

From now on, assume $k \geqslant 11$. Observe that the lemma holds if we can show that

$$\sum_{\pi \in R(P)} \frac{k|\pi^P|}{60^{k-r_\pi-\frac{5}{3}}} < 1. \tag{5.8.5}$$

First assume $11 \leqslant k \leqslant 24$. The group P can be accessed via the primitive group database of MAGMA [10], so one can verify that (5.8.5) holds by checking each group in turn.

Next, we consider the cases where $k > 24$. Then by [100, Corollary 1.2], we have $|P| < 2^k$. By arguing as in the proof of [51, Lemma 4.4], the lemma holds if

$$\frac{k|P|}{|T|^{\frac{\mu(P)}{2}-\frac{5}{3}}} < 1, \tag{5.8.6}$$

where $\mu(P)$ is the *minimal degree* of P (the smallest number of points in $[k]$ moved by any non-identity element in P).

Let us first assume $\mu(P) \geqslant 3k/7$. Then

$$\frac{k|P|}{|T|^{\frac{\mu(P)}{2}-\frac{5}{3}}} \leqslant \frac{k2^k}{360^{\frac{3k}{14}-\frac{5}{3}}} \leqslant 360^{\frac{5}{3}} k \left(\frac{2}{360^{\frac{3}{14}}}\right)^k < 1$$

for $|T| \geqslant 360 = |A_6|$, and so (5.8.6) holds. Similarly, we can eliminate the cases where $T = A_5$ and $k \geqslant 60$, or $T = \mathrm{PSL}_2(7)$ and $k \geqslant 30$. For the remaining cases, we can check the lemma directly with the aid of MAGMA.

It suffices to consider the case where $\mu(P) < 3k/7$ and $k > 24$, so by [64, Corollary 1] we have $k = \binom{m}{\ell}^r$, $m \geqslant 5$, $r \geqslant 1$ and

$$A_m^r \trianglelefteqslant P \leqslant S_m \wr S_r,$$

identifying $[k]$ with Γ^r, where Γ is the set of subsets of $\{1,\dots,m\}$ of size ℓ with $1 \leqslant \ell < m/2$. We divide the proof into three cases.

Case 1. $(r,\ell) \neq (1,2)$ *or* $(2,1)$.

Following the proof of [51, Lemma 4.4], we set

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

and so (5.8.5) holds if

$$3mr\log m + r\log r \leqslant \left(g(m,r,\ell) - \frac{5}{3}\right)\log 60. \tag{5.8.7}$$

As noted in the proof of [51, Lemma 4.4], if $r \geqslant 3$ then $g(m,r,\ell) \geqslant m^{r-1}$; if $r = 2$ and $\ell \geqslant 2$ then $g(m,2,\ell) \geqslant m^2$; and if $r = 1$ and $\ell \geqslant 3$ then $g(m,r,\ell) \geqslant (m-3)^2/2$. Using these bounds, we see that (5.8.7) holds unless $m \leqslant 8$, $r = 1$ and $\ell \geqslant 3$ (note that the conditions $\ell < m/2$ and $k > 24$ yield $m \geqslant 7$ and $\ell = 3$). If $m = 8$ then we see that (5.8.7) still holds by inputting the exact value $g(m,r,\ell) = 15$, while for $m = 7$ we can check that (5.8.5) holds.

Case 2. $(r,\ell) = (1,2)$.

In this case, $P = A_m$ or S_m. As noted in the proof of [51, Lemma 4.2], we have $f_p(S_m) < \frac{m^2}{2}$, where $f_p(X)$ is the number of conjugacy classes of elements of prime order in a group X, which implies that $f_p(P) \leqslant m^2$ by [51, Lemma 4.7]. Note that $k = \binom{m}{2} < m^2$, so we only need to show that $|\pi^P| 60^{\frac{5}{3}+r_\pi - k} \leqslant m^{-4}$ for each $\pi \in P$ of prime order. By arguing as in the proof of [51, Lemma 4.4], it suffices to show that

$$\left(1+\frac{4}{pt}\right)\log m + pt + 1 + \frac{20}{3pt} + s < 2m \tag{5.8.8}$$

for all primes $p \leqslant m$ and integers t such that $1 \leqslant t \leqslant m/p$, where $s = 0$ if $p \geqslant 3$ and $s = 2/p$ if $p = 2$. Assume $m \geqslant 12$, so $3\log m \leqslant m$. When $pt \geqslant 4$, we have

$$\left(1+\frac{4}{pt}\right)\log m + pt + 1 + \frac{20}{3pt} + s < \frac{2}{3}m + m + \frac{11}{3} < 2m$$

and so (5.8.8) is satisfied. One can also check that (5.8.8) holds if $pt \leqslant 3$ (where we have $p \in \{2,3\}$ and $t = 1$). Now assume $m < 12$. Note that $m \geqslant 8$ since $k = \binom{m}{2} \geqslant 25$. Then it is easy to check that (5.8.8) holds in each case with $m \geqslant 9$. For $m = 8$, we can check that (5.8.5) holds.

Case 3. $(r,\ell) = (2,1)$.

To complete the proof, we move to the case where $(r,\ell) = (2,1)$, so $A_m^2 \trianglelefteqslant P \leqslant S_m^2{:}S_2 =: Q$. Here we adopt the notation in the proof of [51, Lemma 4.4], where $\mathscr{C}$ and $\mathscr{C}_\tau$ are the unions of elements of prime order in S_m^2 and $Q \setminus S_m^2$, respectively. As noted in the proof of [51, Lemma 4.4], $\mathscr{C} \cap P$ and $\mathscr{C}_\tau \cap P$ comprise at most $3m^3$ and 8 conjugacy classes of P, respectively. Note that $m = \sqrt{k}$, so in order to prove (5.8.5), it suffices to show that $|\pi^P|60^{\frac{5}{3}+r_\pi-k}$ is less than $\frac{1}{3}m^{-5}$ for all $\pi \in R(P)\cap\mathscr{C}$, and at most $\frac{1}{8}m^{-2}$ for all $\pi \in R(P)\cap\mathscr{C}_\tau$.

For the latter, we have $|\pi^P| \leqslant m^{m-1}$ and $k-r_\pi = \frac{1}{2}(m^2-m)$ as noted in the proof of [51, Lemma 4.4], where $\pi \in \mathscr{C}_\tau \cap P$. Since $\log 60 > 4$, it suffices to prove that

$$(m+1)\log m < 2(m^2-m)-\frac{29}{3}.$$

This is obvious since $\log m < m-1$.

Finally, let $\pi = (s_1,s_2) \in \mathscr{C}\cap P$ be of order p, and let f_π be the number of fixed points of π on $[k]$. As noted in the proof of [51, Lemma 4.4], we have $f_\pi = (m-pt_1)(m-pt_2)$ for some $0 \leqslant t_1,t_2 \leqslant m/p$ and t_1 or t_2 is non-zero. We also have $k-r_\pi \geqslant (k-f_\pi)/2$. Thus, in order to prove that $|\pi^P|60^{\frac{5}{3}+r_\pi-k} \leqslant \frac{1}{3}m^{-5}$, it suffices to show that

$$(pt_1+pt_2+5)\log m + 2p^2t_1t_2 < 2m(pt_1+pt_2)-\frac{5}{6}\log 60-\log 6. \tag{5.8.9}$$

Note that $pt_1+pt_2 \geqslant 2$ and $2p^2t_1t_2 \leqslant mp(t_1+t_2)$ (see the proof of [51, Lemma 4.4]). This implies that (5.8.9) holds for $m \geqslant 10$ as we have $3\log m < m$. We now complete the proof by noting that (5.8.9) holds for $7 \leqslant m \leqslant 9$, while (5.8.5) holds for $m = 5,6$. ■

Lemma 5.8.5. *We have* $r_3(G) < |T|^{-\frac{1}{3}}k^{-1}$.

Proof. As noted in the proof of [51, Lemma 4.3], we have

$$r_3(G) \leqslant \frac{|\mathrm{Out}(T)||P|}{|G|}|T|^{\frac{4}{3}} \sum_{\pi\in R(P)} |\pi^P||T|^{r_\pi}, \tag{5.8.10}$$

where $R(P)$ and r_π are as in the statement of Lemma 5.8.4. Thus, by Lemma 5.8.4, the desired bound holds if $k \geqslant 11$, or if $k \leqslant 10$ and $|T| \geqslant 40031280$. For the groups with $k \leqslant 10$ and $|T| < 40031280$, one can check with the aid of MAGMA that the left-hand side of (5.8.10) is less than $|T|^{-\frac{1}{3}}k^{-1}$. ■

We are now in a position to prove Theorem 5.6, which is our final main result on diagonal type groups.

Proof of Theorem 5.6. As noted above, it suffices to show that $r_1(G)+r_2(G)+r_3(G) < 1/2$. If $(P,k) \neq (S_5,6)$ then

$$r_1(G)+r_2(G)+r_3(G) < |T|^{-1}+10^{4-k}+|T|^{-\frac{1}{3}}k^{-1} \leqslant \frac{1}{60}+\frac{1}{10}+\frac{1}{5\cdot 60^{1/3}} < \frac{1}{2}$$

by Lemmas 5.8.2, 5.8.3 and 5.8.5. Similarly, if $(P,k) = (S_5,6)$, then

$$r_1(G)+r_2(G)+r_3(G) < |T|^{-\frac{1}{6}}+\frac{1}{100}+\frac{1}{6\cdot 60^{1/3}} < \frac{1}{2}$$

if $T \neq A_5$, and for $T = A_5$ the result follows by computing precise values of $r_i(G)$. ■

5.9 Remarks on primitive twisted wreath products

We conclude this chapter by establishing Conjecture II and resolving Problem III for some primitive twisted wreath products (see type V of Table 2.1). Throughout, let T be a non-abelian simple group, $P \leqslant S_k$ be a primitive group on $[k]$, and let $G = T^k{:}P$ be a primitive twisted wreath product. Here $b(G) = 2$ by [50, Theorem 1.1].

Theorem 5.9.1. *Any two vertices in $\Sigma(G)$ have a common neighbour.*

Proof. In view of Lemma 3.1.3(i), it suffices to show that $Q(G,2) < 1/2$. By [50, Lemma 5.5], we have

$$Q(G,2) < \sum_{\pi\in R(P)} \frac{|\pi^P|}{|T|^{k-r_\pi}}, \tag{5.9.1}$$

where $R(P)$ is a set of representatives for the conjugacy classes of prime order elements in P, and r_π denotes the number of orbits of π on $[k]$.

If $P \notin \{A_k, S_k\}$ and $k \geqslant 11$, then we see that $Q(G,2) < 1/2$ by applying (5.9.1) and Lemma 5.8.4. One can check using MAGMA that if $P \notin \{A_k, S_k\}$ and $k \leqslant 10$ then

$$\sum_{\pi\in R(P)} \frac{|\pi^P|}{60^{k-r_\pi}} < \frac{1}{2},$$

which shows that $Q(G,2) < 1/2$ by (5.9.1). Finally, if $P \in \{A_k, S_k\}$ then $k \geqslant 6$ and $T = A_{k-1}$ by [50, Lemma 4.8], and

$$\sum_{\pi\in R(P)} \frac{|\pi^P|}{|T|^{k-r_\pi}} < |T|^{-\frac{1}{3}} \cdot \left(\frac{k(k-1)}{(k-1)!^{\frac{2}{3}}2^{\frac{1}{3}}} + \frac{2^{\frac{5}{3}}k}{(k-1)!^{\frac{2}{3}}}\right)$$

as remarked in the proof of [50, Theorem 5.1]. This shows that $Q(G,2) < 1/2$ for these groups, which completes the proof. ■

Theorem 5.9.2. *We have* $\mathrm{reg}(G) \geqslant 2$. *In particular, $\Sigma(G)$ is not G-arc-transitive.*

Proof. As can be seen in the proof of Theorem 5.9.1, we have $Q(G,2) < 1/2$, so in view of Lemma 3.3.6, it suffices to show that $2|P| < |T|^k$. If $P \notin \{A_k, S_k\}$, then this is given by the main theorem of [105], which shows that $|P| < 4^k$. And if $P \in \{A_k, S_k\}$ then $T = A_{k-1}$ by [50, Lemma 4.8], and hence one can show that $2|P| < |T|^k$ immediately. This shows that $\mathrm{reg}(G) > 1$. The statement concerning $\Sigma(G)$ follows from Lemma 3.1.2. ■

Chapter 6

Product type groups

The work in this chapter is heavily drawn from the papers

> T.C. Burness and H.Y. Huang, *On base sizes for primitive groups of product type*, J. Pure Appl. Algebra **227** (2023), Paper No. 107228, 43 pp.
>
> S.D. Freedman, H.Y. Huang, M. Lee and K. Rekvényi, *On the generalised Saxl graphs of permutation groups*, submitted (2024), arXiv:2410.22613.

which are [26] and [52], respectively.

In this final chapter, we consider the product type primitive groups (see type IV of Table 2.1). Here we have $G \leqslant L \wr P$ and Ω can be identified with the Cartesian product Γ^k, where $k \geqslant 2$, $L \leqslant \mathrm{Sym}(\Gamma)$ is a primitive group of type II or III in Table 2.1, and $P \leqslant S_k$ is transitive on $[k]$.

Our main focus will be on the groups of the form $G = L \wr P$, and we will study $b(G)$ and $\mathrm{reg}(G)$ as before, establishing Theorems 6.1, 6.2 and 6.3 below. By studying bases for these groups, we will show that Conjecture II on the generalised Saxl graphs of primitive groups is equivalent to (a priori, stronger) statement (see Conjecture 6.5 below). Finally, we take the first step in studying the base size of G when it is a proper subgroup of $L \wr P$. One of our main results here is Theorem B from Chapter 1, and a detailed statement is given in Theorem 6.6.

Most of the results in this chapter are taken from my joint paper with Burness [26], while the proof of Theorem 6.2 and the results on generalised Saxl graphs for the groups with $b(G) \geqslant 3$ are from my joint paper [52] with Freedman, Lee and Rekvényi.

6.1 Introduction

Recall that if $G \leqslant \mathrm{Sym}(\Omega)$ is a product type primitive group, then $G \leqslant L \wr S_k$ acts on $\Omega = \Gamma^k$ with its product action (see (6.2.1) in Section 6.2.2), where $k \geqslant 2$ and $L \leqslant \mathrm{Sym}(\Gamma)$ is a primitive group with socle T, which is either almost simple or diagonal type (see Table 2.1). Moreover, G has socle T^k and the subgroup $P \leqslant S_k$ induced by the conjugation action of G on the set of factors of T^k is transitive. It follows that $T^k \trianglelefteqslant G \leqslant L \wr P$ and thus $b(G) \leqslant b(L \wr P)$.

Bases for product type groups of the form $G = L \wr P$ are considered by Bailey and Cameron in [6]. In order to state their main result (which imposes no conditions on L or P), let $D(P)$ denote the *distinguishing number* of P, which is the minimal number of parts in a distinguishing partition for the action of P on $\{1,\dots,k\}$ (a partition is a *distinguishing partition* if the intersection of the setwise stabilisers of the parts in P is trivial). In addition, for a positive integer m, let $\mathrm{reg}(L,m)$ be the number of regular orbits of L in its coordinatewise action on Γ^m (note that $\mathrm{reg}(L,b(L)) = \mathrm{reg}(L)$, and $\mathrm{reg}(L,m) \geqslant 1$ if and only if $m \geqslant b(L)$). Then [6, Theorem 2.13] states that

$$b(L \wr P) \leqslant m \textit{ if and only if } \mathrm{reg}(L,m) \geqslant D(P). \tag{6.1.1}$$

In particular, we have $b(L) \leqslant b(L \wr P)$.

In studying product type groups $G \leqslant L \wr P$ as above, there is a natural distinction to make between the full wreath product $L \wr P$ and its proper (primitive) subgroups. Focussing first on the former case, we consider the groups $G = L \wr P$ with soluble point stabiliser H. In this setting, L has soluble point stabilisers, so L is an almost simple group and the precise $b(L)$ (with respect to the action on Γ) has been computed in [14] (in particular $b(L) \leqslant 5$ in every case). Moreover, the solubility of H implies that P is soluble, and so $D(P) \leqslant 5$ by [110, Theorem 1.2]. In view of (6.1.1), we see that $b(L \wr P) = b(L)$ if and only if $\mathrm{reg}(L) \geqslant 5$, and we recall Propositions 4.5.14 and 4.5.19, which determine the groups L with $\mathrm{reg}(L) \leqslant 4$ (see Tables 4.7, 4.8 and 4.9). With these observations in hand, we will prove the following result in Section 6.3.

Theorem 6.1. *Let $G = L \wr P$ be a product type primitive group with soluble point stabiliser $J \wr P$. Then either*

(i) $b(G) = b(L)$; or

(ii) $b(G) = b(L) + 1$, $\mathrm{reg}(L) < D(P)$ and $(L, J, \mathrm{reg}(L))$ is one of the cases in Table 4.7, 4.8 or 4.9.

Now we turn to the problem of classifying the groups $G = L \wr P$ with $\mathrm{reg}(G) = 1$. In order to state the theorem, let $\mathscr{P}_m([k])$ be the set of ordered partitions of $[k]$ into m parts, where some of the parts are allowed to be empty. In Lemma 6.4.5 we will show that $\mathrm{reg}(G) = 1$ if and only if $\mathrm{reg}(L, b(G)) = D(P)$ and P has a unique regular orbit on $\mathscr{P}_{D(P)}([k])$. We are also able to classify the primitive groups satisfying the latter condition (see Proposition 6.4.15), which extends earlier results of Seress [109] and Dolfi [47]. This allows us to establish the following theorem.

Theorem 6.2. *Let $G = L \wr P$ be a product type primitive group, where $P \leqslant S_k$ is primitive. Then* $\mathrm{reg}(G) = 1$ *if and only if* $\mathrm{reg}(L, b(G)) = D(P)$ *and one of the following holds:*

(i) $P = S_k$ *and* $D(P) = k$*;*

(ii) $P = A_5$*,* $k = 6$ *and* $D(P) = 3$*;*

(iii) $P = \mathrm{P\Gamma L}_2(8)$*,* $k = 9$ *and* $D(P) = 3$*; or*

(iv) $P = \mathrm{AGL}_3(2)$*,* $k = 8$ *and* $D(P) = 4$.

For base-two groups, we are able to determine a formula for $\mathrm{reg}(G) = r(G)$ when $G = L \wr P$ (recall that $r(G)$ is the number of regular suborbits of G, and $r(G) \geqslant 1$ if and only if $b(G) \leqslant 2$), which turns out to have some interesting applications. Here t_m denotes the number of (unordered) distinguishing partitions with m non-empty parts for the action of P on $\{1, \dots, k\}$, so $t_m \geqslant 1$ if and only if $D(P) \leqslant m$.

Theorem 6.3. *Let $G = L \wr P$ be a product type primitive group acting on $\Omega = \Gamma^k$. Then*

$$r(G) = \frac{1}{|P|} \sum_{m=D(P)}^{k} m! \binom{r(L)}{m} t_m.$$

In general, it is difficult to compute t_m precisely, but this can be achieved in some special cases, which then allows us to simplify the given expression for $r(G)$. For example, see Corollaries 6.4.3 and 6.4.4. Notice that we have a trivial upper bound $t_m \leqslant S(k, m)$, which is the total number of partitions of $\{1, \dots, k\}$ into m non-empty parts (a Stirling number of the second kind). In fact, this bound is best possible. For instance, if $P = C_k$ has prime order, then $t_m = S(k, m)$ for all $m \geqslant 2$. On the other hand, if $\Pi = \{\pi_1, \dots, \pi_m\}$ is a distinguishing partition for P, then $P_{\{\Pi\}} \leqslant S_m$ is a permutation group on the set of parts comprising Π and thus $t_m \geqslant |P|/m!$. Note that $t_m = |P|/m!$ only if each part has the same size in every distinguishing partition for P into m parts. For example, if $P = S_k$ and $m = k$, then $t_m = 1 = |P|/m!$ since the partition of $\{1, \dots, k\}$ into singletons is the only distinguishing partition for P.

In a different direction, we can use Theorem 6.3 to establish several new results on the Saxl graphs of base-two product type primitive groups. Recall Lemma 3.1.1(iv), which tells us that the valency of the Saxl graph $\Sigma(G)$ for a base-two group G is $\mathrm{val}(G) = r(G)|H|$, where H is a point stabiliser of G. Our main result on the valency of Saxl graphs of product type groups is Corollary 6.4 below, which extends earlier work in [20] and [37]. For part (i), recall that a connected graph is *Eulerian* if and only if every vertex has even degree.

Corollary 6.4. *Let $G = L \wr P$ be a base-two product type primitive group with Saxl graph $\Sigma(G)$. Then the following hold:*

(i) $\Sigma(G)$ *is Eulerian.*

(ii) $\mathrm{val}(G)$ *is a prime power if and only if* $L = \mathrm{M}_{10}$*,* $J = SD_{16}$*,* P *is a* 2*-group and* $t_2 \geqslant 1$ *is a* 2*-power.*

Note that $\mathrm{val}(G)$ is a prime power only if $|H| = |J|^k|P|$ is a prime power, which implies that both J and P are soluble. Let us also observe that there are genuine examples in part (ii), where P is a 2-group and t_2 is a 2-power. For example, if $P = C_8{:}(C_2 \times C_2)$ is the holomorph of the cyclic group C_8 in its natural action on 8 points, then $t_2 = 16$. We refer the reader to Remark 6.5.4 for further comments.

Now we turn to Conjecture II for the generalised Saxl graph $\Sigma(G)$ of a primitive product type group G. By considering this conjecture for primitive wreath products, we will show that it is equivalent to the following (a priori, stronger) statement. Here $N(\alpha)$ is the set of neighbours of α in $\Sigma(G)$, and a G_β-orbit α^{G_β} is called *almost-regular* if $\{\alpha,\beta\}$ can be extended to a base of size $b(G)$ (in particular, a regular G_β-orbit is almost-regular, and $N(\alpha)$ is the union of all almost-regular G_α-orbits).

Conjecture 6.5. *Let* $G \leqslant \mathrm{Sym}(\Omega)$ *be a finite primitive permutation group and let* $\alpha,\beta \in \Omega$*. Then* $N(\alpha)$ *meets every almost-regular* G_β*-orbit on* Ω*.*

We will present some evidence for Conjecture 6.5 in Section 6.5.2. For example, we will show that the conclusion holds for the action of $\mathrm{L}_2(q)$ on the set of pairs of 1-dimensional subspaces of the natural module $\mathbb{F}_q^2$ (see Proposition 6.5.8).

In the final part of the chapter, we consider general product type groups of the form $G \leqslant L \wr P$. The analysis of bases in this setting is significantly more difficult and there are very few (if any) existing results in the literature that are tailored to this particular situation. As a starting point, we determine the base-two groups in certain families of product type primitive groups of the form

$$T \wr P < G < L \wr P \tag{6.1.2}$$

with soluble point stabilisers. Here P is soluble and L is almost simple with soluble point stabilisers. In addition, we may assume G induces L on each copy of Γ in the Cartesian product $\Omega = \Gamma^k$, so both L and P are uniquely determined by G (see Remarks 6.2.4 and 6.2.5).

Our main results are Theorems 6.6.4 and 6.6.11. For instance, the following result in the special case $k = b(L) = 2$ is stated as Theorem 6.6.4 in Section 6.6, which establishes Theorem B in Chapter 1 for the groups with $G < L \wr P$.

Theorem 6.6. *Let* G *be a product type primitive group as in* (6.1.2)*, where* $k = b(L) = 2$ *and* G *has soluble point stabilisers. Then* $b(G) \leqslant 3$*, with equality if and only if* $|L \wr P : G| = 2$ *and one of the following holds, where* J *is a point stabiliser in* L*:*

(i) $(L,J) = (\mathrm{M}_{10}, 5{:}4)$.

(ii) $(L,J) = (\mathrm{J}_2.2, 5^2{:}(4 \times S_3))$.

(iii) $L = \mathrm{PGU}_4(3)$ *and* J *is of type* $\mathrm{GU}_1(3) \wr S_4$.

For the almost simple primitive group L with soluble point stabilisers, note that $b(L \wr S_2) = b(L)$ or $b(L)+1$ by Theorem 6.1, and the latter holds if and only if $r(L) = 1$. Recall that $r(L) = 1$ if and only if L is a base-two group recorded in Table 4.7 (see Theorem 4.5). This gives Theorem B by combining with Theorem 6.6.

Further observations on the base-two problem for general product type primitive groups are presented at the end of Section 6.6.

Let us briefly describe the structure of this chapter. We begin in Section 6.2 by recording some preliminary results that will be needed in the proofs of our main results. This includes work of Seress [109, 110] on the distinguishing number of permutation groups, which we will combine with a key result of Bailey and Cameron [6] on bases for product type groups (see Theorem 6.2.6). Next in Section 6.3 we focus on the product type groups of the form $G = L \wr P$ with soluble point stabilisers and we will prove Theorem 6.1. Our main results on regular suborbits are presented in Section 6.4 and we investigate applications involving the Saxl graphs of product type groups in Section 6.5. Finally, in Section 6.6 we consider general product type groups with $G \leqslant L \wr P$, focussing on the case where G contains P.

6.2 Preliminaries

In this section we record some preliminary results, which will be needed in the proofs of our main theorems. Throughout this section, $G \leqslant \mathrm{Sym}(\Omega)$ denotes a finite transitive permutation group of degree n with point stabiliser H.

6.2.1 Distinguishing number

Let $\Pi = \{\pi_1, \ldots, \pi_m\}$ be a partition of Ω into m non-empty parts. Then Π is called a *distinguishing partition* for G if its stabiliser $\bigcap_{i=1}^m G_{\{\pi_i\}}$ is trivial, where $G_{\{\pi_i\}}$ is the setwise stabiliser of π_i in G. The *distinguishing number* of G, denoted $D(G)$, is defined to be the smallest number m such that there exists a distinguishing partition for G with m parts. For example, $D(G) = 1$ if and only if G is trivial, whereas $D(G) \leqslant 2$ if and only if G has a regular orbit on the power set of Ω. At the other end of the spectrum, S_n and A_n have distinguishing numbers n and $n-1$, respectively.

We will need the following theorem due to Seress [110, Theorem 1.2], which gives a best possible upper bound on $D(G)$ when G is soluble.

Theorem 6.2.1. *If* G *is soluble, then* $D(G) \leqslant 5$.

Remark 6.2.2. It is worth noting that for each $d \in \{2,3,4,5\}$, there are infinitely many soluble transitive permutation groups G with $D(G) = d$. For example, if $t \in \{2,3,4\}$ and $m \geqslant 2$, then $D(G) = t+1$ for the natural action of $G = S_t \wr C_m$ of degree tm (see [110, p.244]). And by Theorem 6.2.3 below, there are infinitely many soluble primitive groups G with $D(G) = 2$.

The following result on the distinguishing number of primitive groups, which is also due to Seress [109, Theorem 2], will be useful later.

Theorem 6.2.3. *Let G be a primitive group of degree n. Then either $D(G) = 2$ or one of the following holds:*

(i) $G = S_n$ or A_n.

(ii) G is one of 43 groups listed in [109, Theorem 2], each with $n \leqslant 32$ and $D(G) \in \{3,4\}$.

The precise distinguishing numbers of the groups arising in case (ii) of Theorem 6.2.3 were determined by Dolfi (see [47, Lemma 1]).

6.2.2 Product type groups

Let $L \leqslant \mathrm{Sym}(\Gamma)$ be a finite primitive group with socle T and point stabiliser J, which is either almost simple or diagonal type (see Table 2.1). Let $k \geqslant 2$ be an integer and consider the product action of $L \wr S_k$ on the Cartesian product $\Omega = \Gamma_1 \times \cdots \times \Gamma_k = \Gamma^k$:

$$(6.2.1) \qquad (\gamma_1,\dots,\gamma_k)^{(z_1,\dots,z_k)\sigma} = \left(\gamma_{1^{\sigma^{-1}}}^{z_{1^{\sigma^{-1}}}},\dots,\gamma_{k^{\sigma^{-1}}}^{z_{k^{\sigma^{-1}}}}\right),$$

where $\gamma_i \in \Gamma$, $z_i \in L$ and $\sigma \in S_k$. Since this action is faithful and primitive, we can view $L \wr S_k$ as a product type primitive group on Ω, with socle T^k and point stabiliser $J \wr S_k$. More generally, a subgroup $G \leqslant L \wr S_k$ is a primitive group of product type if G has socle T^k and the subgroup $P \leqslant S_k$ induced by the conjugation action of G on the set of factors of T^k is transitive. Therefore

$$(6.2.2) \qquad T^k \trianglelefteqslant G \leqslant L \wr P.$$

Remark 6.2.4. Let $G_1 = \{(z_1,\dots,z_k)\sigma \in G : 1^\sigma = 1\}$ and let $L_1 \leqslant L \leqslant \mathrm{Sym}(\Gamma_1)$ be the group induced by G_1 on Γ_1. Then by a theorem of Kovács [81, (2.2)], we may replace G by a conjugate G^x for some $x \in \prod_{i=1}^k \mathrm{Sym}(\Gamma_i) < \mathrm{Sym}(\Omega)$ so that $G \leqslant L_1 \wr P$ and G induces L_1 on each factor Γ_i of Ω. Since $L_1 \leqslant \mathrm{Sym}(\Gamma_1)$ is primitive, we are free to assume that $L_1 = L$, so (6.2.2) holds and the groups L and P are uniquely determined by G. This observation will be relevant when we consider general product type groups with $G < L \wr P$ in Section 6.6.

Remark 6.2.5. Consider the special case where $G \leqslant L \wr P$ is a product type primitive group with soluble point stabiliser $H = G_\alpha$, where $\alpha = (\gamma,\dots,\gamma) \in \Omega$ for some $\gamma \in \Gamma$. By the transitivity of the socle T^k on Ω, we have $G = T^k H$ and thus H induces P on the set of factors of T^k. Therefore, P is soluble. In addition, we have $(T_\gamma)^k = (T^k)_\alpha \leqslant H$, so T_γ is soluble and thus L is almost simple (indeed, if L is a diagonal type group with socle $T = S^m$ for some non-abelian simple group S, then $T_\gamma \cong S$ is insoluble). In particular, $L/T \leqslant \mathrm{Out}(T)$ is soluble (see Lemma 2.2.6). Now the primitivity of L implies that $L = TL_\gamma$, so $L_\gamma/T_\gamma \cong L/T$ is soluble and we conclude that L_γ is soluble.

Given a positive integer m, let $\mathrm{reg}(L,m)$ be the number of regular L-orbits with respect to the natural coordinatewise action of L on the Cartesian product Γ^m. Note that $\mathrm{reg}(L,2) = r(L)$ is the number of regular suborbits of L on Γ. As before, when $m = b(L)$ we simply write $\mathrm{reg}(L) = \mathrm{reg}(L,m)$.

In this chapter we are primarily interested in product type primitive groups of the form $G = L \wr P$ as above. In this setting, the following theorem of Bailey and Cameron (see [6, Theorem 2.13]) will be an essential tool (with $D(P)$ defined with respect to the action of P on $[k]$).

Theorem 6.2.6. *Let $G = L \wr P$ be a product type primitive group. Then $b(G) \leqslant m$ if and only if $\mathrm{reg}(L,m) \geqslant D(P)$. In particular, $b(G) = b(L)$ if and only if $\mathrm{reg}(L) \geqslant D(P)$.*

6.3 Soluble stabilisers

In this section, we assume $G = L \wr P$ is a product type primitive group on $\Omega = \Gamma^k$, with socle T^k and soluble point stabiliser $J \wr P$. In particular, P is soluble and $L \leqslant \mathrm{Sym}(\Gamma)$ is almost simple with socle T and soluble point stabiliser J. We will prove Theorem 6.1.

We begin with a useful observation in this setting.

Lemma 6.3.1. *Let $G = L \wr P$ be a product type primitive group with soluble point stabilisers. Then either*

(i) $\mathrm{reg}(L) \geqslant D(P)$ *and* $b(G) = b(L)$*; or*

(ii) $\mathrm{reg}(L) < D(P)$ *and* $b(G) = b(L) + 1$.

Proof. Part (i) follows from Theorem 6.2.6. Now assume $\mathrm{reg}(L) < D(P)$, so $b(G) \geqslant b(L) + 1$. By [6, Corollary 2.14], we have

$$b(G) \leqslant b(L) + \lceil \log_m D(P) \rceil,$$

where $m = |\Gamma|$ is the degree of L. Since P is soluble, we have $D(P) \leqslant 5$ by Theorem 6.2.1, while $m \geqslant 5$ since L is almost simple. Therefore, $\lceil \log_m D(P) \rceil = 1$ and thus $b(G) \leqslant b(L) + 1$ as required. ■

Remark 6.3.2. In general, if $G = L \wr P$ does not have soluble point stabilisers, then the difference $b(G) - b(L)$ can be arbitrarily large. For example, if m is a positive integer and $k > \mathrm{reg}(L,m)$, then $b(L \wr S_k) > m$ by Theorem 6.2.6.

Since $D(P) \leqslant 5$ for every transitive soluble group P (see Theorem 6.2.1), we are naturally interested in determining the almost simple primitive groups L with $\mathrm{reg}(L) \leqslant 4$. The following theorem can be deduced immediately from Propositions 4.5.14 and 4.5.19.

Theorem 6.3.3. *Let L be a finite almost simple primitive group with soluble point stabiliser J. Then $\mathrm{reg}(L) \leqslant 4$ if and only if (L,J) is one of the cases in Table 4.7, 4.8 or 4.9.*

The proof of Theorem 6.1 is now completed by combining Lemma 6.3.1 and Theorem 6.3.3.

6.4 Regular orbits

In this section, we describe the bases for a product type primitive group $G = L \wr P$ as in (6.2.2), where $L \leqslant \mathrm{Sym}(\Gamma)$ is a primitive group and $P \leqslant S_k$ acts transitively on $[k]$. Recall from Theorem 6.2.6 that $b(G)$ is the smallest integer m such that $\mathrm{reg}(L,m) \geqslant D(P)$, where $D(P)$ is the distinguishing number of P.

Our first lemma describes the bases for G of size $b := b(G)$, which extends [20, Lemma 2.8] for base-two groups. Let $A := \{\alpha_{i,j}\}$ be a $k \times b$ array, where $\alpha_{i,j} \in \Gamma$. Define a partition Π of $[k]$ such that i and j are in the same part if and only if $(\alpha_{i,1},\dots,\alpha_{i,b})$ and $(\alpha_{j,1},\dots,\alpha_{j,b})$ are in the same L-orbit. Note that a column $(\alpha_{1,j},\dots,\alpha_{k,j})$ of A lies in $\Omega = \Gamma^k$. Let Δ be the set of columns of A, so that $\Delta \subseteq \Omega$.

Lemma 6.4.1. *The set Δ is a base for G if and only if each $\{\alpha_{i,1},\dots,\alpha_{i,b}\}$ is a base for L and Π is a distinguishing partition for P into $D(P)$ parts.*

Proof. First assume that each $\{\alpha_{i,1},\dots,\alpha_{i,b}\}$ is a base for L and Π is a distinguishing partition for P. Suppose that $x \in G_{(\Delta)}$, so that $x = z\sigma$ for some $z = (z_1,\dots,z_k) \in L^k$ and $\sigma \in P$. If $i^\sigma = j$, then $(\alpha_{i,1},\dots,\alpha_{i,b})^{z_i} = (\alpha_{j,1},\dots,\alpha_{j,b})$, which implies that σ fixes the partition Π. Thus, $\sigma = 1$ as Π is a distinguishing partition. Now $z_i \in \bigcap_{m=1}^{b} G_{\alpha_{i,m}} = 1$ since $\{\alpha_{i,1},\dots,\alpha_{i,b}\}$ is a base for L. Therefore, $z = 1$, and so Δ is a base for G.

To complete the proof, we assume that Δ is a base for G. Suppose for a contradiction that $\{\alpha_{i,1},\dots,\alpha_{i,b}\}$ is not a base for L, for some $i \in [k]$. Then there exists a non-identity element $x \in L$ fixing $\{\alpha_{i,1},\dots,\alpha_{i,b}\}$ pointwise. Now, let $z := (z_1,\dots,z_k) \in L$, where $z_i := x$ and $z_j := 1$ for $j \neq i$. It is then easy to show that $1 \neq z \in G_{(\Delta)}$, a contradiction. Thus $\{\alpha_{i,1},\dots,\alpha_{i,b}\}$ is a base for L.

Finally, we prove that Π is a distinguishing partition for P. Recall that Π is defined in terms of the L-orbits on Γ^b, so without loss of generality, we may assume that $\alpha_{i,m} = \alpha_{j,m}$ for any $m \in [k]$ if i and j are in the same part of Π, noting that the columns of A still form a base for G with this assumption. In particular, we have

$$(\alpha_{i,1},\dots,\alpha_{i,b}) = (\alpha_{j,1},\dots,\alpha_{j,b}) \text{ if and only if } i \text{ and } j \text{ are in the same part of } \Pi.$$

Thus, if $\sigma \in P$ fixes the partition Π, then it also fixes every column of A. Since the set Δ of columns of A is a base for G, we obtain $\sigma = 1$, as required. ■

By arguing as in the proof of Lemma 6.4.1, we are also able to derive a formula for the number $r(G) = \mathrm{reg}(G,2)$ of regular suborbits of G. In order to do this, we will write t_m for the number of (unordered) distinguishing partitions for the action of P on $[k]$ into m non-empty parts, where $1 \leqslant m \leqslant k$. Note that $t_m > 0$ if and only if $m \geqslant D(P)$. In general, it is rather difficult to compute t_m precisely, but this is possible in some special cases. For example, if $P = S_k$ then $D(P) = k$

and $t_k = 1$ since the partition of $[k] = \{1,\dots,k\}$ into singletons is clearly the only distinguishing partition for P. Similarly, if $P = A_k$ then $D(P) = k-1$ and we have $t_{k-1} = k(k-1)/2$. In general, if $m \geqslant D(P)$ then

$$\frac{|P|}{m!} \leqslant t_m \leqslant S(k,m),$$

where $S(k,m)$ denotes the number of partitions of $[k]$ into m non-empty parts (a Stirling number of the second kind). The following theorem is stated as Theorem 6.3.

Theorem 6.4.2. *Let $G = L \wr P$ be a product type primitive group acting on $\Omega = \Gamma^k$. Then*

$$r(G) = \frac{1}{|P|} \sum_{m=D(P)}^{k} m! \binom{r(L)}{m} t_m.$$

Proof. Set $r = r(L)$ and $D = D(P)$. If $r < D$ then Theorem 6.2.6 gives $b(G) \geqslant 3$, so $r(G) = 0$ and the result follows (note that each summand in the given expression is 0 in this situation). Now assume $r \geqslant D$. By arguing as in the proof of Lemma 6.4.1, we see that $|G|r(G)$ is the number of $k \times 2$ arrays satisfying the following conditions:

(A1) each row of the array is an ordered base for L; and

(A2) the partition of $[k]$ with respect to L-orbits on rows is a distinguishing partition for P.

Let A be an arbitrary $k \times 2$ array satisfying (A1) and (A2), where Π is the partition of $[k]$ corresponding to (A2). Let m be the number of parts in Π, so $D \leqslant m \leqslant k$ and there are precisely t_m possibilities for Π in total. Each part comprising Π corresponds to a distinct regular L-orbit on Γ^2. Since there are r such orbits, it follows that there are $m!\binom{r}{m}$ different ways to label the rows of A by regular L-orbits on Γ^2. In addition, since each of these L-orbits has length $|L|$, there are $|L|^k$ possibilities for A with respect to each choice of labelling of rows by regular L-orbits. To summarise, we deduce that

$$|G|r(G) = \sum_{m=D}^{k} m! \binom{r}{m} t_m |L|^k,$$

and the result follows since $|G| = |L|^k|P|$. ■

We now present several corollaries of Theorem 6.3. Further applications will be discussed in the next section.

Corollary 6.4.3. *Let $G = L \wr P$ be a product type primitive group acting on $\Omega = \Gamma^k$, where $P = S_k$. Then $r(G) = \binom{r(L)}{k}$.*

Proof. This is an immediate application of Theorem 6.3, noting that for $P = S_k$ we have $D(P) = k$ and $t_k = 1$. ■

The next corollary is [20, Proposition 3.5]; here we give a short proof, as an application of Theorem 6.3.

Corollary 6.4.4. *Let $G = L \wr P$ be a product type primitive group acting on $\Omega = \Gamma^k$, where $P = C_k$ and k is a prime. Then $r(G) = (r(L)^k - r(L))/k$.*

Proof. Set $r = r(L)$ and note that $D(P) = 2$, so Theorem 6.2.6 implies that $r(G) \geqslant 1$ if and only if $r \geqslant 2$. Now any partition of $[k]$ into at least two parts is a distinguishing partition for P, so for $m \geqslant 2$ we observe that t_m coincides with the total number of partitions of $[k]$ into m parts. In other words, $t_m = S(k,m)$ is a Stirling number of the second kind. Therefore,

$$\sum_{m=2}^{k} m!\binom{r}{m} t_m = \sum_{m=2}^{k} m!\binom{r}{m} S(k,m) = r^k - r,$$

where the final equality follows from a basic property of Stirling numbers of the second kind (see [115, p.75], for example). By applying Theorem 6.3, we conclude that $r(G)k = r^k - r$. ■

For the remainder of this section, we focus our attention on the groups with $\mathrm{reg}(G) = 1$. Fix an integer $m \in [k]$ and let

$$\mathscr{P}_m([k]) = \{(\pi_1, \ldots, \pi_m) : \pi_i \subseteq [k],\ \pi_i \cap \pi_j = \emptyset \text{ for } i \neq j,\ \bigcup_i \pi_i = [k]\}$$

be the set of ordered partitions of $[k]$ into m parts, where some of the parts are allowed to be empty. Note that we may identify $\mathscr{P}_2([k])$ with the power set of $[k]$. Then P acts naturally on $\mathscr{P}_m([k])$ via

$$(\pi_1, \ldots, \pi_m)^\sigma = (\pi_1^\sigma, \ldots, \pi_m^\sigma)$$

and we see that $(\pi_1, \ldots, \pi_m)$ is in a regular P-orbit if and only if $\{\pi_1, \ldots, \pi_m\}$ is a distinguishing partition for P.

Lemma 6.4.5. *Let $G = L \wr P$ be a product type primitive group. Then $\mathrm{reg}(G) = 1$ if and only if $\mathrm{reg}(L, b(G)) = D(P)$ and P has a unique regular orbit on $\mathscr{P}_{D(P)}([k])$.*

Proof. Let $b = b(G)$ and let A_1 and A_2 be two $k \times b$ arrays of elements of Γ. For each $i \in \{1,2\}$, write Π_i for the associated partition of $[k]$ with respect to L-orbits of rows of A_i, and write Δ_i for the set of columns of A_i. By Lemma 6.4.1, Δ_i is a base for G if and only if Π_i is a distinguishing partition and each row of A_i is a base for L.

First assume that $\mathrm{reg}(G) = 1$. Note that if Π_1 and Π_2 are in distinct P-orbits, then Δ_1 and Δ_2 are in distinct G-orbits. It follows by Lemma 6.4.1 that $\mathrm{reg}(L, b(G)) = D(P)$ and P has a unique regular orbit on $\mathscr{P}_{D(P)}([k])$.

The other direction is clear by applying Lemma 6.4.1. ■

Now we focus on the cases where $P \leqslant S_k$ is a primitive group, and our aim is to establish Theorem 6.2 stated in Section 6.1. In view of Lemma 6.4.5, we are interested in the primitive groups $P \leqslant S_k$ satisfying the following property:

$$P \text{ has a unique regular orbit on } \mathscr{P}_{D(P)}([k]), \tag{6.4.1}$$

which we will classify in Proposition 6.4.15 below.

Suppose (6.4.1) holds and $\{\pi_1,\dots,\pi_{D(P)}\}$ is a distinguishing partition for P. Then the unique regular P-orbit on $\mathscr{P}_{D(P)}([k])$ is represented by $(\pi_1,\dots,\pi_{D(P)})$ and all $D(P)!$ rearrangements of this ordered partition are in the same P-orbit. Therefore, the π_i all have the same size and thus $D(P)$ must divide k.

Since we are focussing on the case where $P \leqslant S_k$ is primitive, we have a special interest in the groups with $D(P) = 2$ (see Theorem 6.2.3). Here Lemma 6.4.5 implies that (6.4.1) holds if and only if P has a unique regular orbit on the power set of $[k]$ and we will classify the primitive groups with this property (see Corollary 6.4.10 below). This can be viewed as a natural extension of the main theorem of [109] (stated here as Theorem 6.2.3), which determines the primitive groups $P \leqslant S_k$ with a regular orbit on the power set of $[k]$. It also extends earlier work of Dolfi [47], where the primitive groups with a unique regular orbit on $\mathscr{P}_3([k])$ or $\mathscr{P}_4([k])$ are classified.

For the remainder of this section, define

$$X = \{\Lambda \subseteq [k] : |\Lambda| \neq k/2\} \tag{6.4.2}$$

and note that P has a natural action on X. Of course, if k is odd then X coincides with the power set of $[k]$.

Lemma 6.4.6. *If P has a regular orbit on X, then P has at least two regular orbits on $\mathscr{P}_2([k])$.*

Proof. If Λ is in a regular orbit of P on X, then its complement $[k]\setminus\Lambda$ is also contained in a regular P-orbit. ∎

Clearly, if $D(P) = 2$ and k is odd, then P has a regular orbit on X and thus P has at least two regular orbits on $\mathscr{P}_2([k])$ by the lemma. Therefore, we are interested in the case where $D(P) = 2$ and k is even, so

$$|X| = 2^k - \binom{k}{k/2}.$$

Lemma 6.4.7. *We have $|X| \geqslant 2^{k-1}$.*

Proof. We may assume k is even, so it suffices to show that

$$\binom{k}{k/2} \leqslant 2^{k-1}.$$

To do this, we will use the following bounds on $m!$ (valid for all $m \geqslant 1$), which are a consequence of Stirling's approximation (see [107]):

$$\sqrt{2\pi m}\left(\frac{m}{e}\right)^m e^{1/(12m+1)} < m! < \sqrt{2\pi m}\left(\frac{m}{e}\right)^m e^{1/12m}.$$

Therefore, for $k \geqslant 4$ we have

$$\binom{k}{k/2} = \frac{k!}{(k/2)!^2} < \frac{\sqrt{2\pi k}\left(\frac{k}{e}\right)^k e^{1/12k}}{\left(\sqrt{\pi k}\left(\frac{k}{2e}\right)^{k/2} e^{1/(6k+1)}\right)^2} = \left(\frac{2\sqrt{2}}{\sqrt{\pi k}} e^{\frac{1}{12k}-\frac{2}{6k+1}}\right) 2^{k-1} < 2^{k-1}$$

and the result follows, noting that the case $k = 2$ is clear. ■

Let $\mu(P)$ be the *minimal degree* of P, which is the minimal number of points in $[k]$ moved by a non-identity element of P.

Lemma 6.4.8. *If k is even and $|P| < 2^{\mu(P)/2-1}$, then P has a regular orbit on X.*

Proof. We follow the proof of the main theorem of [35]. Suppose P has no regular orbit on X, which means that each set in X is fixed (setwise) by some prime order element of P. Therefore,

$$|X| = \left|\bigcup_{\sigma \in \mathscr{R}} C_X(\sigma)\right| \leqslant \sum_{\sigma \in \mathscr{R}} |C_X(\sigma)|,$$

where $\mathscr{R}$ is the set of prime order elements in P and $C_X(\sigma)$ is the set of fixed points of σ on X. If $\sigma \in P$ has prime order r, then σ has cycle-shape $(r^m, 1^{k-mr})$ on $[k]$ for some $m \geqslant 1$ and it is easy to see that

$$|C_X(\sigma)| \leqslant 2^{k-m(r-1)} \leqslant 2^{k-(r-1)\mu(P)/r} \leqslant 2^{k-\mu(P)/2}$$

since $\mu(P) \leqslant mr$ and $r \geqslant 2$. By applying Lemma 6.4.7 we deduce that

$$2^{k-1} \leqslant |X| \leqslant 2^{k-\mu(P)/2}|P|$$

and thus $|P| \geqslant 2^{\mu(P)/2-1}$. ■

We will use Lemma 6.4.8 and the O'Nan-Scott theorem to prove the following result.

Proposition 6.4.9. *Let $P \leqslant S_k$ be a primitive group with $D(P) = 2$. Then P has no regular orbit on X if and only if $(k,P) = (2, S_2)$ or $(16, 2^4{:}\mathrm{O}_4^-(2))$.*

We then obtain the following as an immediate corollary.

Corollary 6.4.10. *Let $P \leqslant S_k$ be a primitive group. Then P has a unique regular orbit on the power set of $[k]$ if and only if $(k,P) = (2, S_2)$.*

Proof. Suppose P has a unique regular orbit on the power set of $[k]$, so $D(P) = 2$ and P has no regular orbit on X by Lemma 6.4.6. If $(k,P) = (16, 2^4{:}\mathrm{O}_4^-(2))$ then one checks that P has two regular orbits on the power set of $[k]$. Now apply Proposition 6.4.9. ■

We now focus on the proof of Proposition 6.4.9, considering each family of primitive groups in turn (see Table 2.1).

Lemma 6.4.11. *Let $P \leqslant S_k$ be a primitive group of type III, IV or V. Then P has a regular orbit on X.*

Proof. First assume that P is of type III, so $P \leqslant S^m.(\mathrm{Out}(S) \times S_m)$ is a diagonal type group, S is a non-abelian simple group and $k = s^{m-1}$, where $s = |S|$ and $m \geqslant 2$. Now $|P| < s^{m+1}m!$ and [22, Theorem 4] gives $\mu(P) \geqslant 2k/3$, so in view of Lemma 6.4.8, it suffices to show that

$$f(s,m) := \frac{2^{\frac{1}{3}s^{m-1}-1}}{s^{m+1}m!} > 1.$$

If we fix s, then it is easy to check that $f(s,m)$ is an increasing function of m, whence

$$f(s,m) \geqslant f(s,2) = \frac{2^{\frac{1}{3}s-1}}{2s^3} > 1$$

for all $s \geqslant 60$ and the result follows.

Next assume $P \leqslant S_m \wr S_t$ is a product type primitive group of degree $k = m^t$, where $m \geqslant 5$ and $t \geqslant 2$. As explained in the proof of [109, Lemma 4], there exists a subset $\Lambda \subseteq \{1,\dots,k\}$ such that $P_{\{\Lambda\}} = 1$ and

$$|\Lambda| = \ell + \sum_{i=1}^{t}(m-2)^{i-1}m^{t-i},$$

where $\ell = 3m-5$ if $t \geqslant 3$, otherwise $\ell = 2m-3$. If m is odd then $k = m^t$ is odd and thus $\Lambda \in X$. On the other hand, if m is even, then $k/2 = m^t/2$ is even and $|\Lambda|$ is odd, so $\Lambda \in X$ once again.

Finally, suppose P is a primitive group of type V, so $P = S^m.Q$ is a twisted wreath product, where S is a non-abelian simple group and $Q \leqslant S_m$ is transitive. Here we can embed P in a product type primitive group $R = S^2 \wr S_m \leqslant \mathrm{Sym}([k])$ and the result follows since we have already shown that R has a regular orbit on X (see [88, Remark 2(ii)] for the containment of P in R). ■

Next, we turn to the primitive groups of affine type. The following result extends [109, Lemma 7].

Lemma 6.4.12. *Consider the natural action of $P = \mathrm{AGL}_d(p)$ on $k = p^d$ points, where $d \geqslant 1$, p is a prime and $(d,p) \neq (1,2)$. Then either P has a regular orbit on X, or $D(P) > 2$ and one of the following holds:*

(i) $p = 2$ *and* $d \in \{2,3,4,5\}$.

(ii) $d = 1$ *and* $p \in \{3,5,7\}$.

(iii) $d = 2$ *and* $p = 3$.

Proof. First assume p is odd, so $k = p^d$ is also odd. Then as previously noted, P has a regular orbit on X if and only if $D(P) = 2$, and the groups with $D(P) > 2$ can be read off from [109, Lemma 7]. For the remainder, we may assume $p = 2$.

As noted in the proof of [109, Lemma 7], we have $\mu(P) = 2^{d-1}$ and thus

$$|P| < 2^{d^2+d-1} < 2^{\mu(P)/2-1}$$

for $d \geqslant 9$. Therefore, Lemma 6.4.8 implies that P has a regular orbit on X if $d \geqslant 9$. For $d = 6,7,8$, we can use MAGMA to construct P as a permutation group on $[k]$ and by random search we can find a subset $\Lambda \in X$ with $P_{\{\Lambda\}} = 1$ and $|\Lambda| = 16,16,17$, respectively. Finally, if $d \in \{3,4,5\}$ then $D(P) > 2$ by [109, Lemma 7], and similarly $D(P) = 4$ when $d = 2$. ■

We can now complete the analysis of primitive groups of affine type.

Lemma 6.4.13. *Let $P \leqslant \mathrm{AGL}_d(p)$ be a primitive affine group of degree $k = p^d$, where $d \geqslant 1$, p is a prime and $D(P) = 2$. Then P has no regular orbit on X if and only if one of the following holds:*

(i) $k = 2$ *and* $P = S_2$.

(ii) $k = 16$ *and* $P = 2^4{:}\mathrm{O}_4^-(2)$.

Proof. We may assume $p = 2$ and $d \geqslant 2$. If $d \geqslant 6$ then Lemma 6.4.12 implies that $\mathrm{AGL}_d(2)$, and hence P, has a regular orbit on X. Therefore, we may assume $d \in \{2,3,4,5\}$ and $P < \mathrm{AGL}_d(2)$.

If $d = 5$ then $P = 2^5{:}31$ or $2^5{:}(31{:}5)$ and in both cases we can use MAGMA to find a subset of $[32]$ of size 5 with trivial setwise stabiliser in P. Next assume $d = 4$. We can use the MAGMA database of primitive groups to construct each possibility for P; there are 19 such groups, up to permutation isomorphism, and 15 with $D(P) = 2$. In all but one of these cases, we can use random search to find a set in X with trivial setwise stabiliser in P. The exception is the group $P = 2^4{:}\mathrm{O}_4^-(2)$ recorded in case (ii). Here $k = 16$, $D(P) = 2$ and every subset of $[16]$ with trivial setwise stabiliser has size 8, so this is a genuine exception. Finally, if $d \in \{2,3\}$ then $P = 2^3{:}7$ is the only group with $D(P) = 2$ and it is easy to check that there is a subset of size 3 with trivial setwise stabiliser in P. ■

Finally, we deal with the case where P is an almost simple primitive group.

Lemma 6.4.14. *Let $P \leqslant S_k$ be an almost simple primitive group with $D(P) = 2$. Then P has a regular orbit on X.*

Proof. Let R be the socle of P and write Q for the stabiliser of a point in $\Omega = [k]$. For the convenience of the reader, we divide the proof into several cases.

Case 1. R is an alternating group.

First assume $R = A_m$ is an alternating group. The case $m = 6$ can be handled using MAGMA, so we may assume $m \neq 6$ and thus $P = S_m$ or A_m. There are now three cases to consider, according to the action of Q on $\{1,\dots,m\}$.

First assume Q is intransitive, in which case we may identify Ω with the set of t-element subsets of $\{1,\ldots,m\}$ for some $2 \leqslant t < m/2$ (note that $t \neq 1$ since we are assuming $D(P) = 2$). Suppose $m \geqslant t+5$. If $t \geqslant 4$ then the proof of [109, Lemma 9] shows that there exists a subset Λ of Ω such that $P_{\{\Lambda\}} = 1$ and $|\Lambda| = 2(m-t+1) < k/2$, so P has a regular orbit on X. Similarly, if $t = 2,3$ then we can take $|\Lambda| = m-t+1$. On the other hand, if $m < t+5$ then $(m,t) = (7,3)$ or $(5,2)$, noting that $P = A_5$ in the latter case (since $D(P) > 2$ when $P = S_5$). Here it is straightforward to check that Ω has a subset of size 4 with trivial setwise stabiliser in P.

Next assume Q acts primitively on $\{1,\ldots,m\}$. By the main theorem of [105] we have $|Q| < 4^m$ and [22, Theorem 4] implies that $\mu(P) \geqslant 2k/3$. By combining these bounds and applying Lemma 6.4.8, noting that $k = |P:Q|$, we deduce that P has a regular orbit on X if $m \geqslant 14$. For $7 \leqslant m \leqslant 13$ we can use MAGMA to determine the possibilities for Q and it is routine to check that $|P| < 2^{k/3-1}$ unless $(k,P,Q) = (15, A_8, \mathrm{AGL}_3(2))$ or $(15, A_7, \mathrm{L}_3(2))$. In the former case we have $D(P) > 2$, while $D(P) = 2$ in the latter and the result follows since $k = 15$ is odd. Finally, if $m = 5$ then one can check that $D(P) > 2$.

To complete the argument when $R = A_m$, we may assume Q acts imprimitively on $\{1,\ldots,m\}$. Here we may identify Ω with the set of partitions of $\{1,\ldots,m\}$ into b sets of size a, where $a,b \geqslant 2$ and $m = ab \geqslant 8$ (we have already considered the case $m = 6$). Therefore, $k = m!/(a!^b b!)$ and the main theorem of [64] gives $\mu(P) \geqslant k/2$, so it suffices to show that $|P| < 2^{k/4-1}$ (see Lemma 6.4.8). First assume $m = 8$. If $(a,b) = (2,4)$ then it is easy to check that $|P| < 2^{k/4-1}$. On the other hand, if $(a,b) = (4,2)$ then $D(P) = 2$ and the result follows since $k = 35$ is odd. Now assume $m \geqslant 9$. Here $m! < 2^{m^2/4-1}$ and so it suffices to show that $k \geqslant m^2$. This is clear if $a \geqslant 3$ since $k \geqslant \binom{m}{3} > m^2$ for $m \geqslant 9$. Finally, for $a = 2$ it remains to show that

$$f(b) := \frac{(2b)!}{b!2^b 4b^2} > 1$$

for all $b \geqslant 5$. It is easy to verify that this is an increasing function, so $f(b) \geqslant f(5) > 1$ and the result follows.

Case 2. R is a sporadic group.

Next assume R is a sporadic simple group. First observe that $D(P) > 2$ if $R = \mathrm{M}_{22}$ and $k = 22$, so this case does not arise and thus $\mu(P) \geqslant 2k/3$ by [22, Theorem 4]. Therefore, it suffices to show that $|P| < 2^{k/3-1}$. Let ℓ be the minimal index of a core-free subgroup of P, which can be read off from [120]. If P is not a Mathieu group, then it is straightforward to show that $|P| < 2^{\ell/3-1}$ and the result follows. On the other hand, if P is a Mathieu group then the cases with $D(P) > 2$ are determined in [109, Lemma 12]; by excluding these groups, it is easy to check that $|P| < 2^{k/3-1}$ as required.

Case 3. R is a group of Lie type.

For the remainder, we may assume R is a simple group of Lie type over $\mathbb{F}_q$, where $q = p^f$ and p is a prime. As before, let ℓ be the minimal index of a core-free subgroup of P and note that ℓ is recorded in [62, Table 4].

First assume R is an exceptional group of Lie type. By [90, Proposition 2] and [22, Theorem 4], we have $|P| < k^5$ and $\mu(P) \geqslant 2k/3$, so it suffices to show that $k^5 < 2^{k/3-1}$. The latter bound holds for $k \geqslant 104$ and by inspecting [62, Table 4] we reduce to the case where $R = {}^2B_2(8)$ and Q is a Borel subgroup of P. Here $k = 65$ and $|P| \leqslant 3|R| < 2^{k/3-1}$, so once again Lemma 6.4.8 implies that P has a regular orbit on X.

Finally, let us assume R is a classical group. As noted in Remark 2.2.2, we may assume R is one of the following:

$$\mathrm{L}_n(q),\ n \geqslant 2;\ \mathrm{U}_n(q),\ n \geqslant 3;\ \mathrm{PSp}_n(q),\ n \geqslant 4;\ \mathrm{P\Omega}_n^{\varepsilon}(q),\ n \geqslant 7.$$

We may also assume that R is not isomorphic to an alternating group. By [64, Corollary 1] we have $\mu(P) \geqslant 3k/7$.

First assume $n \geqslant 4$ and observe that $|P| < q^{n^2}$. By carefully inspecting [62, Table 4] we see that $\ell > q^{n-2}$ and thus $\mu(P) > \frac{3}{7}q^{n-2}$. Now, if $n \geqslant 12$ or $q \geqslant 19$ then

$$q^{n^2} < 2^{\frac{3}{14}q^{n-2}-1}$$

and we deduce that $|P| < 2^{\mu(P)/2-1}$, which implies that P has a regular orbit on X (in fact, if $q \geqslant 3$ then the same bound holds for all $n \geqslant 8$). This leaves us with finitely many groups to consider. In each of these remaining cases, it is routine to check that $|P| < 2^{3\ell/14-1}$ with the exception of the following possibilities for (R, k):

$$(\mathrm{L}_4(5), 156), (\mathrm{L}_4(3), 40), (\mathrm{U}_4(3), 112), (\mathrm{U}_4(2), 40), (\mathrm{U}_4(2), 36),$$

$$(\mathrm{Sp}_6(2), 36), (\Omega_8^+(2), 120), (\Omega_8^-(2), 136).$$

(Here we also exclude the relevant groups with $D(P) > 2$, as recorded in [109, Lemma 12], together with the groups where $D(P) = 2$ and k is odd.) In each of these cases, we can use MAGMA to construct P as a permutation group on $[k]$ and then find a subset in X by random search with trivial setwise stabiliser in P.

Finally, let us assume $n \in \{2, 3\}$. If $R = \mathrm{L}_3(q)$ then $\ell = q^2 + q + 1$ and

$$|P| \leqslant 2q^3(q^2-1)(q^3-1)\log q < 2^{3\ell/14-1}$$

for $q \geqslant 13$. The remaining groups with $q < 13$ can be dealt with using MAGMA as above. Similarly, if $R = \mathrm{U}_3(q)$ then the problem is quickly reduced to the groups with $q \leqslant 5$, each of which can be handled in the usual fashion with the aid of MAGMA. Finally, suppose $R = \mathrm{L}_2(q)$. If $q \geqslant 113$ then $\ell = q + 1$ and one can check that

$$|P| \leqslant q(q^2-1)\log q < 2^{3\ell/14-1},$$

which implies that P has a regular orbit on X. The remaining groups with $q < 113$ can be handled using MAGMA; either the bound $|P| < 2^{3k/14-1}$ is satisfied and we conclude via Lemma 6.4.8, or we construct P as a permutation group on $[k]$ and then use random search to find a set in X with trivial setwise stabiliser in P. ■

This completes the proof of Proposition 6.4.9 and we are now in a position to classify the primitive groups P such that (6.4.1) holds.

Proposition 6.4.15. *Let $P \leqslant S_k$ be a primitive group. Then* (6.4.1) *holds if and only if $P = S_k$, or* $(k,P,D(P)) = (6,A_5,3)$*,* $(9,\mathrm{P\Gamma L}_2(8),3)$ *or* $(8,\mathrm{AGL}_3(2),4)$*.*

Proof. Set $D = D(P)$. Note that if $P = S_k$ then $D = k$ and (6.4.1) holds, whereas (6.4.1) fails to hold if $P = A_k$ (with $D = k-1$). Now assume $P \neq A_k, S_k$ and recall that $D \leqslant 4$ (see Theorem 6.2.3). If $D = 2$ then Corollary 6.4.10 applies, so we may assume $D \in \{3,4\}$. These groups can be read off by inspecting parts (a) and (c) in [47, Lemma 1]. ■

The proof of Theorem 6.2 is now completed by combining Lemma 6.4.5 with Proposition 6.4.15.

6.5 Saxl graphs

In this section, we use Lemma 6.4.1 and Theorem 6.3 to study the valency and connectedness properties of the generalised Saxl graphs of product type primitive groups.

6.5.1 Valency

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive group with point stabiliser H, and let $\mathrm{val}(G)$ be the valency of the generalised Saxl graph $\Sigma(G)$. In view of Lemma 3.1.1(iv), we have $\mathrm{val}(G) = r(G)|H|$ if $b(G) = 2$. However, as noted in Section 3.2, it is not straightforward to describe $\mathrm{val}(G)$ when $b(G) \geqslant 3$. Thus, we focus on base-two groups to begin with.

Recall that a graph is *Eulerian* if it contains an Eulerian cycle, which is a cycle that uses each edge exactly once. A celebrated theorem of Euler asserts that a connected graph is Eulerian if and only if the degree of every vertex is even. In particular, the Saxl graph of a base-two primitive group G is Eulerian if and only if $\mathrm{val}(G)$ is even.

A complete classification of the finite base-two primitive groups with an Eulerian Saxl graph remains out of reach and some genuine exceptions have been identified. For example, if $G = \mathrm{M}_{23}$ and $H = 23{:}11$, then the action of G on $[G:H]$ is primitive with $b(G) = 2$ and the corresponding Saxl graph is non-Eulerian (indeed, we compute $r(G) = 159$, so $\mathrm{val}(G) = r(G)|H|$ is odd). The problem for almost simple primitive groups is studied in [20, Proposition 3.2] and subsequently extended in [37, Theorem 4].

As an application of Theorem 6.3, the following result establishes part (i) of Corollary 6.4. It can be viewed as an extension of [20, Proposition 3.4].

Proposition 6.5.1. *Let $G = L \wr P$ be a base-two primitive wreath product acting on $\Omega = \Gamma^k$. Then $\Sigma(G)$ is Eulerian.*

Proof. By Theorem 6.3 we have

$$\sum_{m=D(P)}^{k} m!\binom{r(L)}{m} t_m = r(G)|P| \tag{6.5.1}$$

and each summand on the left hand side of this equality is even since $D(P) \geqslant 2$. Therefore, at least one of $r(G)$ or $|P|$ is even, so $\mathrm{val}(G) = r(G)|H|$ is even and the result follows. ■

The finite base-two transitive groups G such that $\Sigma(G)$ has prime valency are determined in [20, Proposition 3.1]. For almost simple primitive groups, this has been extended in my joint paper [37] with Chen. More specifically, the following result is [37, Theorem 3], which classifies all the groups of this form with the property that $\mathrm{val}(G)$ is a prime power (in each case, $\mathrm{val}(G)$ is a 2-power).

Theorem 6.5.2. *Let G be a base-two almost simple primitive group with point stabiliser H. Then* $\mathrm{val}(G)$ *is a prime power if and only if one of the following holds:*

(i) $(G,H) = (\mathrm{M}_{10}, 8{:}2)$ *and* $\mathrm{val}(G) = 32$.

(ii) $(G,H) = (\mathrm{PGL}_2(q), D_{2(q-1)})$*, where $q \geqslant 17$ is a Fermat prime or $q = 9$, $\Sigma(G)$ is isomorphic to the Johnson graph $J(q+1,2)$ and* $\mathrm{val}(G) = 2(q-1)$.

In our next result, which gives part (ii) of Corollary 6.4, we extend the analysis to product type primitive groups of the form $G = L \wr P$.

Proposition 6.5.3. *Let $G = L \wr P$ be a base-two product type primitive group acting on $\Omega = \Gamma^k$ with point stabiliser $J \wr P$. Then* $\mathrm{val}(G)$ *is a prime power if and only if $L = \mathrm{M}_{10}$, $J = SD_{16}$, P is a 2-group and $t_2 \geqslant 1$ is a 2-power.*

Proof. Suppose $\mathrm{val}(G) = p^a$ with p a prime. Then J and P are p-groups, so J is soluble and thus L is almost simple. By [37, Proposition 6.3], the possibilities for (L,J) are recorded in [37, Table 3], which we reproduce as Table 6.1, and we deduce that $p = 2$.

By Theorem 6.3, we see that (6.5.1) holds and thus

$$\sum_{m=D(P)}^{k} m!\binom{r(L)}{m} t_m$$

is a 2-power. This observation immediately implies that $D(P) = 2$, otherwise each summand is divisible by 3. In addition, $r(L) \equiv 2 \pmod 3$ because the binomial coefficient $\binom{r(L)}{2}$ must be indivisible by 3. By inspecting Table 6.1, we now consider each possibility for (L,J) in turn.

L	J	Conditions
$\mathrm{L}_2(q)$	D_{q-1}	$q \geqslant 17$ is a Fermat prime
	D_{q+1}	$q \geqslant 31$ is a Mersenne prime
$\mathrm{PGL}_2(q)$	$D_{2(q-1)}$	$q \geqslant 17$ is a Fermat prime
	$D_{2(q+1)}$	$q \geqslant 7$ is a Mersenne prime
$\mathrm{PGL}_2(9)$	D_{16}	
M_{10}	$8{:}2$	
$\mathrm{P\Gamma L}_2(9)$	$8{:}2^2$	

Table 6.1: Almost simple groups L with a maximal subgroup J of prime-power order

First assume $L = \mathrm{L}_2(q)$ and $J = D_{q-1}$, where $q \geqslant 17$ is a Fermat prime. Then $q \equiv 1 \pmod 4$ and so $r(L) = (q+7)/4$ as noted in Remark 4.5.15(ii). If we write $q = 2^m + 1$ then $r(L) = 2^{m-2} + 2$ and thus $r(L) \not\equiv 2 \pmod 3$, so this case does not arise. Now suppose $L = \mathrm{L}_2(q)$ and $J = D_{q+1}$ with $q = 2^m - 1 \geqslant 31$ a Mersenne prime. Here $q \equiv 3 \pmod 4$ and $r(L) = (q-3)/4$ by the proof of [24, Lemma 7.9]. Therefore $r(L) = 2^{m-2} - 1$ and once again we deduce that $r(L) \not\equiv 2 \pmod 3$.

Finally, let us turn to the remaining cases in Table 6.1. If $L = \mathrm{PGL}_2(q)$ and $J = D_{2(q-1)}$ with $q \geqslant 17$ a Fermat prime, then $r(L) = 1$ (see Example 3.1.4) and thus $b(G) \geqslant 3$. The case where $L = \mathrm{PGL}_2(q)$ and $J = D_{2(q+1)}$ with $q \geqslant 7$ a Mersenne prime can be immediately excluded since $b(L) = 3$ by [14, Theorem 2]. The handful of remaining possibilities can be checked using MAGMA, implementing the approach presented in Section 4.2.4 to compute $r(L)$. In this way, we find that $r(L) \equiv 2 \pmod 3$ if and only if $L = \mathrm{M}_{10}$ and $J = SD_{16}$, where we observe that $r(L) = 2$.

We conclude that $L = \mathrm{M}_{10}$ with $J = SD_{16}$ is the only possibility. Here Theorem 6.3 implies that $|P|r(G) = 2t_2$ and thus t_2 is a 2-power (note that $t_2 = 1$ if and only if $P = S_2$). This completes the proof of the proposition. ■

Remark 6.5.4. There are genuine examples in Proposition 6.5.3, where $P \leqslant S_k$ is a transitive 2-group and t_2 is a 2-power. For example, we can take $(k,P) = (2,S_2)$ or $(4, C_2 \times C_2)$, where $t_2 = 1$ or 4, respectively. By inspecting the MAGMA database of transitive groups, we find that there are 165 groups of degree $k \leqslant 16$ with the desired property. For example, t_2 is a 2-power for 156 of the 1427 transitive 2-groups of degree 16.

6.5.2 Connectedness

Now we turn to an application of Lemma 6.4.1 to the study of Conjecture II for general primitive groups. Recall that if $b(G) = 2$, then the neighbourhood of $\alpha \in \Omega$ in $\Sigma(G)$ is the union of regular G_α-orbits on Ω. We introduce the following terminology in order to generalise this observation to the case $b(G) \geqslant 3$.

Definition 6.5.5. Let $\alpha \in \Omega$. An orbit $O \neq \{\alpha\}$ of G_α on Ω is called *almost-regular* if $O \cap \Delta \neq \emptyset$ for some base Δ for G of size $b(G)$ with $\alpha \in \Delta$.

In other words, β lies in an almost-regular G_α-orbit if $\{\alpha,\beta\}$ can be extended to a base for G of size $b(G)$, i.e. if $\{\alpha,\beta\}$ is an edge in $\Sigma(G)$. Thus, the set of neighbours of α in $\Sigma(G)$ is equal to the union of almost-regular G_α-orbits. Note that any permutation group G with $b(G) \geqslant 2$ has an almost-regular suborbit, and if $b(G) = 2$, then a suborbit is regular if and only if it is almost-regular. The set $N(\alpha)$ of neighbours of α in $\Sigma(G)$ is exactly the union of the almost-regular G_α-orbits.

For a permutation group $G \leqslant \mathrm{Sym}(\Omega)$ with $b(G) \geqslant 2$, we define the following property:

$$(\star\star) \qquad N(\alpha) \textit{ meets every almost-regular } G_\beta\textit{-orbit for all } \alpha,\beta \in \Omega.$$

Note that $(\star\star)$ implies $(\star)$ defined in Section 3.3.1, and recall that Conjecture II asserts that $(\star)$ holds for every primitive group $G \leqslant \mathrm{Sym}(\Omega)$ with $b(G) \geqslant 2$. We now propose the following strengthening of Conjecture II, which is stated as Conjecture 3.3.3 in Section 3.3.1 and Conjecture 6.5 in Section 6.1.

Conjecture 6.5.6. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group with $b(G) \geqslant 2$. Then property $(\star\star)$ holds.*

Theorem 6.5.7. *Conjecture 6.5.6 is equivalent to Conjecture II.*

Proof. Clearly, Conjecture 6.5.6 implies Conjecture II. Let $L \leqslant \mathrm{Sym}(\Gamma)$ be a counter-example for Conjecture 6.5.6. That is, there exist vertices $\alpha,\beta \in \Sigma(L)$ such that $N(\beta) \cap O = \emptyset$ for some almost-regular L_α-orbit O. Set $r := \mathrm{reg}(L)$, and let $G = L \wr S_r$ act on $\Omega = \Gamma^r$ with its product action. Then G is primitive, and by Theorem 6.2.6, we have $b(G) = b(L)$. It suffices to show that the two vertices $(\alpha,\dots,\alpha)$ and $(\beta,\dots,\beta)$ in $\Sigma(G)$ have no common neighbour.

Let $b := b(G)$, and suppose that the set

$$\{(\alpha,\dots,\alpha),(\alpha_{1,2},\dots,\alpha_{r,2}),(\alpha_{1,3},\dots,\alpha_{r,3})\dots,(\alpha_{1,b},\dots,\alpha_{r,b})\}$$

is a base for G. Then by Lemma 6.4.1, each $\{\alpha,\alpha_{i,2},\alpha_{i,3},\dots,\alpha_{i,b}\}$ is a base for L, and for any $i \neq j$, the b-tuples $(\alpha,\alpha_{i,2},\alpha_{i,3},\dots,\alpha_{i,b})$ and $(\alpha,\alpha_{j,2},\alpha_{j,3},\dots,\alpha_{j,b})$ are in distinct L-orbits. Since $r = \mathrm{reg}(L)$, there are at most r almost-regular L_α-orbits, so each set $\{\alpha_{1,i},\dots,\alpha_{r,i}\}$ meets every almost-regular L_α-orbit. In particular, for each $2 \leqslant i \leqslant b$, there exists $j \in [r]$ such that $\alpha_{j,i} \in O$, and so our assumption implies that $\alpha_{j,i} \notin N(\beta)$. By applying Lemma 6.4.1 once again, we see that, for each i, the point $(\alpha_{1,i},\dots,\alpha_{r,i}) \in \Omega$ is not in any almost-regular orbit of $G_{(\beta,\dots,\beta)}$. Therefore, the two vertices $(\alpha,\dots,\alpha)$ and $(\beta,\dots,\beta)$ in $\Sigma(G)$ have no common neighbour. This completes the proof. ■

We conclude with some evidence for Conjecture 6.5.6.

Proposition 6.5.8. *Let $G = \mathrm{L}_2(q)$, where $q \geqslant 4$, and consider the action of G on $\Omega = [G:H]$, where H is a subgroup of type $\mathrm{GL}_1(q) \wr S_2$. Then G satisfies $(\star\star)$.*

Proof. First assume q is even. As noted in Example 3.1.4, $b(G) = 2$ and G satisfies $(\star)$, which coincides with $(\star\star)$ since $r(G) = 1$.

For the remainder, we may assume q is odd, so $H = D_{q-1}$ and [14, Lemma 4.7] implies that $b(G) = 2$. As in Section 4.3.4, we may identify Ω with the set of unordered pairs of distinct 1-dimensional subspaces of $V = \mathbb{F}_q^2$.

Fix a basis $\{e_1,e_2\}$ for V and set $\beta = \{\langle e_1\rangle, \langle e_2\rangle\} \in \Omega$. Note that if $x \in G_\beta$, then x is the image (modulo scalars) of an element $A \in \mathrm{SL}_2(q)$ of the form

$$A = \begin{pmatrix} \lambda & \\ & \lambda^{-1} \end{pmatrix} \text{ or } \begin{pmatrix} & \lambda \\ -\lambda^{-1} & \end{pmatrix}$$

for some $\lambda \in \mathbb{F}_q^\times$, where the matrices are presented with respect to the basis $\{e_1,e_2\}$. We first determine the regular G_β-orbits (as recorded in Remark 4.5.15(ii), G_β has $(q+a)/4$ regular orbits, where $a = 7$ if $q \equiv 1 \pmod 4$, otherwise $a = 5$). Fix an element $\gamma \in \Omega$.

Suppose $\gamma = \{\langle e_1\rangle, \langle e_1 + se_2\rangle\}$ for some $s \in \mathbb{F}_q^\times$. Then an easy calculation shows that $\{\beta,\gamma\}$ is a base for G and the regular G_β-orbit containing γ is

$$R_1 = \{\{\langle e_1\rangle, \langle e_1 + ce_2\rangle\} : c \in \mathbb{F}_q^\times\}.$$

Similarly, if $\gamma = \{\langle e_2\rangle, \langle e_1 + se_2\rangle\}$ for some $s \in \mathbb{F}_q^\times$, then $\{\beta,\gamma\}$ is also a base for G and

$$R_2 = \{\{\langle e_2\rangle, \langle e_1 + ce_2\rangle\} : c \in \mathbb{F}_q^\times\}$$

is the regular G_β-orbit containing γ.

Now suppose $\gamma = \{\langle e_1 + se_2\rangle, \langle e_1 + te_2\rangle\}$, where $s,t \in \mathbb{F}_q^\times$ are distinct. By arguing as in the proof of Lemma 4.3.11 we calculate that $\{\beta,\gamma\}$ is a base for G if and only if $-st^{-1}$ is a non-square in $\mathbb{F}_q$. So let us assume $-st^{-1}$ is non-square and suppose $A \in \mathrm{SL}_2(q)$ fixes β. If $A = \mathrm{diag}(\lambda,\lambda^{-1})$, then

$$\gamma^A = \{\langle e_1 + \lambda^{-2}se_2\rangle, \langle e_1 + \lambda^{-2}te_2\rangle\},$$

whereas

$$\gamma^A = \{\langle e_1 - \lambda^{-2}s^{-1}e_2\rangle, \langle e_1 - \lambda^{-2}t^{-1}e_2\rangle\}$$

if $A = \begin{pmatrix} & \lambda \\ -\lambda^{-1} & \end{pmatrix}$. It follows that the regular G_β-orbit containing γ is

$$R_{s,t} = \{\{\langle e_1 + \lambda^2 se_2\rangle, \langle e_1 + \lambda^2 te_2\rangle\} : \lambda \in \mathbb{F}_q^\times\} \cup \{\{\langle e_1 - \lambda^2 s^{-1}e_2\rangle, \langle e_1 - \lambda^2 t^{-1}e_2\rangle\} : \lambda \in \mathbb{F}_q^\times\}.$$

We conclude that

$$\{R_1, R_2, R_{s,t} : s,t \in \mathbb{F}_q^\times,\ s \neq t \text{ and } -st^{-1} \text{ is a non-square in } \mathbb{F}_q\}$$

is the set of regular G_β-orbits. Note that we are not claiming that the orbits denoted $R_{s,t}$ are all distinct.

Fix an element $\alpha \in \Omega$ with $\alpha \neq \beta$ and let $N(\alpha)$ be the set of neighbours of α in the Saxl graph $\Sigma(G)$. In order to verify $(\star\star)$, we need to show that $N(\alpha)$ meets every regular G_β-orbit. There are several cases to consider.

First assume $\alpha = \{\langle e_1\rangle, \langle e_1 + be_2\rangle\}$ for some $b \in \mathbb{F}_q^\times$. It is easy to see that each $\gamma \in R_1 \setminus \{\alpha\}$ is contained in $N(\alpha)$ and we also have $\{\langle e_2\rangle, \langle e_1+be_2\rangle\} \in R_2 \cap N(\alpha)$. Now consider $R_{s,t}$, where $s,t \in \mathbb{F}_q^\times$ are distinct and $-st^{-1}$ is non-square. Note that either $-bs$ or bt^{-1} is a square in $\mathbb{F}_q$, so there are two cases to consider. If $-bs = \mu^2$ is a square then $b = -\mu^2 s^{-1}$ and

$$\{\langle e_1 - \mu^2 s^{-1} e_2\rangle, \langle e_1 - \mu^2 t^{-1} e_2\rangle\} \in R_{s,t} \cap N(\alpha).$$

On the other hand, if $bt^{-1} = \mu^2$ then $b = \mu^2 t$ and

$$\{\langle e_1 + \mu^2 s e_2\rangle, \langle e_1 + \mu^2 t e_2\rangle\} \in R_{s,t} \cap N(\alpha).$$

Therefore, $N(\alpha)$ meets every regular G_β-orbit as required.

A very similar argument applies when $\alpha = \{\langle e_2\rangle, \langle e_1 + be_2\rangle\}$ for some $b \in \mathbb{F}_q^\times$ and we omit the details.

Finally, let us assume $\alpha = \{\langle e_1 + s_0 e_2\rangle, \langle e_1 + t_0 e_2\rangle\}$, where $s_0, t_0 \in \mathbb{F}_q^\times$ are distinct. Note that $\{\langle e_i\rangle, \langle e_1 + s_0 e_2\rangle\} \in R_i \cap N(\alpha)$ for $i = 1,2$, so it just remains to show that $N(\alpha)$ meets each $R_{s,t}$. As before, either $-s_0 s$ or $s_0 t^{-1}$ is a square in $\mathbb{F}_q^\times$ and we can repeat the above argument in order to construct an element in $R_{s,t} \cap N(\alpha)$. ■

6.6 General product type groups

So far in this chapter, we have focussed on product type groups of the form $G = L \wr P$. As one might expect, the study of bases in the general setting $G \leqslant L \wr P$ is more difficult and this is essentially unchartered territory. In this final section, we take the first steps in this direction by focussing on the special case where $P \leqslant G$, which already turns out to be rather challenging. Our main results are Theorems 6.6.4 and 6.6.11, which describe the groups with $b(G) = 2$ in certain families of product type groups with soluble point stabilisers. Note that Theorem 6.6.4 is stated as Theorem 6.6 in Section 6.1.

6.6.1 Preliminaries

Let us fix the set-up and notation we will work with throughout this section. As before, $G \leqslant L \wr P \leqslant \mathrm{Sym}(\Omega)$ is a product type primitive group on $\Omega = \Gamma_1 \times \cdots \times \Gamma_k = \Gamma^k$, with socle $T_1 \times \cdots \times T_k = T^k$ and point stabiliser H. Here $k \geqslant 2$, $P \leqslant S_k$ is transitive and $L \leqslant \mathrm{Sym}(\Gamma)$ is a primitive group with socle T and point stabiliser J, which is either almost simple or diagonal type. In addition, we may assume P is the permutation group on $[k] = \{1, \ldots, k\}$ induced by the conjugation action of G on the set of k factors of the socle T^k. In view of Remark 6.2.4, we may (and will) also assume that L is the group induced by G on Γ_1. In particular, this means that both L and P are uniquely determined by G. As explained in Remark 6.2.5, if H is soluble then J and P are also soluble.

Since the case $G = L \wr P$ has been studied in the previous sections, we will assume $G < L \wr P$. More importantly, we will also assume that G contains P, which means that we adopt the following hypothesis for the remainder of this section (in particular, note that $L \neq T$).

Hypothesis 6.6.1. *$G \leqslant \mathrm{Sym}(\Omega)$ is a product type primitive group with $T \wr P < G < L \wr P$.*

In the setting of Hypothesis 6.6.1, we introduce some new notation. Given an element $g = (g_1,\dots,g_k) \in L^k \cap G$, let $\tau(g)$ be the number of coordinates of g that are contained in T and set

$$\tau(G) = \max\{\tau(g) : g \in (L^k \cap G) \setminus T^k\} \in \{0,1,\dots,k-1\}. \tag{6.6.1}$$

For example, if $L = \langle T, x\rangle$ and $G = \langle T^k, (x,\dots,x), P\rangle$, then $\tau(G) = 0$. Note that if $\tau(G) = k-1$ and G satisfies Hypothesis 6.6.1, then $|L:T|$ is composite (indeed, if $|L:T|$ is a prime then we get $G = L \wr P$).

As before, let $r(L)$ and $r(T)$ denote the number of regular suborbits of L and T on Γ, respectively (recall that T acts transitively on Γ since L is primitive).

We begin with the following result, which gives a sufficient condition for a group satisfying Hypothesis 6.6.1 to admit a base of size 2.

Proposition 6.6.2. *Assume Hypothesis 6.6.1 and let $m \in \{1,\dots,D(P)\}$ be minimal such that there exists a distinguishing partition $\{\pi_1,\dots,\pi_{D(P)}\}$ for P with $|\bigcup_{i=1}^m \pi_i| > \tau(G)$. Then $b(G) = 2$ if*

(i) $r(L) \geqslant m$; and

(ii) $r(T) \geqslant m(|L:T|-1) + D(P)$.

Proof. Suppose the bounds in (i) and (ii) are satisfied. Set $D = D(P)$ and fix an element $\alpha = (\alpha_0,\dots,\alpha_0) \in \Omega$ for some $\alpha_0 \in \Gamma$. Since $r(L) \geqslant m$, we may choose elements $\gamma_1,\dots,\gamma_m$ in Γ that are contained in distinct regular L_{α_0}-orbits. Now each of these L_{α_0}-orbits is a union of $|L:T|$ regular T_{α_0}-orbits, so the bound in (ii) implies that we can find additional points $\gamma_{m+1},\dots,\gamma_D$ in Γ such that each element in $\{\gamma_1,\dots,\gamma_D\}$ is contained in a distinct regular T_{α_0}-orbit. Define $\beta = (\beta_1,\dots,\beta_k) \in \Omega$, where $\beta_j = \gamma_i$ if $j \in \pi_i$. We claim that $\{\alpha,\beta\}$ is a base for G.

Let $x \in G_\alpha \cap G_\beta$ and write $x = z\sigma$, where $z = (z_1,\dots,z_k) \in L^k \cap G$ and $\sigma \in P$. Recall that $\tau(z)$ denotes the number of coordinates z_i that are contained in T and observe that $z \in T^k$ if $\tau(z) > \tau(G)$ (see (6.6.1)). By Lemma 6.4.1, we see that $\{\alpha,\beta\}$ is a base for $T \wr P$, so it suffices to show that $\tau(z) > \tau(G)$.

Fix $j \in \pi_1$ and notice that $z_j \in L_{\alpha_0}$ since x fixes α. Next observe that the j^σ-th coordinate of β^x is $\beta_j^{z_j} = \gamma_1^{z_j}$, which is equal to $\beta_{j^\sigma} \in \{\gamma_1,\dots,\gamma_D\}$ since x fixes β. By construction, none of the elements $\gamma_2,\dots,\gamma_D$ are contained in the L_{α_0}-orbit of γ_1, whence $\beta_{j^\sigma} = \gamma_1$ and thus $z_j \in L_{\alpha_0} \cap L_{\gamma_1} = 1$. In the same way, we deduce that $z_j = 1$ for all $j \in \bigcup_{i=1}^m \pi_i$ and thus $\tau(z) \geqslant |\bigcup_{i=1}^m \pi_i| > \tau(G)$. The result follows. ■

Remark 6.6.3. Note that Proposition 6.6.2 can be applied when $G = L \wr P$ and $L \neq T$. Here $\tau(G) = k-1$, so $m = D(P)$ and the proposition asserts that $b(G) = 2$ if $r(L) \geqslant D(P)$ and $r(T) \geqslant |L:T|$. Here the condition $r(L) \geqslant D(P)$ coincides with the one in Theorem 6.2.6, while the bound $r(T) \geqslant |L:T|$ always holds when $b(L) = 2$. So in some sense, Proposition 6.6.2 can be viewed as a generalisation of Theorem 6.2.6 for base-two groups. However, it is worth noting that there are groups with $b(G) = 2$ that do not satisfy the bounds labelled (i) and (ii) in the proposition. For example, the proof of Theorem 6.6.4 shows that there are groups G satisfying Hypothesis 6.6.1 with $k = m = 2$, $r(L) = 1$ and $b(G) = 2$.

Let G be a group satisfying Hypothesis 6.6.1 and note that $b(G) = 2$ only if $b(T \wr P) = 2$, so we are interested in the groups with $b(T) = 2$. Moreover, in view of Theorem 6.2.6, we may assume $r(T) \geqslant D(P)$. Recall that if H is soluble, then L is almost simple with soluble point stabilisers and as a consequence of [14, Theorem 2] we observe that $b(L) \in \{2,3\}$. So in the case where G has soluble point stabilisers, as in the two main results of this section, there are two cases to consider according to the base size of L on Γ. To simplify the analysis, we will focus on the groups with $b(L) = 2$, which allows us to bring Proposition 6.6.2 into play. However, it is worth noting that there are groups of this form with $b(L) = 3$ and $b(G) = 2$. Indeed, we refer the reader to Example 6.6.12 at the end of the section for an infinite family of groups G with soluble point stabilisers where we have $b(L) = 3$ and $b(G) = 2$.

6.6.2 Base-two groups with $k = 2$

Our first main result is Theorem 6.6.4 below. Here we assume $k = b(L) = 2$, so $P = S_2$ and $D(P) = 2$. If $r(L) \geqslant 2$ then $b(L \wr P) = 2$ by Theorem 6.2.6, so we may as well assume $r(L) = 1$. Define $\tau(G)$ as in (6.6.1) and note that $\tau(G) \in \{0,1\}$. If $\tau(G) = 0$, then $m = 1$ in Proposition 6.6.2 and we deduce that $b(G) = 2$ if $r(T) \geqslant |L:T|+1$ (recall that the slightly weaker bound $r(T) \geqslant |L:T|$ always holds when $b(L) = 2$). On the other hand, if $\tau(G) = 1$ then $m = 2$ and thus Proposition 6.6.2 is not useful when $r(L) = 1$. Also recall that $|L:T|$ is composite if $\tau(G) = 1$ (otherwise $G = L \wr P$).

The following result is stated as Theorem 6.6 in Section 6.1.

Theorem 6.6.4. *Assume Hypothesis 6.6.1, where $k = b(L) = 2$, H is soluble and J is a point stabiliser in L. Then $b(G) \leqslant 3$, with equality if and only if $|L \wr P : G| = 2$ and one of the following holds:*

(i) $(L, J) = (\mathrm{M}_{10}, 5{:}4)$ *or* $(\mathrm{J}_2.2, 5^2{:}(4 \times S_3))$.

(ii) $L = \mathrm{PGU}_4(3)$ *and J is of type* $\mathrm{GU}_1(3) \wr S_4$.

Proof. Here $P = S_2$ and $D(P) = 2$. By Lemma 6.3.1 we have $b(L \wr P) \leqslant b(L)+1$ and thus $b(G) \leqslant 3$. As explained in Remark 6.2.5, we note that J is soluble and thus L is almost simple. If $r(L) \geqslant 2$ then $b(L \wr P) = 2$ by Theorem 6.2.6, so we may assume $r(L) = 1$ and then inspect the possibilities for

(L,J) recorded in Tables 4.7 and 4.8. As discussed above, Proposition 6.6.2 implies that $b(G)=3$ only if $r(T)=|L:T|$ or $\tau(G)=1$, so there are two cases to consider.

First assume $r(T)=|L:T|$. By inspecting Tables 4.7 and 4.8, we see that $(L,J)=(\mathrm{M}_{10},5{:}4)$ or $(L,J)=(\mathrm{J}_2.2,5^2{:}(4\times S_3))$, so in both cases we have $|L:T|=2$ and $|L\wr P:G|=2$. More precisely, if we write $L=\langle T,a\rangle$ then we may assume $G=\langle T^2,(a,a),P\rangle$. Using MAGMA, we can construct G as a permutation group on $\Omega=\Gamma^2$ with point stabiliser H and we can then find a complete set R of (H,H) double coset representatives, implementing the computational approach described in Section 4.2.4. In both cases, it is routine to check that $|HxH|<|H|^2$ for all $x\in R$ and we conclude that $b(G)=3$ as claimed.

For the remainder, let us assume $\tau(G)=1$ and recall that $|L:T|\geqslant 4$ is composite since G is a proper subgroup of $L\wr P$. By inspecting Tables 4.7 and 4.8 we deduce that there are four possibilities for (L,J):

(a) $L=\mathrm{U}_3(5){:}S_3$ and J is of type $\mathrm{GU}_1(5)\wr S_3$.

(b) $L=\mathrm{L}_3(4){:}D_{12}$ and J is of type $\mathrm{GL}_1(4^3)$.

(c) $L=\mathrm{P\Omega}_8^+(3){:}2^2$ and J is of type $\mathrm{O}_4^+(3)\wr S_2$.

(d) $L=\mathrm{U}_4(3){:}[4]$ and J is of type $\mathrm{GU}_1(3)\wr S_4$.

In cases (a) and (b), we can use MAGMA to check that $b(G)=2$ (here we construct G and H as above, and then we use random search to find an element $g\in G$ with $H\cap H^g=1$). Now let us turn to cases (c) and (d), so $|L:T|=4$ and $|L\wr P:G|\in\{2,4,8\}$. In fact, one can check that the condition $\tau(G)=1$ forces $|L\wr P:G|=2$. More precisely, if $L=T{:}\langle a,b\rangle=T{:}2^2$ then up to permutation isomorphism, we may assume that

$$G=\langle T^2,(a,a),(b,1),P\rangle. \tag{6.6.2}$$

Similarly, if $L=\mathrm{PGU}_4(3)=T{:}\langle a\rangle$, then we can take

$$G=\langle T^2,(a,a),(a^2,1),P\rangle. \tag{6.6.3}$$

First assume $L=T{:}\langle a,b\rangle=T{:}2^2$, so (6.6.2) holds and $T=\mathrm{P\Omega}_8^+(3)$ or $\mathrm{U}_4(3)$. We claim that $b(G)=2$. To see this, fix $\alpha_0\in\Gamma$ and let $\gamma_1,\ldots,\gamma_t$ be representatives of the regular T_{α_0}-orbits on Γ, where $t=r(T)$ (as recorded in Table 4.7, we have $t=12$ if $T=\mathrm{P\Omega}_8^+(3)$ and $t=11$ for $T=\mathrm{U}_4(3)$). We may assume that $L_{\alpha_0}\cap L_{\gamma_1}=1$ and $|L_{\alpha_0}\cap L_{\gamma_2}|=2$ (the existence of γ_2 can be checked using MAGMA). Now $T_{\alpha_0}\cap T_{\gamma_2}=1$, so without loss of generality we may assume that $\{\alpha_0,\gamma_2\}$ is a base for $T{:}\langle b\rangle$. Suppose $x=(z_1,z_2)\sigma\in G$ fixes $\alpha=(\alpha_0,\alpha_0)$ and $\beta=(\gamma_1,\gamma_2)$, where $z_1,z_2\in L$ and $\sigma\in P$. Then $z_i\in L_{\alpha_0}$ for $i=1,2$ and we note that $\sigma=1$ since γ_1 and γ_2 are contained in distinct L_{α_0}-orbits. Therefore, $z_1\in L_{\alpha_0}\cap L_{\gamma_1}=1$ and thus $z_1=1$. From the description of G in (6.6.2), it follows that $z_2\in T{:}\langle b\rangle$ fixes α_0 and γ_2, whence $z_2=1$ and thus $x=1$. This justifies the claim.

Finally, let us assume $L = \mathrm{PGU}_4(3) = T{:}\langle a \rangle$, so the structure of G is given in (6.6.3). We claim that $b(G) = 3$. As before, fix $\alpha_0 \in \Gamma$ and set $\alpha = (\alpha_0, \alpha_0)$ and $\beta = (\gamma_1, \gamma_2)$, where γ_1 and γ_2 are contained in regular T_{α_0}-orbits. It suffices to show that the pointwise stabiliser of α and β in G is non-trivial. It will be useful to observe that a given element $(z_1, z_2) \in L^2$ is contained in G if and only if $z_1 z_2 \in T{:}\langle a^2 \rangle$.

First assume $\{\alpha_0, \gamma_1\}$ is not a base for L. Then using MAGMA we see that $|L_{\alpha_0} \cap L_{\gamma_1}| \in \{2,4\}$, so there is an involution $y \in L$ fixing α_0 and γ_1. Since every involution in L is contained in $T{:}\langle a^2 \rangle$, it follows that $(y,1) \in G$ fixes α and β. An entirely similar argument applies if $\{\alpha_0, \gamma_2\}$ is not a base for L.

Finally, suppose $\{\alpha_0, \gamma_1\}$ and $\{\alpha_0, \gamma_2\}$ are both bases for L, which means that γ_1 and γ_2 are contained in the unique regular L_{α_0}-orbit on Γ. Therefore, there exists $z_1 \in L_{\alpha_0}$ such that $\gamma_1^{z_1} = \gamma_2$ and thus $(z_1, z_1^{-1})\sigma \in G$ is a non-trivial element fixing α and β, where $\sigma = (1,2) \in P$. This completes the proof of the theorem. ■

6.6.3 Base-two groups with $\tau(G) = 0$

For the remainder of Section 6.6, we will continue to assume that Hypothesis 6.6.1 holds and $b(L) = 2$, but we will not impose any conditions on k. In exchange, we will focus on the groups with $\tau(G) = 0$ (see (6.6.1)), which is a natural restriction on the structure of G. In particular, this means that if $x = z\sigma \in G$, where $z = (z_1, \ldots, z_k) \in L^k \cap G$ and $\sigma \in P$, then either $z \in T^k$ or $z_j \in L \setminus T$ for all j.

Our main result in this setting is Theorem 6.6.11 and the proof will require several preliminary results. We begin with an easy corollary of Proposition 6.6.2.

Corollary 6.6.5. *Assume Hypothesis 6.6.1, where $b(L) = 2$ and $\tau(G) = 0$. If $b(G) \geqslant 3$, then*

$$|L:T| \leqslant r(T) \leqslant |L:T| + D(P) - 2.$$

Proof. This follows immediately from Proposition 6.6.2, noting that $m = 1$ in the statement of the proposition. ■

Remark 6.6.6. Let us apply Corollary 6.6.5 in the case where H is soluble. Suppose $b(G) \geqslant 3$, so $r(T) \leqslant |L:T| + D(P) - 2$ by the corollary. Now $r(T) \geqslant r(L)|L:T|$ and the solubility of P implies that $D(P) \leqslant 5$ (see Theorem 6.2.1), whence

$$(r(L)-1)|L:T| \leqslant D(P) - 2 \leqslant 3$$

and either $r(L) = 1$, or $r(L) = 2$ and $|L:T| \in \{2,3\}$. In particular, the possibilities for (L,J) can be read off from Tables 4.7 and 4.8, and we find that $r(L) = 2$, $|L:T| \in \{2,3\}$ and $r(T) \leqslant |L:T| + 3$ if and only if one of the following holds:

(a) $L = \mathrm{L}_3(3).2$ and J is of type $\mathrm{O}_3(3)$.

(b) $L = \mathrm{L}_2(27).3$ and J is of type $\mathrm{GL}_1(27^2)$.

(c) $(L,J) = (\mathrm{M}_{10}, SD_{16})$.

Note that if P is primitive (as in Theorem 6.6.11), then $D(P) \leqslant 4$ by Theorem 6.2.3, so the corollary implies that $r(T) \leqslant |L:T|+2$ and this eliminates cases (a) and (b).

In order to state our next result, we define the following condition on the group $P \leqslant S_k$, with respect to a fixed integer m in the range $D(P) \leqslant m \leqslant k$:

(†) *If $\{\pi_1,\ldots,\pi_m\}$ is a distinguishing partition for P, then for all i, there exists $\rho \in P$ such that $\pi_i \cap \pi_i^\rho$ is empty.*

Note that if there exists a distinguishing partition $\{\pi_1,\ldots,\pi_m\}$ for P with $|\pi_i| > k/2$ for some i, then $\pi_i \cap \pi_i^\rho$ is non-empty for all $\rho \in P$ and thus (P,m) does not satisfy (†).

Remark 6.6.7. Recall that $\mathscr{P}_m([k])$ is the set of ordered partitions of $[k]$ into m parts, where some of the parts are allowed to be empty. It is not difficult to see that if P has a unique regular orbit on $\mathscr{P}_m([k])$ then (P,m) satisfies the condition in (†).

Proposition 6.6.8. *Assume Hypothesis 6.6.1, where $b(L) = 2$ and $\tau(G) = 0$. If $b(G) \geqslant 3$, then* (†) *holds for all $D(P) \leqslant m \leqslant \min\{k, r(T)\}$.*

Proof. This is similar to the proof of Proposition 6.6.2. Suppose there exists a distinguishing partition $\{\pi_1,\ldots,\pi_m\}$ for P such that $D(P) \leqslant m \leqslant r(T)$ and $\pi_1 \cap \pi_1^\rho$ is non-empty for all $\rho \in P$. Fix $\alpha_0 \in \Gamma$. Since $r(T) \geqslant m$, we can choose elements $\gamma_1,\ldots,\gamma_m$ that are contained in distinct regular T_{α_0}-orbits on Γ, so each pair $\{\alpha_0,\gamma_i\}$ is a base for T. In addition, we may assume that $\{\alpha_0,\gamma_1\}$ is a base for L. Define $\alpha = (\alpha_0,\ldots,\alpha_0)$ and $\beta = (\beta_1,\ldots,\beta_k)$ as elements of Ω, where $\beta_j = \gamma_i$ if $j \in \pi_i$. In order to prove the proposition, it suffices to show that $\{\alpha,\beta\}$ is a base for G.

Let $x \in G_\alpha \cap G_\beta$ and write $x = z\sigma$, where $z = (z_1,\ldots,z_k) \in L^k \cap G$ and $\sigma \in P$. Note that each z_j is contained in L_{α_0}. If $z \in T^k$ then $x \in T \wr P$ and thus $x = 1$ since we know that $\{\alpha,\beta\}$ is a base for $T \wr P$ by Lemma 6.4.1. Therefore, since $\tau(G) = 0$, we may assume $z_j \in L \setminus T$ for all j.

Since $\pi_1 \cap \pi_1^\sigma$ is non-empty, there exists $j \in \pi_1$ such that $j^\sigma \in \pi_1$. Then $\beta_j = \gamma_1$ and by considering the j^σ-th coordinate of β^x we deduce that $\gamma_1 = \beta_{j^\sigma} = \beta_j^{z_j} = \gamma_1^{z_j}$. Therefore, $z_j \in L_{\alpha_0} \cap L_{\gamma_1} = 1$ and thus $z_j = 1$, which contradicts the fact that $z_j \in L \setminus T$. The result follows. ■

Notice that P is primitive in the statement of Theorem 6.6.11. Therefore, in view of Theorem 6.2.3, we have a special interest in the case $D(P) = 2$, which means that P has a regular orbit on the power set of $[k] = \{1,\ldots,k\}$. This leads us naturally to consider the following condition, which coincides with (†) when $m = 2$:

(‡) *If the setwise stabiliser of $\Lambda \subseteq [k]$ in P is trivial, then $\Lambda^\sigma = [k] \setminus \Lambda$ for some $\sigma \in P$.*

Clearly, if $D(P) = 2$ then (‡) holds only if k is even and every subset of $[k]$ with trivial setwise stabiliser in P has size $k/2$. In other words, (‡) holds only if P has no regular orbit on the set X defined in (6.4.2). Therefore, if P is primitive and $D(P) = 2$, then Proposition 6.4.9 implies that (‡) holds if and only if $(k,P) = (2,S_2)$ or $(16,2^4{:}\mathrm{O}_4^-(2))$. We will return to this observation in the proof of Theorem 6.6.11 below.

The following result is an immediate corollary of Proposition 6.6.8.

Corollary 6.6.9. *Assume Hypothesis 6.6.1, where $b(L) = D(P) = 2$ and $\tau(G) = 0$. If $b(G) \geqslant 3$, then (‡) holds.*

The final ingredient for the proof of Theorem 6.6.11 is provided by the following lemma.

Lemma 6.6.10. *Assume Hypothesis 6.6.1, where $b(L) = |L:T| = 2$, $\tau(G) = 0$ and $P = S_{r(T)}$. Then $b(G) \geqslant 3$.*

Proof. Set $k = r(T)$ and fix $\alpha_0 \in \Gamma$. Recall that an element $z = (z_1,\dots,z_k) \in L^k$ is contained in G if and only if $z \in T^k$ or $z_i \in L \setminus T$ for all i. In view of Lemma 6.4.1, it suffices to show that $\alpha = (\alpha_0,\dots,\alpha_0)$ and $\beta = (\gamma_1,\dots,\gamma_k)$ do not form a base for G, where the γ_i are contained in distinct regular T_{α_0}-orbits.

Since $|L:T| = 2$, each regular L_{α_0}-orbit is a union of two regular T_{α_0}-orbits. This allows us to define $r = r(L)$ distinct pairs $\{s,t\} \subseteq \{1,\dots,k\}$, where $\{s,t\}$ is a pair if and only if γ_s and γ_t are in the same regular L_{α_0}-orbit. Let $\{s_1,t_1\},\dots,\{s_r,t_r\}$ be the pairs arising in this way. For each $i \in \{1,\dots,r\}$, there exist $z_{s_i}, z_{t_i} \in L_{\alpha_0}$ such that $\gamma_{s_i}^{z_{s_i}} = \gamma_{t_i}$ and $\gamma_{t_i}^{z_{t_i}} = \gamma_{s_i}$. In addition, if $\ell \notin \{s_1,t_1,\dots,s_r,t_r\}$ then there exists $1 \neq z_\ell \in L_{\alpha_0}$ such that $\gamma_\ell^{z_\ell} = \gamma_\ell$. By construction, all of the elements z_{s_i}, z_{t_i} and z_ℓ are contained in $L \setminus T$. Therefore, if we define $z = (z_1,\dots,z_k) \in L^k$, then $z \in G$. Finally, we note that $1 \neq z\sigma \in G_\alpha \cap G_\beta$, where $\sigma = (s_1,t_1)\cdots(s_r,t_r) \in P$, and we conclude that $\{\alpha,\beta\}$ is not a base for G. ■

Theorem 6.6.11. *Assume Hypothesis 6.6.1, where $b(L) = 2$, P is primitive, $\tau(G) = 0$ and H is soluble. Then $b(G) \leqslant 3$, with equality if and only if (L,J) is one of the cases in Table 6.2 and either $r(T) < D(P)$, or $P = S_k$, $k \in \{2,3,4\}$ and $r(T) = D(P) = k$.*

Proof. First note that L is almost simple with soluble point stabiliser J, and P is also soluble (see Remark 6.2.5). By Lemma 6.3.1 we have $b(L \wr P) \leqslant b(L) + 1$ and thus $b(G) \leqslant 3$. Since P is primitive, Theorem 6.2.3 implies that either $D(P) = 2$, or one of the following holds:

(a) $D(P) = 3$ and $(k,P) = (4,A_4)$, $(3,S_3)$ or one of 8 cases listed in [109, Theorem 2] with P soluble.

(b) $D(P) = 4$ and $(k,P) = (4,S_4)$.

$r(T)$	L	Type of J	Conditions
2	M_{10}	5:4	
	$\mathrm{J}_2.2$	$5^2{:}(4 \times S_3)$	
3	$\mathrm{L}_3(4).2$	$\mathrm{GU}_3(2)$	$L \neq \mathrm{P\Sigma L}_3(4)$
	$\mathrm{PGL}_2(11)$	$2_{-}^{1+2}.\mathrm{O}_2^{-}(2)$	
	$\mathrm{PGL}_2(7)$	D_{12}	
4	$\mathrm{PGL}_2(q)$	$D_{2(q-1)}$	$q \in \{9,11\}$
	$G_2(3).2$	$\mathrm{SL}_2(3)^2$	
	S_7	$\mathrm{AGL}_1(7)$	
	M_{10}	SD_{16}	

Table 6.2: The groups (L,J) in Theorem 6.6.11

First assume $r(T) < D(P)$. Here Theorem 6.2.6 gives $b(T \wr P) \geqslant 3$, so $b(G) = 3$ and the possibilities for (L,J) can be read off from Tables 4.7 and 4.8, noting that $L \neq T$ since we are assuming G satisfies Hypothesis 6.6.1. In this way, we obtain the cases recorded in Table 6.2 with $r(T) \in \{2,3\}$.

For the remainder, we will assume $r(T) \geqslant D(P)$. We now divide the proof into three cases, according to $D(P)$.

Case 1. $D(P) = 2$.

First assume $D(P) = 2$. By combining Theorem 6.2.6 and Corollary 6.6.5, we deduce that $b(G) = 3$ only if $r(L) = 1$ and $r(T) = |L:T|$. Therefore, by inspecting Table 4.7 we see that $(L,J) = (\mathrm{M}_{10}, 5{:}4)$ or $(\mathrm{J}_2.2, 5^2{:}(4 \times S_3))$ are the only possibilities, and in both cases we have $|L:T| = 2$. If $b(G) = 3$ then Corollary 6.6.9 implies that the condition (‡) holds, which means that P has no regular orbit on the set X defined in (6.4.2). In addition, since P is soluble, Proposition 6.4.9 implies that $(k,P) = (2,S_2)$ and we conclude that $b(G) = 3$ via Lemma 6.6.10.

Case 2. $D(P) = 3$.

Next assume $D(P) = 3$, so the possibilities for (k,P) are described in case (a) above. Suppose $b(G) = 3$ and first observe that Proposition 6.6.8 implies that (†) holds with $m = 3$. By considering the cases in (a), with the aid of MAGMA it is straightforward to check that (†) holds with $m = 3$ if and only if $(k,P) = (3,S_3)$, $(4,A_4)$ or $(9,\mathrm{AGL}_2(3))$.

Next observe that $r(T) = |L:T|$ or $|L:T| + 1$ by Corollary 6.6.5. Therefore, $r(L) = 1$ and by inspecting Table 4.7 we deduce that (L,J) is one of the three cases recorded in Table 6.2 with $r(T) = |L:T| + 1 = 3$. In particular, if $(k,P) = (3,S_3)$ then $b(G) = 3$ in both cases by Lemma 6.6.10. We now consider the two remaining possibilities for (k,P) in turn.

Suppose $(k,P) = (9,\mathrm{AGL}_2(3))$. Using MAGMA, we can find a distinguishing partition $\{\pi_1,\pi_2,\pi_3\}$ for P such that $|\pi_i| = i+1$ for all i. Let (L,J) be one of the relevant cases in Table 6.2 and fix $\alpha_0 \in \Gamma = [L:J]$. Since $r(T) = 3$, there exist points $\gamma_1,\gamma_2,\gamma_3$ that are contained in distinct regular T_{α_0}-orbits on Γ. In addition, we may assume that $\{\alpha_0,\gamma_1\}$ is not a base for L, whereas γ_2 and γ_3 are in the unique regular L_{α_0}-orbit on Γ. Set $\alpha = (\alpha_0,\ldots,\alpha_0)$ and $\beta = (\beta_1,\ldots,\beta_k)$ in $\Omega = \Gamma^k$, where

$\beta_j = \gamma_i$ if $j \in \pi_i$. We claim that $\{\alpha,\beta\}$ is a base for G, which is incompatible with our assumption that $b(G) = 3$. To see this, suppose $x \in G_\alpha \cap G_\beta$ and write $x = z\sigma$, where $z = (z_1,\dots,z_k) \in L^k \cap G$ and $\sigma \in P$. Suppose $j \in \pi_1$, so $\beta_j = \gamma_1$. Since γ_2 and γ_3 are not in the L_{α_0}-orbit of γ_1, it follows that $\beta_j^{z_j} = \gamma_1$. Therefore, σ fixes π_1 and $\pi_2 \cup \pi_3$ (setwise). As a consequence, since $|\pi_2| = 3$ and $|\pi_3| = 4$, we deduce that there exists $j \in \pi_3$ such that $j^\sigma \in \pi_3$. Therefore, $z_j \in L_{\alpha_0} \cap L_{\gamma_3}$ and thus $z_j = 1$. At this point, the condition $\tau(G) = 0$ forces $z \in T^k$ and thus Lemma 6.4.1 implies that $x = 1$. Therefore, $\{\alpha,\beta\}$ is indeed a base for G and so the case $(k,P) = (9,\mathrm{AGL}_2(3))$ is eliminated.

An almost identical argument also eliminates the case $(k,P) = (4,A_4)$, working with a distinguishing partition $\{\pi_1,\pi_2,\pi_3\}$ for P with $|\pi_1| = |\pi_2| = 1$ and $|\pi_3| = 2$. We omit the details.

Case 3. $D(P) = 4$.

Finally, let us assume $D(P) = 4$ and $b(G) = 3$, in which case $(k,P) = (4,S_4)$ (see case (b) above) and Corollary 6.6.5 implies that $|L:T| \leqslant r(T) \leqslant |L:T| + 2$. Therefore $r(T) \leqslant 2|L:T|$ and thus $r(L) \in \{1,2\}$. By inspecting Tables 4.7 and 4.8, we deduce that either (L,J) is one of the cases in Table 6.2 with $r(T) = |L:T| + 2 = 4$, or $L = \Omega_8^+(2){:}3$ and J is of type $\mathrm{O}_2^-(2) \times \mathrm{GU}_3(2)$. In the former case, Lemma 6.6.10 shows that $b(G) = 3$, so it just remains to eliminate the latter possibility.

Suppose $L = T{:}\langle a\rangle = \Omega_8^+(2){:}3$ and J is of type $\mathrm{O}_2^-(2) \times \mathrm{GU}_3(2)$, so $r(L) = 1$ and $r(T) = 5$. Since $|L:T| = 3$ is a prime and we are assuming that $\tau(G) = 0$ and $P = S_4$, it follows that

$$G = \langle T^4, (a,a,a,a), P\rangle,$$

so an element $(z_1,z_2,z_3,z_4) \in L^4$ is contained in G if and only if each z_i is in the same coset of T in L. Fix $\alpha_0,\gamma_1,\dots,\gamma_4 \in \Gamma$, where the γ_i are contained in distinct regular T_{α_0}-orbits and $\{\alpha_0,\gamma_i\}$ is a base for L if and only if $i \in \{1,2\}$. Notice that if $i \in \{3,4\}$ then $|L_{\alpha_0} \cap L_{\gamma_i}| = 3$, which implies that the L_{α_0}-orbit and T_{α_0}-orbit of γ_i are equal (in particular, γ_3 and γ_4 are in distinct L_{α_0}-orbits). Set $\alpha = (\alpha_0,\alpha_0,\alpha_0,\alpha_0)$ and $\beta = (\gamma_1,\gamma_2,\gamma_3,\gamma_4)$ in $\Omega = \Gamma^4$. We claim that $\{\alpha,\beta\}$ is a base for G.

Assume $x \in G_\alpha \cap G_\beta$ and write $x = z\sigma$, where $z = (z_1,z_2,z_3,z_4) \in L^4 \cap G$ and $\sigma \in P$. Since none of the points γ_1, γ_2 and γ_4 are in the same L_{α_0}-orbit as γ_3, we deduce that $3^\sigma = 3$. Similarly, $4^\sigma = 4$. Suppose $\sigma = (1,2)$. Then $\gamma_1^{z_1} = \gamma_2$ and $\gamma_2^{z_2} = \gamma_1$, which implies that $z_1, z_2 \in L \setminus T$. Moreover, $z_1z_2 \in L_{\alpha_0} \cap L_{\gamma_1} = 1$, so $z_1 = z_2^{-1}$ and we deduce that z_1 and z_2 are contained in different cosets of T in L. But this means that $z \notin G$ and we have reached a contradiction. This forces $\sigma = 1$. Finally, since $\{\alpha_0,\gamma_1\}$ is a base for L we deduce that $z_1 = 1$ and thus $z \in T^4$. Since each $\{\alpha_0,\gamma_i\}$ is a base for T, we conclude that $z = 1$ and the proof of both the claim and the theorem is complete. ■

6.6.4 Final remarks

We conclude by briefly discussing the general problem of determining the base-two product type groups with soluble point stabilisers. Let $G \leqslant L \wr P$ be such a group with socle T^k, and adopt all the usual notation as before. The case where $G = L \wr P$ is handled in Theorem 6.1, so we may assume $G < L \wr P$ and $b(L \wr P) \geqslant 3$. Continuing with the main theme of Section 6.6, let us also assume that Hypothesis 6.6.1 holds. Here $L \neq T$ and $b(G) = 2$ only if $b(T \wr P) = 2$, so $r(T) \geqslant D(P)$ and we deduce that $b(L) \in \{2,3\}$ as a consequence of [14, Theorem 2]. In this setting, we have handled the cases

(a) $b(L) = k = 2$ (see Theorem 6.6.4); and

(b) $b(L) = 2$, P is primitive and $\tau(G) = 0$ (see Theorem 6.6.11).

So even under the assumption $b(L) = 2$, there is more work to be done here and it would be interesting to see if it is possible to relax the conditions on P and $\tau(G)$ in case (b). For example, it might be fruitful to consider the groups with $\tau(G) = k-1$ as a starting point.

As the following example demonstrates, we can also find base-two groups under Hypothesis 6.6.1 when $b(L) = 3$.

Example 6.6.12. Take $L = \mathrm{P\Gamma L}_2(q) = T{:}\langle a,b\rangle = T{:}2^2$ and let J be a maximal subgroup of type $\mathrm{GL}_1(q) \wr S_2$, where $q = p^2$, $p \geqslant 3$ is a prime and $\mathrm{PGL}_2(q) = T{:}\langle a\rangle$ and $\mathrm{P\Sigma L}_2(q) = T{:}\langle b\rangle$. By [14, Lemma 4.7] we have $b(L) = 3$ and $b(\mathrm{PGL}_2(q)) = b(\mathrm{P\Sigma L}_2(q)) = 2$. Set $(k,P) = (2,S_2)$ and consider

$$G = \langle T^2, (a,a), (b,b), P\rangle$$

as a primitive product type group on $\Omega = \Gamma^2$, where $\Gamma = [L : J]$.

As before, we may identify Γ with the set of distinct pairs of 1-dimensional subspaces of the natural module for T. Given this identification, a precise description of the 2-element bases for $\mathrm{PGL}_2(q)$ and $\mathrm{P\Sigma L}_2(q)$ is presented in Section 4.3.4 and this allows us to choose bases $\{\alpha_0,\gamma_1\}$ and $\{\alpha_0,\gamma_2\}$ for $\mathrm{PGL}_2(q)$ and $\mathrm{P\Sigma L}_2(q)$, respectively, where γ_1 and γ_2 are contained in distinct L_{α_0}-orbits. In addition, notice that $\{\alpha_0,\gamma_2\}$ is a base for $T{:}\langle ab\rangle$ by Corollary 4.3.13. Set $\alpha = (\alpha_0,\alpha_0)$ and $\beta = (\gamma_1,\gamma_2)$. We claim that $\{\alpha,\beta\}$ is a base for G and thus $b(G) = 2$. To see this, suppose $x = (z_1,z_2)\sigma \in G$ fixes α and β. Then each z_i is contained in L_{α_0} and thus $\sigma = 1$ since γ_1 and γ_2 are in distinct L_{α_0}-orbits. Since $x \in G$, we may write $z_i = t_ic$ with $t_i \in T$ and $c \in \{1,a,b,ab\}$. If $c = 1$ then $z_i \in T_{\alpha_0} \cap T_{\gamma_i} = 1$ and thus $x = 1$. If $c = a$ then $z_1 \in \mathrm{PGL}_2(q)_{\alpha_0} \cap \mathrm{PGL}_2(q)_{\gamma_1} = 1$, which is a contradiction since $z_1 \in L \setminus T$. An entirely similar argument applies if $c \in \{b,ab\}$ and the proof of the claim is complete.

Notice that $|L:T| = 4$ in Example 6.6.12. By the following result, there are no examples with $b(L) = 3$, $|L:T| = 2$ and $b(G) = 2$. Here there is no need to assume that G has soluble point stabilisers and it is worth noting that the same proof goes through under the weaker hypothesis $T^k < L^k \cap G$.

Proposition 6.6.13. *Assume Hypothesis 6.6.1, with $b(L) \geqslant 3$ and $|L:T| = 2$. Then $b(G) \geqslant 3$.*

Proof. We may as well assume $b(T) = 2$. Fix $\alpha_0 \in \Gamma$ and set $\alpha = (\alpha_0,\dots,\alpha_0) \in \Omega$. It suffices to show that $\{\alpha,\beta\}$ is not a base for G, where $\beta = (\gamma_1,\dots,\gamma_k)$ and each γ_i is contained in a regular T_{α_0}-orbit. Since $b(L) \geqslant 3$, for each i there exists $x_i \in L \setminus T$ fixing both α_0 and γ_i.

T	Type of J	$r(T)$	Conditions
$\mathrm{L}_2(q)$	$\mathrm{GL}_1(q) \wr S_2$	$(q+a)/4$	q odd, $\mathrm{PGL}_2(q) < L$
	$\mathrm{GL}_1(q^2)$	$(q-b)/4$	q odd, $\mathrm{PGL}_2(q) \leqslant L$
$\mathrm{L}_3(4)$	$\mathrm{GU}_3(2)$	3	
$\mathrm{L}_4(3)$	$\mathrm{O}_4^+(3)$	6	$L = T.2^2$
$\mathrm{U}_4(3)$	$\mathrm{GU}_1(3) \wr S_4$	11	$L = T.D_8$
$\Omega_8^+(2)$	$\mathrm{O}_2^-(2) \times \mathrm{GU}_3(2)$	5	$L = T.S_3$
$\mathrm{P}\Omega_8^+(3)$	$\mathrm{O}_4^+(3) \wr S_2$	12	$\lvert L:T\rvert \geqslant 6$

Table 6.3: The groups (L,J) in Proposition 6.6.14(ii)

Fix $z = (z_1,\ldots,z_k) \in (L^k \cap G) \setminus T^k$ and define a subset A of $[k]$ such that $i \in A$ if and only if $z_i \notin T$. Note that A is non-empty since $z \notin T^k$. Set $y = (y_1,\ldots,y_k) \in L^k$, where $y_i = x_i$ if $x \in A$, otherwise $y_i = 1$, and observe that y is non-trivial and it fixes α and β. Finally, since $|L:T| = 2$ we deduce that $yz \in T^k \leqslant G$, so $y \in G_\alpha \cap G_\beta$ and the result follows. ■

By the proposition, if G has soluble point stabilisers and $b(L) = 3$, then $b(G) = 2$ only if $b(T) = 2$, $r(T) \geqslant D(P)$ and $|L:T| \geqslant 3$. Since L is almost simple, the possibilities for (L,J) can be read off from [14, Tables 4–7], noting that $b(T) = 2$ only if $\log_m |T| < 2$, where $m = |\Gamma|$. In [14, Table 4], we deduce that the only possibility is $L = A_6.2^2$ with $J = [32]$ or $D_{20}.2$ (here L is isomorphic to $\mathrm{P\Gamma L}_2(9)$ and J is of type $\mathrm{GL}_1(9) \wr S_2$ or $\mathrm{GL}_1(9^2)$, respectively). One can check that no examples arise in [14, Tables 5 and 6], while the relevant possibilities for (L,J) in [14, Table 7] are recorded in Table 6.3 (here we implicitly assume the additional condition $|L:T| \geqslant 3$). For the values of $r(T)$ in the first two rows, we have $(a,b) = (7,1)$ if $q \equiv 1 \pmod 4$, otherwise $(a,b) = (5,3)$ (see Remark 4.5.15(ii) and the proof of [24, Lemma 7.9]).

It is straightforward to check that none of these possibilities correspond to cases in Table 4.9, which implies that $\mathrm{reg}(L) \geqslant 5$ and we obtain the following result via Theorem 6.2.6.

Proposition 6.6.14. *Assume Hypothesis 6.6.1 and H is soluble. Then $b(G) = 2$ only if one of the following holds:*

(i) $b(L) = 2$ and either $b(L \wr P) = 2$, or $b(L \wr P) = 3$, $r(L) < D(P)$ and (L,J) is one of the cases in Table 4.7 or 4.8.

(ii) $b(L) = b(L \wr P) = 3$ and (L,J) is one of the cases in Table 6.3, where $r(T) \geqslant D(P)$ and $|L:T| \geqslant 3$.

The study of bases for product type groups becomes rather more complicated if we drop Hypothesis 6.6.1. As an illustration, we close with the following example.

Example 6.6.15. Let $G \leqslant L \wr P$ be a product type primitive group on $\Omega = \Gamma^3$, where $P = S_3$ and $L \leqslant \mathrm{Sym}(\Gamma)$ is a primitive group with point stabiliser J. As before, we may assume G induces L on each factor of Ω, and P on the set of factors of the socle T^3. Take $L = \mathrm{PGL}_2(11) = T{:}\langle a\rangle = T.2$ and $J = S_4$, so $b(L) = 2$, $r(L) = 1$ and $r(T) = 3$ (see Table 4.7, noting that J is of type $2_-^{1+2}.\mathrm{O}_2^-(2)$).

First assume G contains P and note that there are precisely three possibilities, namely $L \wr P$, $\langle T^3, (a,a,a), P\rangle$ and $\langle T^3, (a,a,1), P\rangle$. For the full wreath product $G = L \wr P$, Theorem 6.1 implies that $b(G) = 3$ since $r(L) < D(P)$. Similarly, if $G = \langle T^3, (a,a,a), P\rangle$ then $\tau(G) = 0$ (see (6.6.1)) and thus $b(G) = 3$ by Theorem 6.6.11, while a MAGMA calculation gives $b(G) = 3$ if $G = \langle T^3, (a,a,1), P\rangle$.

Now assume G does not contain P, so $|P \cap G| \in \{1,2,3\}$. With the aid of MAGMA, we find that there are 8 product type primitive groups of this form, up to permutation isomorphism. More precisely, there are 3 groups with $P \cap G = 1$ and in each case $b(G) = 2$. There are also 3 groups with $|P \cap G| = 2$ and here we find that $b(G) = 3$. Finally, let G_1 and G_2 be the two remaining groups with $|P \cap G_i| = 3$. For one of them, say G_1, we have $\langle G_1, P\rangle = L \wr P$ and $b(G_1) = 3$. On the other hand, $\langle G_2, P\rangle$ has index 4 in $L \wr P$ and one can check that $b(G_2) = 2$.

Appendix A

Appendix: Magma and GAP code

In this appendix, we present code for implementing our computational methods. Here we mainly use Magma V2.26-11 [10], and we will use the GAP Character Table Library [12] as an important tool to do some computations on sporadic groups.

All the calculation times, if not specified otherwise, are based on my own computer (with 8 GB RAM). The author thanks Saul Freedman for the code in A.1.1, A.1.2.1, A.1.2.2, A.1.2.5.

A.1 Magma code

A.1.1 Calculation of base sizes

Our first Magma function `BaseSizeTest` determines whether or not the base size of a transitive permutation group G is at most a given integer k. Here the "iter" variable corresponds to the iteration depth. As discussed in Section 4.2.2, we first get a set of G-orbit representatives of $(k-1)$-tuples and then inspect the pointwise stabiliser of every representative to check if there is a regular orbit. The function takes as input a permutation group G and an integer k, which returns `true` if and only if $b(G) \geqslant k$ (equivalently, G has a base of size k).

```
function BaseSizeTest(G,k:iter:=1);
    if iter eq 1 then
        if IsRegular(G) then
            return true;
        end if;
        orbs:=[1];
    else
        orbs:=[i[2]:i in OrbitRepresentatives(G)|i[1] ne 1];
    end if;
    for i in orbs do
        S:=Stabiliser(G,i);
        if iter le k-1 and #S le Max({j[1]:j in OrbitRepresentatives(S)}) then
            return true;
        end if;
        if iter lt k-1 then
            if BaseSizeTest(S,k:iter:=iter+1) then
                return true;
            end if;
        end if;
    end for;
return false;
end function;
```

Now we use BaseSizeTest to compute $b(G)$. Note that $b(G) \geqslant \log_{|\Omega|}|G|$ for any permutation group $G \leqslant \mathrm{Sym}(\Omega)$. Starting from the integer $\lceil \log_{|\Omega|}|G| \rceil$, we use BaseSizeTest to check if G has a base of size a given integer.

The command BaseSizeCalc(G) returns the precise base size of a transitive permutation group G in MAGMA.

```
function BaseSizeCalc(G);
    bslower:=Ceiling(Log(Degree(G),#G))-1;
    // Ceiling(Log(Degree(G),#G)) is the lower bound for the base size
    repeat
        bslower:=bslower+1;
    until BaseSizeTest(G,bslower) eq true;
    return bslower;
end function;
```

For example, if $G = S_7 \wr S_3$ is a product type primitive group of degree 7^3, then the function BaseSizeCalc computes $b(G) = 7$ in around 22 seconds.

A.1.2 Calculations on generalised Saxl graphs

In this section, we present the MAGMA functions we use to study the generalised Saxl graph $\Sigma(G)$ of a transitive group $G \leqslant \mathrm{Sym}(\Omega)$ with $b(G) \geqslant 2$.

A.1.2.1 The common neighbour property

We first present the MAGMA code to check whether or not G satisfies the property

($\star$) *Any two vertices in $\Sigma(G)$ have a common neighbour.*

As explained in Section 4.2.5, we first obtain the pairs of points in Ω lying in bases of size $b(G)$ (recall the function `BaseSizeCalc` above to compute $b(G)$). The pairs are stored in MAGMA as a set of representatives of orbitals by the function `PairsInMinSizeBase` below. To do this, we first need the following procedure, which computes a set of G-orbit representatives of bases for G of size $b(G)$, stored as the sequence `E`. As before, this can be done iteratively. Here the sequence `tup` is a (possibly empty) sequence of points in Ω, the group `S` is the pointwise stabiliser of `tup` in G, and the integer `b` is the base size $b(G)$.

```
procedure OrbitIter(S,b,tup,~E)
    orbs:=[i[2]:i in OrbitRepresentatives(S)|i[1] ne 1];
    for r in orbs do
        Snew:=Stabiliser(S,r);
        tupnew:=Append(tup,r);
        if #tupnew eq b-1 then
            E:=E cat [Seqset(Append(tupnew,j[2])):j in
            OrbitRepresentatives(Snew)|j[1] eq #Snew];
        elif #tupnew lt b-1 then
            OrbitIter(Snew,b,tupnew,~E);
        else
            break r;
        end if;
    end for;
end procedure;
```

We now use `OrbitIter` to obtain a set of representatives for pairs of points lying in bases of size $b(G)$, up to equivalence under the action of G. Here the input is G and the integer $b(G)$ (the latter can be computed from the function `BaseSizeCalc` above).

```
function PairsInMinSizeBase(G,b)
    tup:=[];
    if IsRegular(G) then
        E:=[[1]];
    else
        E:=[];
        OrbitIter(G,b,tup,~E);
    end if;
    E:=Seqset(E);
    minbasereps:=[];
    while not IsEmpty(E) do
        r:=Rep(E);
        Append(~minbasereps,r);
        E:=E diff {i:i in E|IsConjugate(G,i,r)};
    end while;
    minpairs:={i:i in Subsets(j,2),j in minbasereps};
    minpairreps:=[];
    while not IsEmpty(minpairs) do
        r:=Rep(minpairs);
        Append(~minpairreps,r);
        minpairs:=minpairs diff {i:i in minpairs|IsConjugate(G,i,r)};
    end while;
return minpairreps;
end function;
```

For independent interest, one can easily construct the generalised Saxl graph $\Sigma(G)$ via the function `PairsInMinSizeBase`. We omit the details since we do not need to construct $\Sigma(G)$ in this thesis.

Now we record the MAGMA function to check whether or not G satisfies property $(\star)$. This requires a set of representatives for pairs of points lying in bases of size $b(G)$, as can be obtained via the function `PairsInMinSizeBase`. Here the input is G, and the function returns `true` if and only if $(\star)$ holds.

```
function FastMinSizeComNeighbTest(G)
    b:=BaseSizeCalc(G);
    minpairreps:=PairsInMinSizeBase(G,b);
    comb:={};
    for m in minpairreps do
        comb:=comb join m^G;
    end for;
    G1:=Stabiliser(G,1);
    orbreps:=[i[2]:i in OrbitRepresentatives(G1)|i[2] ne 1];
    for o in orbreps do
        found:=false;
        if exists{s:s in comb|1 in s and {o,Rep(s diff {1})} in comb} then
            found:=true;
        end if;
        if not found then
            return false;
        end if;
    end for;
return true;
end function;
```

For example, if the input $G = S_7 \wr S_3$ is a product type primitive group of degree 7^3, then `FastMinSizeComNeighbTest` returns `true` in 91 seconds.

A.1.2.2 Check if G is semi-Frobenius

Now we present a function to determine whether or not G is semi-Frobenius. Recall that G is called semi-Frobenius if $\Sigma(G)$ is complete, or equivalently, if any 2-subset of Ω can be extended to a base of size $b(G)$.

To do this, we first introduce the following procedure. Again, the sequence `tup` is a (possibly empty) sequence of points in Ω, the group `S` is the pointwise stabiliser of `tup` in G, which is the input of the function `FastMinSizeIsComplete` below, and the integer `b` is the base size $b(G)$. Moreover, the sequence `orbreps` is initially a set of representatives for the orbits of G_1 other than $\{1\}$, and `done` is initially set to be `false`.

We iteratively check orbits of non-trivial point stabilisers up to equivalence, using the variables `tup` and `tupnew` to keep track of this, until `tupnew` has size $b(G)-1$. During this process, an element α in `orbreps` is deleted if we find $\alpha_3,\dots,\alpha_{b(G)-1}$ such that $G_{(1,\alpha,\alpha_3,\dots,\alpha_{b(G)-1})}$ has a regular orbit (this means that $\{1,\alpha\}$ is an edge in $\Sigma(G)$). If `orbreps` ever becomes empty, then G is semi-Frobenius and `done` is set to be `true`.

```
procedure OrbitIter2(S,b,tup,~orbreps,~done:init:=0)
    if Type(init) eq GrpPerm then
        orbs:=[1];
    else
        orbs:=Reverse([i[2]:i in OrbitRepresentatives(S)|i[1] ne 1]);
    end if;
    for r in orbs do
        if Type(init) eq GrpPerm then
            Snew:=init;
        else
            Snew:=Stabiliser(S,r);
        end if;
        tupnew:=Append(tup,r);
        if #tupnew eq b-1 then
            orbdiff:={j[2]:j in OrbitRepresentatives(Snew)|j[1] eq #Snew};
            if not IsEmpty(orbdiff) then
                orbreps:=(orbreps diff Seqset(tupnew)) diff orbdiff;
            end if;
            if IsEmpty(orbreps) then
                done:=true;
                break r;
            end if;
        elif #tupnew lt b-1 then
            OrbitIter2(Snew,b,tupnew,~orbreps,~done);
            if done then
                break r;
            end if;
        else
            break r;
        end if;
    end for;
end procedure;
```

Using the procedure OrbitIter2, the function FastMinSizeIsComplete has input a transitive permutation group G with $b(G) \geqslant 2$, which returns true if and only if G is semi-Frobenius.

```
function FastMinSizeIsComplete(G)
    b:=BaseSizeCalc(G);
    G1:=Stabiliser(G,1);
    orbreps:={i[2]:i in OrbitRepresentatives(G1)|i[2] ne 1};
    tup:=[];
    done:=false;
    OrbitIter2(G,b,tup,~orbreps,~done);
return done;
end function;
```

For example, if the input is the primitive group $G = S_7 \wr S_3$ as before, then the function FastMinSizeIsComplete returns false in 90 seconds.

A.1.2.3 Probability

Recall that for a primitive group G with point stabiliser H, the common neighbour property $(\star)$ holds if $Q(G,b(G)) < 1/2$ (see Lemma 3.2.6(i)), and recall that $Q(G,c) \leqslant \widehat{Q}(G,c)$, where

$$\widehat{Q}(G,c) = \sum_{i=1}^{k} \frac{|x_i^G \cap H|^c}{|x_i^G|^{c-1}}$$

and $\bigcup_i x_i^G$ is the set of elements of prime order in G.

Here we present a MAGMA function for computing $\widehat{Q}(G,c)$, as explained in Section 4.2.3. The command `Q(G,H,c)` returns the precise value of $\widehat{Q}(G,c)$ for the transitive permutation group G with point stabiliser H. Note that obtaining the conjugacy classes of G is expensive since $|G|$ is large. Instead, we compute the conjugacy classes of H and then use the function `IsConjugate` to determine the fusion of these classes in G.

```
Q:=function(G,H,c);
    C:=ConjugacyClasses(H);
    q:=PrimeDivisors(#H);
    z:=0;
    for r in q do
        a:={@ i : i in [1..#C] | C[i][1] eq r @};
        A:={#G div #Centralizer(G,C[i][3]) : i in a};
        A:=[x : x in A];
        for i in [1..#A] do
            m:=A[i];
            B:=[j : j in a | (#G div #Centralizer(G,C[j][3])) eq m];
            E:=B;
            while #E ge 1 do
                j:=E[1];
                x:=C[j][3];
                d:=0;
                F:=[];
                for k in E do
                    y:=C[k][3];
                    if IsConjugate(G,x,y) eq true then
                        d:=d+C[k][2];
                        Append(~F,k);
                    end if;
                end for;
                z:=z+d^c/m^(c-1);
                E:=[x : x in E | x in F eq false];
            end while;
        end for;
    end for;
return z, RealField(4)!z;
end function;
```

For example, in the proof of Lemma 4.5.6 we need to show that $\widehat{Q}(G,2) < 1/2$ when $G = \mathrm{Aut}(^2G_2(27))$ and $H = N_G(K)$, where K is a Sylow 37-subgroup of G. The command `Q(G,H,2)` computes $\widehat{Q}(G,2) = 85/27702$ in 6 seconds.

In the proofs of Lemma 4.5.6 and Proposition 4.5.12, we need to compute $\widetilde{Q}(G,2)$ (see (4.2.1)), noting that $\widehat{Q}(G,2) < \widetilde{Q}(G,2)$. The following function `Q2c` returns the precise value of $\widetilde{Q}(G,2)$, with input the permutation group G. Compare to the function `Q` above, the only difference is that there are no `IsConjugate` commands needed for the function `Q2c`, which is a significant saving.

```
Q2c:=function(G,H);
C:=ConjugacyClasses(H);
Q:=PrimeDivisors(#H);
z:=0;
for r in Q do
    a:={@ i : i in [1..#C] | C[i][1] eq r @};
    A:={#G div #Centralizer(G,C[i][3]) : i in a};
    A:=[x : x in A];
    for i in [1..#A] do
        c:=A[i];
        B:=[j : j in a | (#G div #Centralizer(G,C[j][3])) eq c];
        E:=B;
        while #E ge 1 do
            j:=E[1];
            x:=C[j][3];
            d:=0;
            F:=[];
            for k in E do
                Cx:=#Centraliser(G,x);
                y:=C[k][3];
                if #Centraliser(G,y) eq Cx then
                    d:=d+C[k][2];
                    Append(~F,k);
                end if;
            end for;
            z:=z+d^2/c;
            E:=[x : x in E | x in F eq false];
        end while;
    end for;
end for;
return z, RealField(4)!z;
end function;
```

For example, if $G = \mathrm{Aut}(\mathrm{P}\Omega_8^+(9))$ and H is of type $\mathrm{O}_2^-(9^2) \times \mathrm{O}_2^-(9^2)$, then we construct H in MAGMA as the normaliser of a Sylow 41-subgroup of G, and the function Q2c computes

$$\widetilde{Q}(G,2) = 1090030513829/3335430063721392000 \approx 3 \times 10^{-7}$$

in 5 hours. This case arises in the proof of Proposition 4.5.12.

A.1.2.4 Double cosets

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive group with point stabiliser H. As explained in Section 4.2.4, we can work with (H,H) double cosets in order to bound or to compute $r(G)$ (see (4.2.2)). If $|\Omega| = |G:H| < 10^7$ we can directly compute $r(G)$ using the function DoubleCosetRepresentatives in MAGMA. However, in some cases, $|G:H| > 10^7$ and so this method does not work well in MAGMA. Instead, we can sometimes use the function DoubleCosetCanonical to establish the existence of sufficiently many regular H-orbits to force $Q(G,2) < 1/4$, with the aim of proving Theorem 4.5.1. This approach is implemented in the proofs of Propositions 4.5.11 and 4.5.12. More specifically, the method is used to treat the cases where $\mathrm{soc}(G) = \mathrm{PSp}_8(3)$ with H of type $\mathrm{Sp}_2(3) \wr S_4$, and $G = \mathrm{P}\Omega_8^+(3).A_4$ with H of type $\mathrm{O}_2^-(3) \wr S_4$.

Example A.1.1. Suppose $G = \mathrm{Aut}(\mathrm{PSp}_8(3))$ and H is of type $\mathrm{Sp}_2(3) \wr S_4$. Here

$$|G:H| = 16523386425 > 10^{10}$$

and we use the function DoubleCosetCanonical to show that $Q(G,2) \leqslant 1/4$ proceeding as follows, noting that G has a unique conjugacy class of soluble maximal subgroups.

```
G:=AutomorphismGroupSimpleGroup("S",8,3);
M:=MaximalSubgroups(G:IsSolvable:=true);
H:=M[1]‘subgroup;
m:=Ceiling(0.75*Index(G,H)/#H); // m = 1557
repeat
    g := Random (G);
    a := DoubleCoset(G, H, g, H);
    until #a eq #H^2;
```

```
Im, base := DoubleCosetCanonical (G, H, g, H);
    L := [];
    DC := [];
for i in [1..1000000] do
    if i mod 100 eq 0 then "test i = ", i; end if;
    g := Random (G);
    a := DoubleCoset(G, H, g, H);
    if #a eq #H^2 then
        Append (~L, g);
        im := DoubleCosetCanonical (G, H, g, H: B := base);
        Append (~DC, im);
        r := #Set (DC);
        i, #L, r;
        if r ge m then break; end if;
    end if;
end for;
```

The “for” loop takes 108.23 seconds. The final line of the output is

```
8218 6278 1557
```

which means that 8218 random elements g of G are chosen, 6278 of which are such that $|HgH| = |H|^2$, and they give 1557 distinct (H,H) double cosets with size $|H|^2$. Therefore, there are at least 1557 regular H-orbits, whence $Q(G,2) \leqslant 1/4$.

A.1.2.5 Sporadic groups

Now we present the code involved in the calculations for sporadic groups in Section 4.4.

First, we detail how we construct the primitive permutation groups $G \leqslant \mathrm{Sym}(\Omega)$ with $G \in \{\mathrm{Ly}, \mathrm{Th}\}$ and $b(G) \geqslant 3$, which arises in the proof of Proposition 4.4.1. In view of [30, Theorem 1], the latter condition implies that $b(G) = 3$ and

$$(G,H) = (\mathrm{Ly}, G_2(5)),\ (\mathrm{Ly}, 3.\mathrm{McL}{:}2),\ (\mathrm{Th}, {}^3D_4(2){:}3) \text{ or } (\mathrm{Th}, 2^5.\mathrm{L}_5(2)),$$

where H is a point stabiliser in G. Here we construct a matrix group $\widehat{G} < \mathrm{GL}_d(q)$ isomorphic to G with

$$(d,q) = \begin{cases} (248,2) & G = \mathrm{Th} \\ (111,5) & (G,H) = (\mathrm{Ly}, G_2(5)) \\ (517,5) & (G,H) = (\mathrm{Ly}, 3.\mathrm{McL}{:}2). \end{cases}$$

This can be done in MAGMA using the function `MatrixGroup`. For example, `MatrixGroup("Th",1)` returns a group $\widehat{G} < \mathrm{GL}_{248}(2)$. We then construct a subgroup $\widehat{H}$ of $\widehat{G}$ isomorphic to H using the generators from the Web ATLAS [123], and obtain a low-dimensional $\widehat{H}$-submodule of $\mathbb{F}_q^d$. This allows us construct the permutation group $G \leqslant \mathrm{Sym}(\Omega)$ using the function `OrbitImage`.

As an example, we present the code we use for the case $(G,H) = (\mathrm{Th}, 2^5.\mathrm{L}_5(2))$ below, recalling that our aim is to show that G is semi-Frobenius. Here the function `OrbitImage`, which returns the permutation group $G \leqslant \mathrm{Sym}(\Omega)$, requires a significant amount of RAM (around 171 GB). The author thanks Saul Freedman for his assistance with this computation (which took 122 hours, as he noted).

```
G:=MatrixGroup("Th",1);
SS:=function(S)
    w1 := S.1;
    w2 := S.2;
    w3 := w1 * w2;
    w4 := w3 * w2;
    w5 := w4 * w3;
    w6 := w5 * w5;
    w5 := w3^15;
    w7 := w4^9;
    w8 := w5 * w7;
    w5 := w3^12;
    w7 := w8 * w5;
    w5 := w4^16;
    w8 := w7 * w5;
    w5 := w3^17;
    w7 := w8 * w5;
    w8 := w7^-1;
    w3 := w8 * w6;
    w2 := w3 * w7;
    return [w1,w2];
end function;
H:=sub<Generic(G)|SS(G)>;
MH:=GModule(H);
C:=Submodules(MH);
V:=C[2];  // dimension 5
f:=Morphism(V,MH);
U:=VectorSpace(MH);
W:=sub<U|U!f(V.1),U!f(V.2)>; // setting up V as a subspace of U
I:=OrbitImage(G,W);
FastMinSizeIsComplete(I); // true
```

Next, we treat the special case $(G,H) = (\mathrm{Fi}_{23}, 3^{1+8}.2^{1+6}.3^{1+2}.2S_4)$ arising in the proof of Proposition 4.4.1, and we show that G is semi-Frobenius with its action on $[G:H]$. Here $b(G) = 3$ and $|G:H| = 1252451200 > 10^9$, so the degree is too large for MAGMA to construct G using `CosetAction`. Instead, we use the function `DoubleCosetCanonical` to verify that for each (H,H) double coset representative $x \notin H$, there exists an element $y \in G$ such that $H \cap H^x \cap H^y = 1$. The code is shown as below.

```
G:=Socle(AutomorphismGroupSimpleGroup("Fi23"));
M:=MaximalSubgroups(G:OrderEqual:=3265173504);
H:=M[1]‘subgroup;
Gsize:=#G;
im,base:=DoubleCosetCanonical(G,H,H.1,H);
breps:=[im];
dcsize:=#H;
for g in G do
    x:=DoubleCosetCanonical(G,H,g,H:B:=base);
    if not x in breps then
        Append(~breps,x);
        dcsize:=dcsize+#DoubleCoset(G,H,g,H);
        C:=H meet H^g;
        found:=false;
        repeat
            y:=Random(G);
            if #(C meet H^y) eq 1 then
                found:=true;
            end if;
        until found;
        if dcsize eq Gsize then
            print "Done.";
            break g;
        end if;
    end if;
end for;
```

In the proof of Theorem 4.4.4, we need to show that the common neighbour property $(\star)$ holds for the permutation group $G \leqslant \mathrm{Sym}(\Omega)$ with $G = \mathrm{Fi}_{24}$ and point stabiliser $H = (2 \times 2.\mathrm{Fi}_{22}){:}2$. Here $b(G) = 3$ by [30, Theorem 1]. Once again, the degree of G is too large for MAGMA to construct G as a permutation group on Ω, and so the function `FastMinSizeComNeighbTest` cannot be applied.

Instead, we will show that there exists $r,s \in G \setminus H$ such that $H \cap H^r \cap H^s = 1$ and $2|HrH| > |G|$, noting that this implies that $\mathrm{val}(G)/|\Omega| > 1/2$ and thus $(\star)$ holds.

To do this, we first construct H using the generators given in the Web ATLAS [123] (Version 2.0). Then we can find the elements r,s described above via random search as shown in the following code.

```
G:=AutomorphismGroupSimpleGroup("Fi24");
w1:=G.1;
w2:=G.2;
w3:=w1*w2;
w4:=w3*w2;
w5:=w4*w3;
w6:=w2^3;
w7:=w4*w6;
w8:=w3*w6;
w9:=w7*w7;
w10:=w9*w8;
w11:=w10^-1;
w12:=w11*w5;
w2:=w12*w10;
H:=sub<G|w1,w2>;
repeat
    r:=Random(G);
until 2*#DoubleCoset(G,H,r,H) gt #G and exists(s){s : s in G |
    #((H meet Conjugate(H,r)) meet Conjugate(H,s)) eq 1};
#DoubleCoset(G,H,r,H); // 142943065044047364096000
```

A.1.3 Random search for subsets with $\mathrm{Hol}(T,S) = 1$

Let $G = T^k.(\mathrm{Out}(T) \times S_k)$ be a diagonal type primitive group (see Section 5.2.1). Recall Lemma 5.3.2 that G has at least 2 regular suborbits if and only if the holomorph $\mathrm{Hol}(T)$ has at least 2 regular orbits on the set of k-subsets of T. We implement this approach in MAGMA by random search, finding two random k-subsets of T lying in distinct regular $\mathrm{Hol}(T)$-orbits. The function RanHol below is used in the proofs of Proposition 5.4.7 and Lemma 5.5.12. Here the input is a simple group T and an integer k, and the function returns two k-subsets of T (stored as $\{1,\dots,|T|\}$ in MAGMA) lying in distinct regular $\mathrm{Hol}(T)$-orbits.

```
RanHol:=function(T,k);
G:=Holomorph(T);
d:=#T;
```

```
repeat
    A:=[];
    B:=[];
    repeat // we keep adding elements to A until it is a k-set
        Append(~A,Random([1..d]));
    until #{x : x in A} eq k;
    repeat
        Append(~B,Random([1..d]));
    until #{x : x in B} eq k;
    A:={x : x in A};
    B:={x : x in B};
    S1:=Stabiliser(G,A);
    S2:=Stabiliser(G,B);
until #S1 eq 1 and #S2 eq 1 and not exists(g){g : g in G | B eq
    {Image(g,x) : x in A}};
return A,B;
end function;
```

We only use the function RanHol when $|T| \leqslant 1092$. For example, for the group $T = \mathrm{L}_2(13)$ with $|T| = 1092$, the command RanHol(T,25) returns the following two random subsets in 40 seconds

```
{ 21, 32, 36, 111, 186, 187, 274, 312, 343, 364, 470, 489, 497, 501, 525, 679,
684, 686, 699, 723, 945, 982, 1007, 1038, 1091 }
{ 5, 13, 38, 101, 116, 125, 140, 156, 324, 341, 350, 395, 459, 473, 482, 547,
644, 788, 831, 857, 936, 944, 981, 986, 1077 }
```

To determine whether or not the two random subsets A and B obtained in the function RanHol are indeed in distinct $\mathrm{Hol}(T)$-orbits, we inspect every element $g \in \mathrm{Hol}(T)$ and check whether or not $A^g = B$. This process, as well as the calculation of setwise stabilisers, becomes very expensive when $|T|$ (and hence $|\mathrm{Hol}(T)|$) is large. Thus, for the groups with $|T| > 1092$, we implement the approach described in Remark 5.3.7.

More precisely, we find two k-subsets of T with suitable element orders by random search, using the function RanHolOrder below. Once again, the input is a simple group T and an integer k. With the notation in Remark 5.3.7(i), the function RanHolOrder finds two k-subsets X_1 and X_2 containing 1 and satisfying the properties that $\langle X_j \rangle = T$, $|O_j| = k$, $O_j \neq \{|x^{-1}t| : t \in X_j\}$ for any $x \in X_j \setminus \{1\}$, and $O_2 \neq \{|x^{-1}t| : t \in X_1\}$, where

$$O_j = \{|t| : t \in X_j\}$$

is the set of element orders in X_j. The function returns $O_1 \setminus \{1\}$ and $O_2 \setminus \{1\}$. As noted in Remark 5.3.7(i), the two k-subsets X_1 and X_2 are in distinct regular $\mathrm{Hol}(T)$-orbits, and we only need to use this method for $k \leqslant 11$.

```
RanHolOrder:=function(T,k);
repeat
    A:=[];
    B:=[];
    for i in [1..k-1] do
        Append(~A,Random(T));
        Append(~B,Random(T));
    end for;
    A:={x : x in A};
    B:={x : x in B};
    O1:={Order(x) : x in A};
    O2:={Order(x) : x in B};
until ((#O1 eq k-1 and #sub<T|A> eq #T and not exists(y){y : y in A |
    {Order(y^(-1)*x) : x in A} eq O1 or {Order(y^(-1)*x) : x in A} eq
    O2}) and (#O2 eq k-1 and #sub<T|B> eq #T and not exists(y){y : y in B |
    {Order(y^(-1)*x) : x in B} eq O2}));
return O1,O2;
end function;
```

For example, if $T = \mathrm{Fi}_{24}'$ and $k = 8$, the command `RanHolOrder(T,k)` returns the following in 40 seconds

```
{ 8, 17, 21, 26, 27, 29, 39 }
{ 14, 21, 24, 26, 33, 35, 36 }
```

This means that there exist subsets X_1 and X_2 of T lying in distinct regular $\mathrm{Hol}(T)$-orbits such that $1 \in X_1 \cap X_2$, $|X_1| = |X_2| = 8$,

$$\{|t| : t \in X_1\} = \{1,8,17,21,26,27,29,39\} \text{ and } \{|t| : t \in X_2\} = \{1,14,21,24,26,33,35,36\}.$$

A.1.4 Proof of Proposition 5.6.10

In this section, we present the MAGMA code involved in the proof of Proposition 5.6.10. Here we assume

$$T \in \mathscr{A} := \{\mathrm{M}_{12}, \mathrm{HS}, \mathrm{Suz}, \mathrm{He}, \mathrm{J}_1, \mathrm{J}_2, \mathrm{J}_3, \mathrm{Fi}_{22}, \mathrm{O'N},\ \mathrm{HN}\}.$$

We will handle the sporadic groups with $T \notin \mathscr{A} \cup \{\mathbb{B}, \mathbb{M}\}$ using GAP (see Appendix A.2.2).

First assume $T \in \mathscr{A}$ and $T \neq \mathrm{HN}$. Here we first inspect the conjugacy classes of $\mathrm{Aut}(T)$ and obtain an element y of order m, where m is as described in Table 5.4. Then we compute the group $I(y)$, where

$$I(y) = \{\alpha \in \mathrm{Aut}(T) : y^{\alpha} \in \{y, y^{-1}\}\}$$

is the group of automorphisms of T centralising or inverting y. Note that if y is not $\mathrm{Aut}(T)$-conjugate to y^{-1}, then $I(y) = C_{\mathrm{Aut}(T)}(y)$, otherwise $I(y) = \langle C_{\mathrm{Aut}(T)}(y), g\rangle$, where $g \in \mathrm{Aut}(T)$ is such that $y^g = y^{-1}$.

Recall that our aim is to show that for any $z \in T \setminus y^T$, there exists $x \in z^T$ such that $\langle x, y\rangle = T$ and there is no $\alpha \in \mathrm{Aut}(T)$ with $(x,y)^\alpha = (x^{-1}, y^{-1})$, noting that the latter condition holds if $I(x) \cap I(y) = 1$ and one of x and y has order at least 3. For each T-class representative $z \in T \setminus y^T$ of prime order, one can obtain a random element $x \in z^T$ satisfying $\langle x, y\rangle = T$ and $I(x) \cap I(y) = 1$. This can be done with the aid of MAGMA via the following code. Here we present the calculation for the group $T = \mathrm{Fi}_{22}$, noting that other groups in $\mathscr{A} \setminus \{\mathrm{HN}\}$ can be handled similarly.

```
G:=AutomorphismGroupSimpleGroup("Fi22");
T:=Socle(G);
t:=#T;
C:=Classes(T);
y:=C[61][3]; // an element in Table 5.4
P:=[i : i in [2..#C] | IsPrime(C[i][1]) and not i eq 61];
// a set of represetatives of prime order elements in T not conjugating to y
P; // output: [ 2, 3, 4, 5, 6, 7, 8, 14, 26, 36, 37, 49, 50 ]
Cy:=Centraliser(G,y);
Y,g:=IsConjugate(G,y,y^(-1));
// y^g = y^(-1), or g = Id(G) if y^g and y^(-1) are not G-conjugate
Iy:=sub<G|Cy,g>; // the group I(y)
for i in P do
    z:=C[i][3];
    Cz:=Centraliser(G,z);
    Z,gz:=IsConjugate(G,z,z^(-1));
    Iz:=sub<G|Cz,gz>; // the group I(z)
    repeat
        h:=Random(G);
        x:=z^h; // a random element in z^T
        Ix:=(Iz)^h; // the group I(x)
    until #sub<T|x,y> eq t and #(Ix meet Iy) eq 1;
    [Order(z),Order(h),i];
end for;
```

The output is a sequence consisting of $|z|$, $|h|$ with $x := z^h$ satisfying the prescribed properties, and the class number of z in `Classes(T)`.

We treat the group $T = \mathrm{HN}$ separately in the proof of Proposition 5.6.10. This is because computing the conjugacy classes in this setting is expensive for MAGMA. We now present a method of constructing conjugacy classes of prime order elements without using the function Classes. As before, we construct $\mathrm{Aut}(T)$ using AutomorphismGroupSimpleGroup, and T is constructed as the socle of $\mathrm{Aut}(T)$.

First, let us construct an element y of order 19, which is an element of order as described in Table 5.4. We work with a maximal subgroup $H = \mathrm{U}_3(8).6$ of $\mathrm{Aut}(T)$, which can be constructed using the generators given in the Web ATLAS [123]. Note that a Sylow 19-subgroup S of H is of order 19, and y can be obtained as a generator of S.

It is worth noting that $S = C_{\mathrm{Aut}(T)}(y)$. Thus, for an element $g \in \mathrm{Aut}(T)$ such that $y^g = y^{-1}$, which can be obtained as discussed in the above example, the set of elements in $\mathrm{Aut}(T)$ inverting y is the coset gS. Thus, for an element $x \in T$, if there is no element in gS inverting x, then there is no element $\alpha \in \mathrm{Aut}(T)$ such that $(x, y)^\alpha = (x^{-1}, y^{-1})$. Given this observation, we do not need to compute $C_{\mathrm{Aut}(T)}(x)$, which is a significant saving.

Next, we construct representatives z of elements in T of prime order $r < 19$ (note that 19 is the largest prime divisor of $|T|$), so $r \leqslant 11$. Assume z is not of class 5B, 5C or 5D. Then $z^T \cap K$ is non-empty, where $K \cong A_{12}$ is a maximal subgroup of T. Here K can be constructed as a point stabiliser of T. Once again, since the degree of K is large, it is expensive for MAGMA to obtain the set of conjugacy classes in K directly. To overcome this difficulty, we work with the group A_{12} with its natural permutation representation on 12 points, in which the conjugacy classes of prime order can be obtained easily. We are then able to obtain a set of K-class representatives of prime order elements via an isomorphism of K and A_{12}.

Finally, assume z is of class 5B, 5C or 5D. Here $z^T \cap K$ is empty, so instead we work with a maximal subgroup $L = 2^{1+8}.(A_5 \times A_5).2.2$ of $\mathrm{Aut}(T)$, noting that $z^T \cap L$ is non-empty. We then work with a Sylow 5-subgroup of L, which is isomorphic to C_5^2.

The method explained above can be implemented in MAGMA via the following code.

```
G:=AutomorphismGroupSimpleGroup("HN");
T:=Socle(G);
t:=#T;

// construction of a maximal subgroup U(3,8).6 of Aut(T)
w1:=G.1;
w2:=G.2;
w3 := w1 * w2;
w4 := w3 * w2;
w5 := w3^14;
w6 := w4 * w4;
w4 := w3 * w3;
w3 := w2 * w2;
w2 := w6 * w3;
```

```
w3 := w2 * w4;
w2 := w3^-1;
w4 := w2 * w5;
w2 := w4 * w3;
H:=sub<G|w1,w2>; // H is isomorphic to U(3,8).6

S:=SylowSubgroup(H,19);
y:=S.1;
// an element in Table 5.4, noting that its centraliser in G is equal to S
Y,g:=IsConjugate(H,y,y^(-1));
Inv:={g*a : a in S}; // the set of elements in G inverting y

z:=y^(-1); // check the proposition for z = y^(-1)
repeat
    h:=Random(G);
    x:=z^h; // a random element in z^T
until #sub<T|x,y> eq t and not exists(a){a : a in Inv | x^a eq x^(-1)};

K:=Stabiliser(T,1); // a maximal subgroup of T isomorphic to Alt(12)
tr,f:=IsIsomorphic(Alt(12),K); // f is an isomorphism from Alt(12) to K
C:=Classes(Alt(12));
P:=[i : i in [2..#C] | IsPrime(C[i][1])];
Ele:=[f(C[i][3]) : i in P];
// the sequence of prime order elements which cover prime order classes
// other than 5B, 5C, 5D, 19A, 19B
for z in Ele do
// check the proposition for |z| < 19 and z is not of class 5B, 5C or 5D
    repeat
        h:=Random(G);
        x:=z^h; // a random element in z^T
    until #sub<T|x,y> eq t and not exists(a){a : a in Inv | x^a eq x^(-1)};
end for;

// construction of a maximal subgroup 2^(1+8).(A5xA5).2.2 of G
w1:=G.1;
w2:=G.2;
w3 := w1 * w2;
w4 := w3 * w2;
```

```
w5 := w4 * w2;
w6 := w2 * w2;
w7 := w5 * w3;
w8 := w7^5;
w9 := w6 * w4;
w10 := w9^-1;
w11 := w10 * w8;
w12 := w11 * w9;
w10 := w8 * w12;
w11 := w10^5;
w1 := w9 * w11;
w9 := w4 * w3;
w10 := w9 * w4;
w9 := w10^-1;
w11 := w9 * w8;
w9 := w11 * w10;
w10 := w8 * w9;
w9 := w10^15;
w2 := w7 * w9;
L:=sub<G|w1,w2>; // L is isomorphic to 2^(1+8).(A5xA5).2.2

S2:=SylowSubgroup(L,5);
// a Sylow 5-subgroup of L, which is isomorphic to 5^2 and contains
// elements of class 5B, 5C and 5D
for z in S2 do // check the proposition for z of class 5B, 5C and 5D
    if Order(z) eq 5 then
        repeat
            h:=Random(G);
            x:=z^h; // a random element in z^T
        until #sub<T|x,y> eq t and not exists(a){a:a in Inv | x^a eq x^(-1)};
    end if;
end for;
```

A.2 GAP code

Throughout this section, let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive sporadic group with socle T and point stabiliser H. The character table of G can be accessed via the Character Table Library of GAP [12], and one can use the function Maxes to access the character table of H unless

$G = \mathbb{M}$ is the Monster group. Moreover, if $G \neq \mathbb{M}$ and $(G,H) \neq (\mathbb{B},(2^2 \times F_4(2)){:}2)$, the fusion map from H-classes to G-classes is also available in [12].

A.2.1 Probability

First, we present the function to compute $\widehat{Q}(G,c)$, recalling that

$$\widehat{Q}(G,c) = \sum_{i=1}^{k} \frac{|x_i^G \cap H|^c}{|x_i^G|^{c-1}},$$

where $\bigcup_i x_i^G$ is the set of elements of prime order in G. The input of the following function is the character table of G, the character table of H and an integer c. It returns the precise value of $\widehat{Q}(G,c)$.

```
Q:=function(T,t,c);
F:=FusionConjugacyClasses(t,T);;
O:=OrdersClassRepresentatives(t);;
P:=[];;
for i in [1..Size(O)] do
    if IsPrime(O[i]) then
    Add(P,i);;
    fi;
od;
PO:=[];;
for i in P do
    Add(PO,F[i]);;
od;
fO:=Set(PO);;
nO:=[];;
for n in fO do
    N:=[];;
    for i in [1..Size(P)] do
        if PO[i] = n then Add(N,P[i]);; fi;
    od;
    Add(nO,N);;
od;
S:=SizesConjugacyClasses(T);;
s:=SizesConjugacyClasses(t);;
q:=0;;
for i in [1..Size(nO)] do
    n:=nO[i];;
    a:=0;;
    for j in [1..Size(n)] do
        a:=a+s[n[j]];;
    od;
    b:=S[f0[i]];;
    q:=q+a^c/(b^(c-1));;
od;
return q;;
end;
```

For example, in the proof of Theorem 4.4.4 we need to show that $\widehat{Q}(G,b(G)) < 1/2$ for the case $(G,H) = (\mathrm{Co}_1, 3.\mathrm{Suz{:}2})$, noting that $b(G) = 4$ by [30, Theorem 1]. The code

```
T:=CharacterTable("Co1");;
M:=Maxes(T);;
t:=CharacterTable(M[2]);;
Q(T,t,4);
```

returns

```
12413565400307859/68375035904000000
```

which is the precise $\widehat{Q}(G,b(G))$. It is then routine to check that $\widehat{Q}(G,b(G)) < 1/2$.

Note that the function Q requires the information of the fusion map from H-classes to G-classes. For the group with $G = \mathbb{B}$ and $H = (2^2 \times F_4(2)){:}2$, this information is not stored in GAP, and so the function Q does not work. In this setting, we use the function `PossibleClassFusions` instead of `FusionConjugacyClasses`, which returns the possible fusion maps. All possibilities for this fusion yield the same value for $\widehat{Q}(G,b(G))$, which is

$$281269824015848730254/18329682579606295200703125 \approx 1.534 \times 10^{-5}.$$

A.2.2 Proof of Proposition 5.6.10

Finally, let us present the GAP code for the computations in the proof of Proposition 5.6.10 for the groups with

$$T \in \mathscr{B} := \{\mathrm{M}_{11},\ \mathrm{M}_{22},\ \mathrm{M}_{23},\ \mathrm{M}_{24},\ \mathrm{McL},\ \mathrm{J}_4,\ \mathrm{Co}_1,\ \mathrm{Co}_2,\ \mathrm{Co}_3,\ \mathrm{Ru},\ \mathrm{Fi}_{23},\ \mathrm{Fi}_{24}',\ \mathrm{Th},\ \mathrm{Ly}\}.$$

Recall that a T-conjugacy class y^T is called a *witness* if for any $z \in T^{\#}$, there exists $x \in z^T$ such that $\langle x,y\rangle = T$. In other words, y^T is a witness if, for any $z \in T^{\#}$ or prime order, the probability $\mathbb{P}_z(y)$ that z and a uniformly random element in y^T generate T is positive. As noted in [63, Section 2.2], we have

$$1 - \mathbb{P}_z(y) \leqslant \sum_{K \in \mathscr{M}(y)} \frac{|z^T \cap K|}{|z^T|} =: \widehat{\mathbb{Q}}_z(y),$$

where $\mathcal{M}(y)$ is the set of maximal subgroups of T containing y.

Our aim here is to determine whether or not there exists an element $y \in T$ (with $T \in \mathscr{B}$) such that $y^{-1} \notin y^{\mathrm{Aut}(T)}$ and $\widehat{\mathbb{Q}}_z(y) < 1$ for all $z \in T^{\#}$. Note that the former condition can be checked easily via the function InverseClasses on the character table of $\mathrm{Aut}(T)$, while the latter condition implies that y^T is a witness. The elements y satisfying the required properties can be obtained via the following code (here we take $T = \mathrm{Fi}_{24}'$ as an example, and the other cases with $T \in \mathscr{B}$ can be handled similarly).

```
T:=CharacterTable("Fi24");;
G:="Fi24’";;
t:=CharacterTable(G);;
Fu:=FusionConjugacyClasses(t,T);;
Inv:=InverseClasses(T);;
o:=OrdersClassRepresentatives(t);;
m:=Maxes(t);;
D:=[];;
for k in [1..Size(m)] do
    t1:=CharacterTable(m[k]);;
    chi:=TrivialCharacter(t1)^t;;
    Add(D,[t1,chi]);;
od;
P:=PrimeDivisors(Size(t));;
Q:=[];;
for j in [2..Size(o)] do
    if o[j] in P then Add(Q,j);; fi;
od;
for j in [2..Size(o)] do
    B:=[];;
    F:=[];;
    C:=[];;
    for k in [1..Size(m)] do
        t1:=D[k][1];;
        chi:=D[k][2];;
        if chi[j] > 0 then
            Add(F,m[k]);;
            Add(C,chi[j]);;
        fi;
    od;
    for q in Q do
```

```
        z:=0;;
        for k in [1..Size(m)] do
            t1:=D[k][1];;
            chi:=D[k][2];;
            z:=z+chi[j]*chi[q]*Size(t1)/Size(t);;
        od;
        Add(B,z);;
    od;
    a:=Fu[j];;
    if Maximum(B) < 1 and not Inv[a] = a then
        Print(AtlasClassNames(t)[j],"\n",F,"\n",C,"\n","\n");
    fi;
od;
```

The output is as follows:

```
23A
[ "Fi23", "F3+M7" ]
[ 1, 1 ]

23B
[ "Fi23", "F3+M7" ]
[ 1, 1 ]
```

which means that there are precisely two witnesses y^T such that $y^{-1} \notin y^{\mathrm{Aut}(T)}$, namely the classes 23A and 23B. In either case, y has precisely 2 maximal overgroups in T, which are isomorphic to Fi_{23} and $2^{11}.\mathrm{M}_{24}$, respectively.

BIBLIOGRAPHY

[1] A. Aabrandt and V.L. Hansen, *The circle equation over finite fields*, Quaest. Math. **41** (2018), 665–674.

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

[3] M. Aschbacher and L. Scott, *Maximal subgroups of finite groups*, J. Algebra **92** (1985), 44–80.

[4] M. Aschbacher and G.M. Seitz, *Involutions in Chevalley groups over fields of even order*, Nagoya Math. J. **63** (1976), 1–91.

[5] R.W. Baddeley, *Primitive permutation groups with a regular nonabelian normal subgroup*, Proc. London Math. Soc. **67** (1993), 547–595.

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

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

[8] A. Bochert, *Ueber die Zahl der verschiedenen Werthe, die eine Function gegebener Buchstaben durch Vertauschung derselben erlangen kann*, Math. Ann. **33** (1889), no.4, 584–590.

[9] A.V. Borovik, *The structure of finite subgroups of simple algebraic groups* (Russian), Algebra i Logika **28** (1989), 249–279, 366; translation in Algebra and Logic **28** (1989), 163–182.

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

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

[12] T. Breuer, *The GAP Character Table Library, Version 1.3.1*, GAP package, `http://www.math.rwth-aachen.de/~Thomas.Breuer/ctbllib`, 2020.

[13] T. Breuer, R.M. Guralnick and W.M. Kantor, *Probabilistic generation of finite simple groups, II*, J. Algebra **320** (2008), 443–494.

[14] T.C. Burness, *Base sizes for primitive groups with soluble stabilisers*, Algebra Number Theory **15** (2021), 1755–1807.

[15] T.C. Burness, *Fixed point ratios in actions of finite classical groups. I*, J. Algebra **309** (2007), 69–79.

[16] T.C. Burness, *Fixed point ratios in actions of finite classical groups. II*, J. Algebra **309** (2007), 80–138.

[17] T.C. Burness, *Fixed point ratios in actions of finite classical groups. III*, J. Algebra **314** (2007), 693–748.

[18] T.C. Burness, *Fixed point ratios in actions of finite classical groups. IV*, J. Algebra **314** (2007), 749–788.

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

[20] T.C. Burness and M. Giudici, *On the Saxl graph of a permutation group*, Math. Proc. Cambridge Philos. Soc. **168** (2020), 219–248.

[21] T.C. Burness and M. Giudici, *Classical groups, derangements and primes*, Australian Mathematical Society Lecture Series, vol. 25, Cambridge University Press, Cambridge, 2016.

[22] T.C. Burness and R.M. Guralnick, *Fixed point ratios for finite primitive groups and applications*, Adv. Math. **411** (2022), Paper No. 108778, 90 pp.

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

[24] T.C. Burness and S. Harper, *Finite groups, 2-generation and the uniform domination number*, Israel J. Math. **239** (2020), 271–367.

[25] T.C. Burness and S. Harper, *Computations concerning the uniform domination number of a finite simple group*, 2019, available at `http://seis.bristol.ac.uk/~tb13602/udncomp.pdf`.

[26] T.C. Burness and H.Y. Huang, *On base sizes for primitive groups of product type*, J. Pure Appl. Algebra **227** (2023), Paper No. 107228, 43 pp.

[27] T.C. Burness and H.Y. Huang, *On the Saxl graphs of primitive groups with soluble stabilisers*, Algebr. Comb. **5** (2022), 1053–1087.

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

[29] T.C. Burness, A. Lucchini and D. Nemmi, *On the soluble graph of a finite group*, J. Combin. Theory Ser. A **194** (2023), Paper No. 105708, 39 pp.

[30] T.C. Burness, E.A. O'Brien and R.A. Wilson, *Base sizes for sporadic simple groups*, Israel J. Math. **177** (2010), 307–333.

[31] T.C. Burness and A.R. Thomas, *The classification of extremely primitive groups*, Int. Math. Res. Not. IMRN 2022, 10148–10248.

[32] T.C. Burness and A.R. Thomas, *Computations concerning the classification of extremely primitive groups*, available at `http://seis.bristol.ac.uk/~tb13602/epcomp.pdf`.

[33] P.J. Cameron, *Permutation groups*, London Math. Soc. Student Texts, vol. 45, Cambridge University Press, 1999.

[34] P.J. Cameron, D.G. Fon-Der-Flaas, *Bases for permutation groups and matroids*, Eur. J. Comb. **16** (1995), 537–544.

[35] P.J. Cameron, P.M. Neumann and J. Saxl, *On groups with no regular orbits on the set of subsets*, Arch. Math. **43** (1984), 295–296.

[36] H. Chen and S. Du, *On the Burness-Giudici conjecture*, Comm. Algebra **51** (2023), 5019–5045.

[37] J. Chen and H.Y. Huang, *On valency problems of Saxl graphs*, J. Group Theory **25** (2022), 543–577.

[38] B.N. Cooperstein, *Maximal subgroups of $G_2(2^n)$*, J. Algebra **70** (1981), 23–36.

[39] A.M. Cohen, M.W. Liebeck, J. Saxl and G.M. Seitz, *The local maximal subgroups of exceptional groups of Lie type, finite and algebraic*, Proc. London Math. Soc. **64** (1992), 21–48.

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

[41] D.A. Craven, *The maximal subgroups of the exceptional groups $F_4(q)$, $E_6(q)$ and ${}^2E_6(q)$ and related almost simple groups*, Invent. Math. **234** (2023), 637–719.

[42] D.A. Craven, *On the maximal subgroups of $E_7(q)$ and related almost simple groups*, submitted (2022), arXiv:2201.07081.

[43] C. del Valle and C.M. Roney-Dougal, *The base size of the symmetric group acting on subsets*, Algebr. Comb. **7** (2024), 959–967.

[44] L.E. Dickson, *Linear groups, with an exposition of the Galois Field Theory*, Teubner, Leipzig, 1901.

[45] H. Dietrich, M. Lee and T. Popiel, *The maximal subgroups of the Monster*, Adv. Math. **469** (2025), Paper No. 110214, 33 pp.

[46] G.A. Dirac, *Some theorems on abstract graphs*, Proc. London Math. Soc. **2** (1952), 69–81.

[47] S. Dolfi, *Orbits of permutation groups on the power set*, Arch. Math. **75** (2000), 321–327.

[48] H. Duyan, Z. Halasi and A. Maróti, *A proof of Pyber's base size conjecture*, Adv. Math. **331** (2018), 720–747.

[49] I.A. Faradžev and A.A. Ivanov, *Distance-transitive representations of groups G with* $\mathrm{PSL}_2(q) \trianglelefteq G \trianglelefteq \mathrm{P\Gamma L}_2(q)$, European J. Combin. **11** (1990), 347–356.

[50] J.B. Fawcett, *Bases of twisted wreath products*, J. Algebra **607** (2022), 247–271.

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

[52] S.D. Freedman, H.Y. Huang, M. Lee and K. Rekvényi, *On the generalised Saxl graphs of permutation groups*, submitted (2024), arXiv:2410.22613.

[53] J. Fulman and R.M. Guralnick, *The number of regular semisimple conjugacy classes in the finite classical groups*, Linear Algebra Appl. **439** (2013), 488–503.

[54] J. Fulman and R.M. Guralnick, *Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements*, Trans. Amer. Math. Soc. **364** (2012), 3023–3070.

[55] P.X. Gallagher, *The number of conjugacy classes in a finite group*, Math. Z. **118** (1970), 175–179.

[56] S. Garion, *Expansion of conjugacy classes in* $\mathrm{PSL}_2(q)$, J. Group Theory **18** (2015), 961–980.

[57] D. Garzoni and N. Gill, *On the number of conjugacy classes of a primitive permutation group*, Proc. Roy. Soc. Edinburgh Sect. A **153** (2023), 115–136.

[58] N. Gill, B. Lodà and P. Spiga, *On the height and relational complexity of a finite permutation group*, Nagoya Math. J. **246** (2022), 372–411.

[59] D. Gluck, K. Magaard, U. Riese and P. Schmid, *The solution of the $k(GV)$-problem*, J. Algebra **279** (2004), 694–719.

[60] D. Gorenstein, R. Lyons and R. Solomon, *The Classification of the Finite Simple Groups. Number 3*, Mathematical Surveys and Monographs, vol. 40. American Mathematical Society, Providence, RI., 1998.

[61] R. Gow, *Commutators in finite simple groups of Lie type*, Bull. London Math. Soc. **32** (2000), 311–315.

[62] S. Guest, J. Morris, C.E. Praeger and P. Spiga, *On the maximum orders of elements of finite almost simple groups and primitive permutation groups*, Trans. Amer. Math. Soc. **367** (2015), 7665–7694.

[63] R.M. Guralnick and W.M. Kantor, *Probabilistic generation of finite simple groups*, J. Algebra **234** (2000), 743–792.

[64] R.M. Guralnick and K. Magaard, *On the minimal degree of a primitive permutation group*, J. Algebra **207** (1998), 127–145.

[65] R.M. Guralnick and G. Malle, *Simple groups admit Beauville structures*, J. Lond. Math. Soc. **85** (2012), 694–721.

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

[67] Z. Halasi, M.W. Liebeck and A. Maróti, *Base sizes of primitive groups: bounds with explicit constants*, J. Algebra **521** (2019), 16–43.

[68] Z. Halasi and K. Podoski, *Every coprime linear group admits a base of size two*, Trans. Amer. Math. Soc. **368** (2016), 5857–5887.

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

[70] H.Y. Huang, *On chiral generating pairs of finite simple groups*, in preparation.

[71] H.Y. Huang, *Base sizes of primitive groups of diagonal type*, Forum Math. Sigma **12** (2024), Paper No. e2, 43 pp.

[72] B. Huppert. *Endliche Gruppen. I.*. Die Grundlehren der mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin-New York, 1967.

[73] B. Huppert, *Zweifach transitive, auflösbare Permutationsgruppen*, Math. Z. **68** (1957), 126–150.

[74] G.A. Jones, *Finite simple automorphism groups of edge-transitive maps*, J. Algebra **607** (2022), 454–472.

[75] C. Jordan, *Sur la limite de transitivité des groupes non alternés*, Bull. Soc. Math. France **1** (1872/73), 40–71.

[76] W.M. Kantor, *Primitive permutation groups of odd degree, and an application to finite projective planes*, J. Algebra **106** (1987), 15–45.

[77] W.M. Kantor, A. Lubotzky and A. Shalev, *Invariable generation and the Chebotarev invariant of a finite group*, J. Algebra **348** (2011), 302–314.

[78] P.B. Kleidman, *The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, the Ree groups ${}^2G_2(q)$, and their automorphism groups*, J. Algebra **117** (1988), 30–71.

[79] P.B. Kleidman, *The maximal subgroups of the Steinberg triality groups ${}^3D_4(q)$ and of their automorphism groups*, J. Algebra **115** (1988), 182–199.

[80] P.B. Kleidman and M.W. Liebeck, *The subgroup structure of the finite classical groups*, London Math. Soc. Lecture Note Series, vol. 129, Cambridge University Press, 1990.

[81] L.G. Kovács, *Primitive subgroups of wreath products in product action*, Proc. London Math. Soc. **58** (1989), 306–322.

[82] R. Lawther, M.W. Liebeck and G.M. Seitz, *Fixed point ratios in actions of finite exceptional groups of Lie type*, Pacific J. Math. **205** (2002), 393–464.

[83] M. Lee, *Regular orbits of quasisimple linear groups I*, J. Algebra **586** (2021), 1122–1194.

[84] M. Lee, *Regular orbits of quasisimple linear groups II*, J. Algebra **586** (2021), 643–717.

[85] M. Lee and T. Popiel, *Saxl graphs of primitive affine groups with sporadic point stabilisers*, Internat. J. Algebra Comput. **33** (2023), 369–389.

[86] D. Leemans and M.W. Liebeck, *Chiral polyhedra and finite simple groups*, Bull. Lond. Math. Soc. **49** (2017), 581–592.

[87] C.H. Li and H. Zhang, *The finite primitive groups with soluble stabilizers, and the edge-primitive s-arc-transitive graphs*, Proc. Lond. Math. Soc. **103** (2011), 441–472.

[88] M.W. Liebeck, C.E. Praeger and J. Saxl, *On the O'Nan-Scott theorem for finite primitive permutation groups*, J. Austral. Math. Soc. **44** (1988), 389–396.

[89] M.W. Liebeck, C.E. Praeger and J. Saxl, *A classification of the maximal subgroups of the finite alternating and symmetric groups*, J. Algebra **111** (1987), 365–383.

[90] M.W. Liebeck and J. Saxl, *Maximal subgroups of finite simple groups and their automorphism groups*, in Proceedings of the International Conference on Algebra, Part 1 (Novosibirsk, 1989), 243–259, Contemp. Math., 131, Part 1, Amer. Math. Soc., Providence, RI, 1992.

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

[92] M.W. Liebeck and J. Saxl, *The primitive permutation groups of odd degree*, J. London Math. Soc. **31** (1985), 250–264.

[93] M.W. Liebeck, J. Saxl and G.M. Seitz, *Subgroups of maximal rank in finite exceptional groups of Lie type*, Proc. London Math. Soc. **65** (1992), 297–325.

[94] M.W. Liebeck and G.M. Seitz, *Unipotent and nilpotent classes in simple algebraic groups and Lie algebras*, Mathematical Surveys and Monographs, vol. 180, Amer. Math. Soc., 2012.

[95] M.W. Liebeck and G.M. Seitz, *Maximal subgroups of exceptional groups of Lie type, finite and algebraic*, Geom. Dedicata **35** (1990), 353–387.

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

[97] F. Lübeck, *Centralisers and numbers of semisimple classes in exceptional groups of Lie type*, `http://www.math.rwth-aachen.de/~Frank.Luebeck/chev/CentSSClasses`

[98] A. Lucchini, M. Morigi and M. Moscatiello, *Primitive permutation IBIS groups*, J. Combin. Theory Ser. A **184** (2021), Paper No. 105516, 17 pp.

[99] G. Malle, *The maximal subgroups of* ${}^2F_4(q^2)$, J. Algebra **139** (1991), 52–69.

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

[101] G. Mecenero and P. Spiga, *A formula for the base size of the symmetric group in its action on subsets*, Australas. J. Combin. **88** (2024), 244–255.

[102] G.A. Miller, *On the groups generated by two operators*, Bull. Amer. Math. Soc. **7** (1901), 424–426.

[103] J. Morris and P. Spiga, *On the base size of the symmetric and the alternating group acting on partitions*, J. Algebra **587** (2021), 569–593.

[104] M. Neunhöffer, F. Noeske, E.A. O'Brien and R.A. Wilson, *Orbit invariants and an application to the Baby Monster*, J. Algebra **341** (2011), 297–305.

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

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

[107] H. Robbins, *A remark on Stirling's formula*, Amer. Math. Monthly **62** (1955), 26–29.

[108] J.B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.

[109] Á. Seress, *Primitive groups with no regular orbits on the set of subsets*, Bull. London Math. Soc. **29** (1997), 697–704.

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

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

[112] D. Singerman, *Symmetries of Riemann surfaces with large automorphism group*, Math. Ann. **210** (1974), 17–32.

[113] N. Spaltenstein, *Caractères unipotents de* ${}^3D_4(\mathbb{F}_q)$, Comment. Math. Helv. **57** (1982), 676–691.

[114] P. Stănică, *Good lower and upper bounds on binomial coefficients*, JIPAM. J. Inequal. Pure Appl. Math. **2** (2001), Article 30, 5 pp.

[115] R.P. Stanley, *Enumerative combinatorics. Volume 1*, Second edition. Cambridge Studies in Advanced Mathematics, vol. 49. Cambridge University Press, 2012.

[116] R. Steinberg, *Lectures on Chevalley groups*, Univ. Lecture Ser., vol. 66, American Mathematical Society, Providence, RI, 2016.

[117] M. Suzuki, *On a class of doubly transitive groups*, Annals of Math. **75** (1962), 105–145.

[118] K.B. Tchakerian, *The maximal subgroups of the Tits simple group*, Pliska Stud. Math. Bulgar. **8** (1986), 85–93.

[119] H.N. Ward, *On Ree's series of simple groups*, Trans. Amer. Math. Soc. **121** (1966), 62–89.

[120] R.A. Wilson, *Maximal subgroups of sporadic groups*, in Finite simple groups: thirty years of the Atlas and beyond, 57–72, Contemp. Math., vol. 694, Amer. Math. Soc., Providence, RI, 2017.

[121] R.A. Wilson, *The finite simple groups*, Grad. Texts in Math., vol. 251, Springer-Verlag London, Ltd., London, 2009.

[122] R.A. Wilson, *The geometry and maximal subgroups of the simple groups of A. Rudvalis and J. Tits*, Proc. London Math. Soc. **48** (1984), 533–563.

[123] R.A. Wilson et al., *A World-Wide-Web Atlas of finite group representations*, `http://brauer.maths.qmul.ac.uk/Atlas/v3/`

[124] R.A. Wilson, R.A. Parker, S. Nickerson, J.N. Bray and T. Breuer, *AtlasRep GAP Package, Version 2.1.6*, 2022.