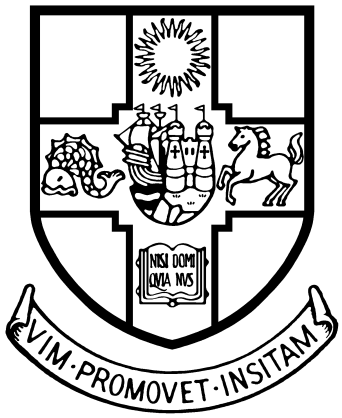
Author:
Harper, Scott

Title:
On the Spread of Classical Groups

On the Spread of Classical Groups

Scott Harper



University of Bristol

School of Mathematics

April 2019

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

approx. 51,888 words

Abstract

It is well known that every finite simple group can be generated by two elements. In 2000, Guralnick and Kantor resolved a 1962 question of Steinberg by proving that in a finite simple group every nontrivial element belongs to a generating pair. Groups with this property are said to be $\frac{3}{2}$-generated.

It is natural to ask which groups are $\frac{3}{2}$-generated. It is easy to see that every proper quotient of a $\frac{3}{2}$-generated group is cyclic, and in 2008, Breuer, Guralnick and Kantor made the striking conjecture that this condition alone provides a complete characterisation of the finite groups with this property. That is, they conjectured that a finite group is $\frac{3}{2}$-generated if and only if every proper quotient of the group is cyclic. This conjecture has been reduced to the almost simple groups through recent work of Guralnick. By work of Piccard (1939) and Woldar (1994), the conjecture is known to be true for almost simple groups whose socles are alternating or sporadic groups. Therefore, the central focus is the almost simple groups of Lie type.

In this thesis we prove a stronger version of this conjecture for almost simple symplectic and orthogonal groups, building on earlier work of Burness and Guest (2013) for linear groups. More generally, we study the uniform spread of these groups, obtaining lower bounds and related asymptotics. We adopt a probabilistic approach using fixed point ratios, which relies on a detailed analysis of the conjugacy classes and subgroup structure of the almost simple classical groups.

Acknowledgements

First of all, I would like to thank Tim Burness, who has taught me a great deal over the past four years, both about mathematics and being a mathematician. Thank you for your patience, encouragement and unbelievable attention to detail.

Chris Parker and Jeremy Rickard deserve much thanks for examining this thesis and for their wise comments on my work. I also wish to thank Robert Guralnick for several helpful discussions on topics featured in this thesis.

I want to thank the algebra group in Bristol for many interesting and entertaining discussions and the staff of the Quinton House for facilitating these conversations.

Thanks to all of the mathematics PhD students in Bristol, who made being a postgraduate student a real joy. Special thanks go to those in the second floor office, who provided support and distraction in perfect proportions. Joe Allen deserves particular mention on account of his truly encouraging nature and his skill in setting an Easter egg hunt.

Let me thank the Engineering and Physical Sciences Research Council, the Heilbronn Institute for Mathematical Research and the London Mathematical Society, who provided the funding for this research to happen and for me to travel the world in the process.

I am very grateful to the mathematicians across the world who have welcomed me as a visitor, particularly those in Australia and New Zealand, who made me feel at home while visiting their beautiful countries.

Thanks to James Ward for being an excellent flatmate and for keeping me interested in the world beyond mathematics.

Of course deep and heartfelt thanks go to my parents and grandparents, who have always encouraged me to pursue my interests. Thank you for believing that my work involves more than making pictures of butterflies.

In the words of Psalm 124, featured on the University's crest: If it had not been the LORD who was on our side ...

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.

Signature: ..... Date: .....

Contents

1 Introduction **1**

2 Preliminaries **9**
2.1 Probabilistic method 10
2.2 Classical groups 12
2.3 Semisimple elements in classical groups 19
2.4 Conjugacy in classical groups 32
2.5 Maximal subgroups of classical groups 37
2.6 Algebraic groups 43
2.7 Shintani descent 53
2.8 Computational methods 60

3 Fixed Point Ratios **61**
3.1 Subspace actions 62
3.2 Nonsubspace actions 69

4 Groups of Types B_m and C_m **75**
4.1 Automorphisms 79
4.2 Case I 83
4.3 Case II 85
4.4 Case III 105

5 Groups of Type D_m **113**
5.1 Automorphisms 116
5.2 Case I 122
5.3 Case II 133

A MAGMA Code **157**

References **163**

Tables

2.1 Finite simple classical groups 15
2.2 Geometric subgroups 38
2.3 Exceptions in Theorem 2.5.14 when $q > p$ 42
2.4 Simple classical algebraic groups 44

3.1 Fixed point ratios: Values of a, b, c 62

4.1 The relevant automorphisms in types B_m and C_m 81
4.2 Case II: The element y for the automorphism θ 87
4.3 Case II: Description of $\mathcal{M}(G, t\theta)$ 88
4.4 Case III: Description of $\mathcal{M}(G, t\theta)$ 107

5.1 The relevant automorphisms θ in type D_m 120
5.2 Case I(b): Description of $\mathcal{M}(G, y)$ 126
5.3 Definition of Cases II(i)–(v) 133
5.4 Case II(a): The element y for the automorphism θ 136
5.5 Case II(a): Description of $\mathcal{M}(G, t\theta)$ 138
5.6 Case II(b): The element y for the automorphism θ 145
5.7 Case II(b): Description of $\mathcal{M}(G, t\theta)$ for $m \notin \{5, 7\}$ 147
5.8 Case II(b): Description of $\mathcal{M}(G, t\theta)$ for $m \in \{5, 7\}$ 148

1

Introduction

There is a long and rich history of studying generating sets for groups. We say that a group is d-generated if it has a generating set of size d. Many familiar groups are 2-generated. For instance, the symmetric group S_n is generated by $(1\,2)$ and $(1\,2\,\ldots\,n)$. This thesis is concerned with proving that a general class of groups are 2-generated in a very strong sense. We begin by providing some historical context.

For a 2-generated group G, it is natural to ask how likely it is that a randomly chosen pair of elements generate G. As early as 1882, Netto [55] wrote the following

> *If we arbitrarily select two or more [permutations] of n elements, it is to be regarded as extremely probable that the group of lowest order which contains these is the symmetric group, or at least the alternating group.*

That two elements of the alternating group almost surely generate the entire group became known as Netto's Conjecture and was proved by Dixon in 1969 [26]. Moreover, Dixon conjectured that two elements of any finite simple group almost surely generate it.

A group is *simple* if it has no proper nontrivial normal subgroups. Therefore, the simple groups are the indivisible groups, and, accordingly, these groups play a fundamental role in the general theory of groups. Indeed, many problems about all finite groups can be reduced to ones about finite simple groups. The simple groups have some remarkable properties, and generation is one lens through which we see their striking behaviour.

By the *Classification of Finite Simple Groups*, every finite simple group is a cyclic group of prime order, an alternating group of degree at least five, a finite group of Lie type or one of twenty-six sporadic groups.

In 1962, Steinberg [60] proved that every finite simple group of Lie type is 2-generated, by exhibiting an explicit pair of generators. In light of the Classification, we know that the conclusion holds for every finite simple group. Moreover, in 1997, building on previous work of Kantor and Lubotzky [40], Liebeck and Shalev [51] proved Dixon's Conjecture.

For groups with many generating pairs, it is natural to ask how these pairs are distributed across the group. In the opening of his 1962 paper on the 2-generation of the groups of Lie type, Steinberg wrote

> *It is possible that one of the generators can be chosen of order 2, as is the case for the projective unimodular group, or even that one of the generators can be chosen as an arbitrary element other than the identity, as is the case for the alternating groups. Either of these results, if true, would quite likely require methods much more detailed than those used here.*

This comment motivates the following definition, which plays a central role in this thesis.

Definition. A group G is $\frac{3}{2}$-*generated* if for every nontrivial element $g \in G$, there exists an element $h \in G$ such that $\langle g, h \rangle = G$.

Steinberg predicted that different methods would be required to prove that the finite simple groups are $\frac{3}{2}$-generated, if indeed they are. In recent years, probabilistic methods have been very successful in solving several formidable deterministic problems in group theory [15, 47, 57]. Indeed, through a probabilistic approach, in 2000, Guralnick and Kantor [33] proved that every finite simple group is $\frac{3}{2}$-generated.

Classifying the 1-generated groups is trivial and classifying the 2-generated groups is impossible. Can we classify the $\frac{3}{2}$-generated groups? It is straightforward to demonstrate that every proper quotient of an arbitrary $\frac{3}{2}$-generated group is necessarily cyclic. In 2008, Breuer, Guralnick and Kantor [10] conjectured that this evidently necessary condition is actually sufficient for finite groups.

Conjecture. *A finite group is $\frac{3}{2}$-generated if and only if every proper quotient is cyclic.*

The aim of this thesis is to make substantial progress towards proving this conjecture, which we refer to as the $\frac{3}{2}$-Generation Conjecture.

Let us note that this necessary condition for $\frac{3}{2}$-generation is not sufficient for infinite groups. For example, the infinite alternating group A_∞ is simple but not finitely generated, let alone $\frac{3}{2}$-generated. However, the author is not aware of any 2-generated group with no noncyclic proper quotients that is not $\frac{3}{2}$-generated.

The $\frac{3}{2}$-Generation Conjecture is true for soluble groups [8, Theorem 2.01]. Recent work of Guralnick [32] establishes a reduction of the conjecture to the almost simple groups. A group G is *almost simple* if $T \leqslant G \leqslant \mathrm{Aut}(T)$ for a nonabelian simple group T. In this case, T is the *socle* of G. Therefore, to prove the $\frac{3}{2}$-Generation Conjecture for almost simple groups is exactly to prove that $\langle T, \theta \rangle$ is $\frac{3}{2}$-generated for all nonabelian simple groups T and automorphisms $\theta \in \mathrm{Aut}(T)$.

The alternating and symmetric groups of degree at least 5 have been known to be $\frac{3}{2}$-generated since the work of Piccard in 1939 [56], to which Steinberg refers in the quote above. In addition, the $\frac{3}{2}$-generation of the relevant almost simple sporadic groups (and the two further almost simple cyclic extensions of A_6) follows from the computational results of Breuer, Guralnick and Kantor [10] (see also [64]). Therefore, to prove the $\frac{3}{2}$-Generation Conjecture, it suffices to focus on almost simple groups of Lie type.

In 2013, Burness and Guest [18] proved the $\frac{3}{2}$-Generation Conjecture for almost simple groups with socle $\mathrm{PSL}_n(q)$. They followed the probabilistic approach of Guralnick and Kantor in [33] but brought a powerful technique to the problem: *Shintani descent* (see p.5). This thesis is inspired by the work of Guralnick and Kantor and of Burness and Guest.

In this thesis we prove the following theorem.

Theorem. *Let G be an almost simple group whose socle is a symplectic or orthogonal group other than $\mathrm{P}\Omega_8^+(q)$. Then G is $\frac{3}{2}$-generated if every proper quotient of G is cyclic.*

There are natural generalisations of $\frac{3}{2}$-generation.

Definition. Let G be a finite group.

(i) The *spread* of G, written $s(G)$, is the greatest integer k such that for any k nontrivial elements $x_1, \ldots, x_k$, there exists $y \in G$ such that

$$\langle x_1, y \rangle = \langle x_2, y \rangle = \cdots = \langle x_k, y \rangle = G.$$

(ii) The *uniform spread* of G, written $u(G)$, is the greatest integer k for which there exists a fixed conjugacy class C such that for any k nontrivial elements $x_1, \ldots, x_k$, there exists an element $y \in C$ satisfying the above equalities.

Observe that $s(G) \geqslant u(G)$ and that $s(G) \geqslant 1$ if and only if G is $\frac{3}{2}$-generated.

If G is simple, then Breuer, Guralnick and Kantor [10] proved that $u(G) \geqslant 2$ with equality if and only if $G \in \{A_5, A_6, \Omega_8^+(2)\}$ or G is $\mathrm{Sp}_{2m}(2)$ for $m \geqslant 3$. This generalises the result that $s(G) \geqslant 1$ for simple groups G. Moreover, if (G_i) is a sequence of simple groups with $|G_i| \to \infty$, then Guralnick and Shalev [37] proved that $u(G_i) \to \infty$ if and only if there is not an infinite subsequence consisting of: alternating groups of degree all divisible by a fixed prime; or odd-dimensional orthogonal groups over a field of fixed size; or symplectic groups over a field of even characteristic and fixed size.

It is natural to seek analogues of these stronger results for almost simple groups. If G is an almost simple group with socle $\mathrm{PSL}_n(q)$, then Burness and Guest [18] proved that $u(G) \geqslant 2$, unless $G = \mathrm{PSL}_2(9).2 \cong S_6$, for which $s(G) = 2$ but $u(G) = 0$. Moreover, they determined when sequences of such groups have bounded uniform spread. In this thesis we establish similar results for almost simple symplectic and orthogonal groups.

We now present our two main results of the thesis.

Theorem A. *Let G be an almost simple group whose socle is a symplectic or orthogonal group other than $\mathrm{P\Omega}_8^+(q)$. If $G/\mathrm{soc}(G)$ is cyclic, then $u(G) \geqslant 2$, unless $G = \mathrm{Sp}_4(2)'.2 \cong S_6$.*

Theorem B. *Let (G_i) be a sequence of almost simple groups whose socles are symplectic or orthogonal groups other than $\mathrm{P\Omega}_8^+(q)$. Assume that $G_i/\mathrm{soc}(G_i)$ is cyclic and $|G_i| \to \infty$. Then $u(G_i) \to \infty$ if (G_i) does not have an infinite subsequence of groups satisfying one of the following*

(i) $\mathrm{soc}(G_i) = \mathrm{Sp}_{2m_i}(q)$ *for a fixed even q*

(ii) $\mathrm{soc}(G_i) = \Omega_{2m_i+1}(q)$ *for a fixed odd q*

(iii) $\mathrm{soc}(G_i) = \mathrm{P\Omega}^{\pm}_{2m_i}(q)$ *for a fixed q and G_i contains a graph automorphism.*

Moreover, the spread of the groups in (i) *and* (ii) *is bounded.*

The author suspects that the spread of the groups in (iii) is also bounded, and this will feature in future work (see Remark 5.3.25).

For symplectic and odd-dimensional orthogonal groups, we establish stronger results and we refer the reader to the introduction to Chapter 4 for statements and discussions of these results (particularly Theorems 4C and 4D).

Let us now turn to a brief discussion of the techniques employed in this thesis. The framework for proving Theorems A and B is given by the probabilistic method introduced by Guralnick and Kantor [33]. We give a full account of this method in Section 2.1. The general idea is to select an element $s \in G$ and show that s^G witnesses that $u(G) \geqslant k$. To do this, we let $P(x, s)$ be the probability that $\langle x, z \rangle \neq G$ for a random conjugate z of s. Evidently, $u(G) \geqslant 1$ if $P(x, s) < 1$ for all nontrivial $x \in G$. Indeed, $u(G) \geqslant k$ if $P(x, s) < \frac{1}{k}$ for all prime order $x \in G$ (see Lemma 2.1.1(i)).

Let $\mathcal{M}(G, s)$ be the set of maximal subgroups of G that contain s. In addition, for $H \leqslant G$ and $x \in G$, let $\mathrm{fpr}(x, G/H)$ be the *fixed point ratio* of x in the action of G on G/H. Then, by Lemma 2.1.1(ii)

$$P(x, s) \leqslant \sum_{H \in \mathcal{M}(G,s)} \mathrm{fpr}(x, G/H).$$

Therefore, our probabilistic method has three steps: select an appropriate element $s \in G$, determine $\mathcal{M}(G, s)$ and use fixed point ratio estimates to bound $P(x, s)$.

Selecting a viable element $s \in G$ is perhaps the most interesting and challenging aspect of the proofs. Write $G = \langle T, \theta \rangle$ where $T = \mathrm{soc}(G)$ and $\theta \in \mathrm{Aut}(T)$. If s^G witnesses $u(G) \geqslant k > 0$, then s is not contained in any proper normal subgroup of G, so we may assume that $s \in T\theta$. Consequently, we need to understand the conjugacy classes in the coset $T\theta$. In many cases, we apply Shintani descent to do this.

The modern way of studying the finite groups of Lie type is to view them as the fixed points under Steinberg endomorphisms of simple algebraic groups. Shintani descent is a technique residing in this general setting, which in the main part has been applied in character theory [41, 58]. At the heart of this method is a bijection with useful group theoretic properties that, given a connected algebraic group X, a Steinberg endomorphism σ of X and an integer $e > 1$, provides a correspondence between the conjugacy classes of elements in the coset $X_{\sigma^e}\sigma$ and in the subgroup X_σ. We use this bijection to transform a problem about almost simple groups into one about simple groups.

In this thesis we provide new ways of using Shintani descent to overcome various difficulties and subtleties which the symplectic and orthogonal groups pose. For example, even-dimensional orthogonal groups have a particularly intricate automorphism group; $\mathrm{Sp}_4(2^f)$ admits a graph-field automorphism; and symplectic groups in even characteristic have orthogonal groups as subgroups. We discuss these topics at length in the introductions to Chapters 4 and 5.

Our framework for understanding $\mathcal{M}(G, s)$ is provided by Aschbacher's subgroup structure theorem for finite classical groups [1] (see Section 2.5). The general idea of this theorem is that the maximal subgroups of classical groups are the stabilisers of geometric structures on the natural module, unless they arise from an absolutely irreducible representation of a quasisimple group. By studying how our chosen element, or a suitable power thereof, acts on the natural module, we can constrain the possible maximal subgroups that could contain this element.

Once we have a description of $\mathcal{M}(G, s)$, we use fixed point ratio estimates to bound $P(x, s)$. There is a vast literature on fixed point ratios for primitive actions of almost simple groups, and these quantities find applications to a wide variety of problems. In Chapter 3, we comment on some of these applications, record general results in this area and prove new fixed point ratio bounds that we require for our proofs.

The techniques developed in this thesis provide a framework for proving the $\frac{3}{2}$-Generation Conjecture for the remaining almost simple classical groups, namely, those whose socles are $\mathrm{P}\Omega_8^+(q)$ or unitary, and this will be the subject of imminent future work. For example, the obstacles posed by the twisted nature of the unitary groups can be surmounted using the methods developed for working with the minus-type orthogonal groups (see Remark 5.3.27). The group $\mathrm{P}\Omega_8^+(q)$ is the most exceptional classical group of Lie type. Both its triality automorphism and its low rank pose challenges, but we have strategies for facing them (see Remark 5.3.26).

The almost simple exceptional groups pose different challenges. On the one hand, the automorphism groups of exceptional groups have a more transparent structure and the setup afforded by Shintani descent presented in this thesis will provide a framework for proving the $\frac{3}{2}$-Generation Conjecture for these groups. On the other hand, we will need to use different techniques to study the maximal overgroups in exceptional groups. Through the study of the exceptional groups in future work the author aims to prove the $\frac{3}{2}$-Generation Conjecture in full generality.

The work in this thesis suggests the following two conjectures, which aver that spread and uniform spread are intimately connected.

Conjecture A. *Let G be a nonabelian finite group other than the symmetric group S_6. Then*

$$s(G) \geqslant 1 \iff s(G) \geqslant 2 \iff u(G) \geqslant 1 \iff u(G) \geqslant 2.$$

Moreover, each of these conditions is equivalent to every proper quotient of G being cyclic.

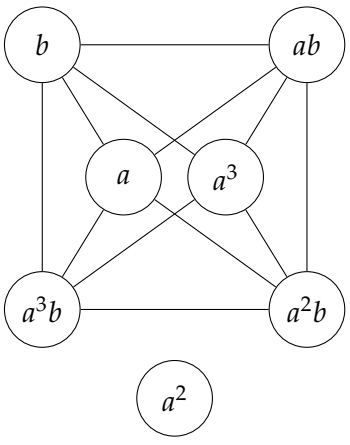
Conjecture B. *Let (G_i) be a sequence of nonabelian finite groups. Then*

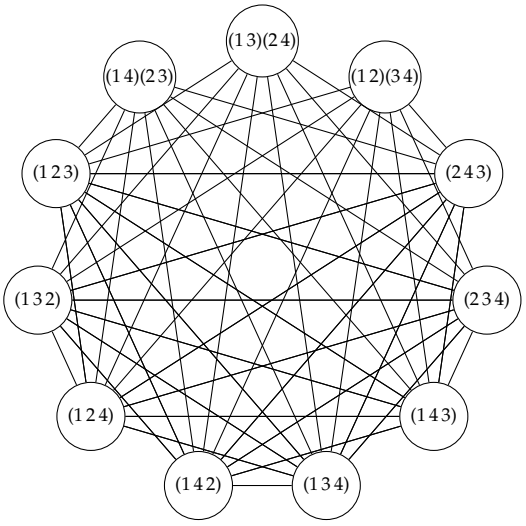
$$s(G_i) \to \infty \iff u(G_i) \to \infty.$$

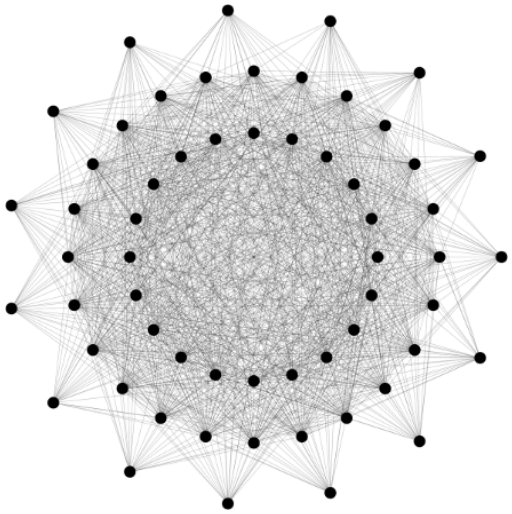
Recall that $s(S_6) = 2$ but $u(S_6) = 0$. As far as the author is aware, the only known family of nonabelian simple groups for which $s(G) - u(G)$ is unbounded is $G = \mathrm{PSL}_2(p)$ where p is a prime number satisfying $p \equiv 3 \pmod 4$ (see [21, Proposition 7.4]).

If Conjectures A and B could be reduced to the almost simple groups, then Theorems A and B would play an important role in proving them.

To conclude this introduction, let us highlight a combinatorial connection to this work. The *generating graph* of a group G is the graph $\Gamma(G)$ whose vertices are the nontrivial elements of G and where two vertices g and h are adjacent if $\langle g, h \rangle = G$. The generating graphs of the dihedral group D_8 and the alternating groups A_4 and A_5 are given below.







Evidently, $\Gamma(G)$ has no isolated vertices if and only if G is $\frac{3}{2}$-generated. Indeed, the dichotomy is demonstrated by $\Gamma(D_8)$ and $\Gamma(A_4)$, where we note that D_8 has a noncyclic quotient whereas A_4 does not. Further, if $s(G) \geqslant 2$, then $\Gamma(G)$ is connected with diameter at most 2. Therefore, by [10, Theorem 1.2], the diameter of the generating graph of any nonabelian finite simple group is two.

Many other natural questions about generating graphs have been investigated in recent years. For instance, if G is a sufficiently large simple group, then $\Gamma(G)$ is *Hamiltonian* (that is, has a cycle containing every vertex exactly once) [11]. Moreover, if $n \geqslant 120$, then the generating graphs $\Gamma(A_n)$ and $\Gamma(S_n)$ are Hamiltonian [28]. Indeed, it is conjectured that for all finite groups G of order at least four, the generating graph $\Gamma(G)$ is Hamiltonian if and only if every proper quotient of G is cyclic. This is a significant strengthening of the $\frac{3}{2}$-Generation Conjecture.

In a different direction, the *total domination number* of a graph Γ is the minimal size of a set S of vertices of Γ such that every vertex of Γ is adjacent to a vertex in S. In recent work of the author and Burness [20, 21], close to best possible bounds on the total domination number of generating graphs of simple groups were obtained, together with related probabilities. For instance, there are infinitely many finite simple groups G for which the total domination number of $\Gamma(G)$ is the minimal possible value of two (for example, A_p when $p \geqslant 13$ is prime, $\mathrm{PSL}_n(q)$ when $n > 3$ is odd, $E_8(q)$ and the Monster). This is a vast generalisation of the fact that these groups are $\frac{3}{2}$-generated.

For further reading on group generation, especially in the context of simple groups and probabilistic methods, see Burness' recent survey article [16]. The recent paper of Burness and the author [21] also features a detailed account of the spread of simple groups and related groups.

2

Preliminaries

In this chapter we introduce background material for the work in Chapters 3–5. All of the original work in this chapter can be found in Section 2.3, where we study semisimple elements, and Section 2.7 on Shintani descent; the remainder of the material in this chapter is well known, but we see benefit in collecting it together here.

Notational conventions

Let a, b, n be positive integers and let G, H be groups. Throughout this thesis we write

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

a_b for the greatest power of b dividing a

δ_{ab} for the Kronecker delta

$\log a$ for the *base two* logarithm of a

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

$G.H$ for an unspecified extension of G by H (with quotient H)

$G{:}H$ for an unspecified split extension of G by H

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

$G \circ H$ for the central product of G and H

$G \wr H$ for the wreath product $G^n{:}H$ where $H \leqslant S_n$ permutes the factors of G^n

Groups always act on the right. Accordingly, matrices act on the right of row vectors, x^g denotes $g^{-1}xg$ and G/H is the set of right cosets of H in G.

2.1 Probabilistic method

Probabilistic methods featuring fixed point ratios, introduced below, are a fruitful means of studying a vast range of problems. Indeed these methods led to the resolution of the Cameron–Kantor conjecture on base sizes of permutation groups [52] and the Guralnick–Thompson conjecture on monodromy groups [30]. The lecture notes [15] provide an excellent overview of this topic. In this section, we outline the probabilistic method for studying uniform spread introduced by Guralnick and Kantor [33].

Let G be a finite group acting on a finite set Ω. The *fixed point ratio* of $x \in G$ is

$$\mathrm{fpr}(x, \Omega) = \frac{\mathrm{fix}(x, \Omega)}{|\Omega|} \quad \text{where} \quad \mathrm{fix}(x, \Omega) = |\{\omega \in \Omega \mid \omega x = \omega\}|.$$

Evidently, $0 \leqslant \mathrm{fpr}(x, \Omega) \leqslant 1$ with the lower and upper bounds achieved if and only if x is derangement or x is in the kernel of the action, respectively. If $H \leqslant G$, then G acts transitively on the set G/H of right cosets of H in G and one sees that

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

We discuss recent work on fixed point ratios, particularly in the context of primitive actions of almost simple groups, at the opening of Chapter 3.

Let us now describe the probabilistic method for uniform spread. For $x, s \in G$, write

$$P(x, s) = \frac{|\{z \in s^G \mid \langle x, z \rangle \neq G\}|}{|s^G|} \tag{2.1}$$

the probability that x does not generate G with a (uniformly) randomly chosen conjugate of s. Moreover, let $\mathcal{M}(G, s)$ be the set of maximal subgroups of G that contain s. The following lemma encapsulates the method (see [18, Lemmas 2.1 and 2.2]).

Lemma 2.1.1. *Let G be a finite group and let $s \in G$.*

(i) *For $x \in G$,*

$$P(x, s) \leqslant \sum_{H \in \mathcal{M}(G,s)} \mathrm{fpr}(x, G/H).$$

(ii) *If for all k-tuples $(x_1, \ldots, x_k)$ of prime order elements of G*

$$\sum_{i=1}^{k} P(x_i, s) < 1,$$

then $u(G) \geqslant k$ with respect to the conjugacy class s^G.

Proof. For (i), let $x \in G$. Then $\langle x, s^g \rangle \neq G$ if and only if $x \in H^g$, or equivalently $x^{g^{-1}} \in H$, for some $H \in \mathcal{M}(G, s)$. Therefore,

$$P(x, s) = \frac{|\{z \in s^G \mid \langle x, z \rangle \neq G\}|}{|s^G|} \leqslant \sum_{H \in \mathcal{M}(G,s)} \frac{|x^G \cap H|}{|x^G|} = \sum_{H \in \mathcal{M}(G,s)} \mathrm{fpr}(x, G/H).$$

For (ii), fix k. To prove that $u(G) \geqslant k$ with respect to the class s^G, it suffices to prove that for all elements $x_1, \ldots, x_k \in G$ of *prime order* there exists $z \in s^G$ such that $\langle x_i, z\rangle = G$ for all $1 \leqslant i \leqslant k$. Therefore, let $x_1, \ldots, x_k \in G$ have prime order. If $\sum_{i=1}^k P(x_i, s) < 1$, then

$$1 - \frac{|\{z \in s^G \mid \langle x_i, z\rangle = G \text{ for all } 1 \leqslant i \leqslant k\}|}{|s^G|} \leqslant \sum_{i=1}^{k} P(x_i, s) < 1,$$

so there exists $z \in s^G$ such that $\langle x_i, z\rangle = G$ for all $1 \leqslant i \leqslant k$. This completes the proof. □

We present a basic example to highlight how we apply Lemma 2.1.1.

Example 2.1.2. Let $G = A_5$. We will prove that $u(G) \geqslant 2$.

Step 1: Select a particular element

We must first fix $s \in G$. In light of the steps that follow, we should choose an element s that is contained in few and small maximal subgroups of G. We will select $s = (1\,2\,3\,4\,5)$.

Step 2: Study the element's maximal overgroups

There are three conjugacy classes of maximal subgroups of G, which are isomorphic to A_4, S_3 and D_{10}. Write $H = N_G(\langle s\rangle) \cong D_{10}$. Evidently, any subgroup containing s is conjugate to H, and one quickly sees that, in fact, $\mathcal{M}(G, s) = \{H\}$.

Step 3: Bound a probability using fixed point ratios

Let $x \in G$ have prime order r. By Lemma 2.1.1(i),

$$P(x, s) \leqslant \mathrm{fpr}(x, G/H) = \frac{|x^G \cap H|}{|x^G|}.$$

If $r = 3$, then $P(x, s) = |x^G \cap H| = 0$, since H contains no elements of order 3. Next, if $r = 2$, then $|x^G| = 15$ and $|x^G \cap H| = 5$, since all involutions in G are conjugate, so $P(x, s) = \frac{1}{3}$. Finally, if $r = 5$, then we check that $|x^G| = 12$ and $|x^G \cap H| = 2$, so $P(x, s) = \frac{1}{6}$. Therefore, in all cases, $P(x, s) < \frac{1}{2}$, so Lemma 2.1.1(ii) gives $u(G) \geqslant 2$.

In fact, $s(G) = u(G) = 2$ since there is no element $g \in G$ such that

$$\langle (1\,2)(3\,4), g\rangle = \langle (1\,2)(4\,5), g\rangle = \langle (1\,2)(3\,5), g\rangle = G.$$

The above example, demonstrates that our approach demands control over three factors, which could be crudely summarised as: well-chosen elements, maximal subgroups and fixed point ratios. For this reason, much of Chapters 2 and 3 focus on these three topics. The example also demonstrates the power of the probabilistic method: in this case it gave the exact value of the uniform spread (indeed spread).

We conclude this section with a straightforward application of fixed point ratios.

Lemma 2.1.3. *Let G be a finite group, let $H \leqslant G$ and let $x \in G$. Then the number of G-conjugates of H that contain x is* $\mathrm{fpr}(x, G/H) \cdot |G : N_G(H)|$.

2.2 Classical groups

In this section, we fix our notation for symplectic and orthogonal groups and record some basic facts. A full account can be found in [43, Chapter 2]. Throughout this section, V is an n-dimensional vector space over a field F of characteristic $p > 0$. (From Section 2.2.2 onwards we will assume that F is either finite or algebraically closed.)

2.2.1 Symplectic and orthogonal groups

We write $\Gamma\mathrm{L}(V)$, $\mathrm{GL}(V)$, $\mathrm{SL}(V)$ for the groups of invertible transformations of V that are semilinear, linear and linear with determinant one, respectively. We also write $\Gamma\mathrm{L}_n(F)$, $\mathrm{GL}_n(F)$, $\mathrm{SL}_n(F)$ for these groups. If $F = \mathbb{F}_q$, then we write $\mathrm{GL}_n(q)$ rather than $\mathrm{GL}_n(\mathbb{F}_q)$, and similarly for all of the other classical groups.

Let $Z(V) \leqslant \mathrm{GL}(V) \leqslant \Gamma\mathrm{L}(V)$ be the group of scalar transformations, which is the centre of $\mathrm{GL}(V)$ and is normal in $\Gamma\mathrm{L}(V)$. This gives *projective groups* $\mathrm{PGL}(V) = \mathrm{GL}(V)/Z(V)$ and $\mathrm{P\Gamma L}(V) = \Gamma\mathrm{L}(V)/Z(V)$. In general, for a classical group $G \leqslant \Gamma\mathrm{L}(V)$, we write $\mathrm{P}G = GZ(V)/Z(V) \cong G/(G \cap Z(V))$. In particular, $\mathrm{PSL}(V) \cong \mathrm{SL}(V)/Z(\mathrm{SL}(V))$.

Let κ be a bilinear form $(\cdot,\cdot)$ (or quadratic form Q) on V. A map $g \in \Gamma\mathrm{L}(V)$ is

(i) an *isometry* of κ if for all $u, v \in V$ we have $(ug, vg) = (u, v)$ (or $Q(vg) = Q(v)$)

(ii) a *similarity* of κ if there exists $\tau(g) \in F^\times$ such that for all $u, v \in V$ we have $(ug, vg) = \tau(g)(u, v)$ (or $Q(vg) = \tau(g)Q(v)$)

(iii) a *semisimilarity* of κ if there exists $\tau(g) \in F^\times$ and $\alpha(g) \in \mathrm{Aut}(F)$ such that for all $u, v \in V$ we have $(ug, vg) = \tau(g)(u, v)^{\alpha(g)}$ (or $Q(vg) = \tau(g)Q(v)^{\alpha(g)}$).

The sets of isometries, similarities and semisimilarities of such a form are groups under composition. If $(\cdot,\cdot)$ is the bilinear form defined as $(u, v) = 0$ for all $u, v \in V$, then $\mathrm{GL}(V)$ is the isometry and similarity group of $(\cdot,\cdot)$ on V and $\Gamma\mathrm{L}(V)$ is the semisimiliarity group.

Let $\kappa = (\cdot,\cdot)$ be a bilinear form on V. Recall that κ is *nondegenerate* if

$$\mathrm{rad}(\kappa) = \{u \in V \mid (u, v) = 0 \text{ for all } v \in V\} = 0. \tag{2.2}$$

If $n = 2m$ and $(\cdot,\cdot)$ is a *symplectic form* (that is, a nondegenerate alternating bilinear form), then we write $\mathrm{Sp}(V)$, $\mathrm{GSp}(V)$ and $\Gamma\mathrm{Sp}(V)$ for the groups of isometries, similarities and semisimilarities of $(\cdot,\cdot)$ on V.

Next let Q be a quadratic form on V, with associated bilinear form $(\cdot,\cdot)_Q$ defined as

$$(u, v)_Q = Q(u + v) - Q(u) - Q(v).$$

The *norm* of a vector $v \in V$ is $(v, v)_Q$. Note that $(v, v)_Q = 2Q(v)$, so Q is determined by $(\cdot,\cdot)_Q$ if p is odd, but $(\cdot,\cdot)_Q$ is alternating (and does not determine Q) if $p = 2$. Now Q is *nondegenerate* if $(\cdot,\cdot)_Q$ is nondegenerate, and Q is *nonsingular* if

$$\mathrm{rad}(Q) = \{u \in V \mid Q(u) = 0 \text{ and } (u, v)_Q = 0 \text{ for all } v \in V\} = 0. \tag{2.3}$$

If Q is a nonsingular quadratic form on V, then we write $\mathrm{O}(V)$, $\mathrm{GO}(V)$ and $\Gamma\mathrm{O}(V)$ for the groups of isometries, similarities and semisimilarities of Q on V, and we write

$$\mathrm{SO}(V) = \{g \in \mathrm{O}(V) \mid \det(g) = 1\}.$$

Note that $\mathrm{SO}(V) = \mathrm{O}(V)$ if $p = 2$ and $|\mathrm{O}(V) : \mathrm{SO}(V)| = 2$ if p is odd.

If $\kappa = (\cdot, \cdot)$ is a bilinear form on V and $\mathcal{B} = (u_1, \ldots, u_n)$ is a basis for V, then the $n \times n$ matrix $M = (m_{ij})$ defined as $m_{ij} = (u_i, u_j)$ is the *matrix of κ with respect to $\mathcal{B}$*. If $g \in \mathrm{GL}(V)$ is a similarity of κ, then $gMg^{\mathsf{T}} = \tau(g)M$, where A^{T} is the transpose of a matrix A.

Remark 2.2.1. The notation introduced in this section is consistent with [2, 10, 17, 31, 43], sources to which we often refer. However, this notation is not universal. In particular, CSp, CO and GO often refer to the groups denoted here as GSp, GO and O, respectively (where C stands for *conformal*). This alternative is adopted in MAGMA [5], extends the $\mathbb{ATLAS}$ notation of writing GO for O [24, 63] and is closer to the notation of [7].

2.2.2 Forms and bases

From now on in Section 2.2, we assume that F is a finite field $\mathbb{F}_q$, where $q = p^f$, or is an algebraically closed field (of characteristic $p > 0$).

First consider symplectic forms. If n is odd, then V does not admit a symplectic form. Therefore, we assume that $n = 2m$. Up to isometry, there is a unique symplectic form on V, so we may write $\mathrm{Sp}_{2m}(F)$ for $\mathrm{Sp}(V)$ and $\mathrm{GSp}_{2m}(F)$ for $\mathrm{GSp}(V)$. Fix the standard basis

$$\mathcal{B} = (e_1, f_1, \ldots, e_m, f_m)$$

for V and define the bilinear form $(\cdot, \cdot)$ as

$$(e_i, e_j) = (f_i, f_j) = 0, \quad (e_i, f_j) = \delta_{ij}. \tag{2.4}$$

We now turn to quadratic forms. The *Witt index* of a quadratic form on V is the dimension of a maximal totally singular subspace of V with respect to the form.

First assume that n is even and write $n = 2m$. Any nondegenerate quadratic form on V has Witt index m or $m - 1$, and two nondegenerate quadratic forms are isometric if and only if they have the same Witt index. Those with Witt index m are said to be *plus-type* and Witt index $m - 1$ are *minus-type*. If F is algebraically closed, then all nondegenerate quadratic forms are plus-type, but both isometry classes are realised when F is finite. For $\varepsilon \in \{+, -\}$, we write $\mathrm{sgn}(Q) = \varepsilon$ when Q is ε-type.

With respect to the basis

$$\mathcal{B}^+ = (e_1, f_1, \ldots, e_m, f_m)$$

define the quadratic form Q^+, with associated bilinear form $(\cdot, \cdot) = (\cdot, \cdot)_{Q^+}$, as

$$Q^+(e_i) = Q^+(f_i) = 0, \quad (e_i, f_j) = \delta_{ij}. \tag{2.5}$$

Now assume that $F = \mathbb{F}_q$. Deviating from [43] and following [31], fix a basis

$$\mathcal{B}^- = (e_1, f_1, \dots, e_{m-1}, f_{m-1}, u_m, v_m)$$

and define Q^- and $(\cdot,\cdot) = (\cdot,\cdot)_{Q^-}$ as

$$\begin{gathered} Q^-(e_i) = Q^-(f_i) = (e_i, u_m) = (f_i, u_m) = (e_i, v_m) = (f_i, v_m) = 0, \\ (e_i, f_j) = \delta_{ij}, \quad Q^-(u_m) = Q^-(v_m) = 1, \quad (u_m, v_m) = \xi^2 + \xi^{-2} \end{gathered} \tag{2.6}$$

where $\xi \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ satisfies $\xi^{q+1} = 1$.

As the notation suggests, $\operatorname{sgn}(Q^\varepsilon) = \varepsilon$, and we write $\mathrm{O}^\varepsilon_{2m}(F)$ for $\mathrm{O}(V)$ when V is equipped with the ε-type form Q^ε. When F is algebraically closed, we will usually omit the $+$ sign.

Now assume that n is odd and write $n = 2m + 1$. Fix a basis

$$\mathcal{B} = (e_1, f_1, \dots, e_m, f_m, x)$$

and define Q and $(\cdot,\cdot) = (\cdot,\cdot)_Q$ as

$$Q(e_i) = Q(f_i) = 0, \quad Q(x) = 1, \quad (e_i, f_j) = \delta_{ij}, \quad (e_i, x) = (f_i, x) = 0. \tag{2.7}$$

For now assume that p is odd. Then Q is the unique nondegenerate quadratic form on V up to similarity, and since similar forms have isomorphic isometry groups, we can write $\mathrm{O}_{2m+1}(F)$ for $\mathrm{O}(V)$. (If F is finite, then are exactly two isometry classes of nondegenerate quadratic forms, see Remark 2.2.2.) It is sometimes convenient to write $\operatorname{sgn}(Q) = \circ$ and $\mathrm{O}^\circ_{2m+1}(F) = \mathrm{O}_{2m+1}(F)$ in this case.

Now assume that $p = 2$. In this case, all quadratic forms on V are degenerate. The form Q from (2.7) is the unique nonsingular (degenerate) quadratic form on V, up to similarity, and we write $\mathrm{O}_{2m+1}(F)$ for $\mathrm{O}(V)$. (Notice that $\langle x \rangle$ is the radical of $(\cdot,\cdot)$, see (2.2)). We rarely consider this group since $\mathrm{O}_{2m+1}(F) \cong \mathrm{Sp}_{2m}(F)$ (see [63, Section 3.4.7] and Lemma 2.6.2). Unless we specify otherwise, for $\mathrm{O}_{2m+1}(F)$ we assume that p is odd.

Remark 2.2.2. Assume that $F = \mathbb{F}_q$ where q is odd. Write $(\mathbb{F}_q^\times)^2$ for the index two subgroup of squares in $\mathbb{F}_q^\times$ and write $\mathbb{F}_q^\times / (\mathbb{F}_q^\times)^2 = \{\square, \boxtimes\}$, where $\square$ denotes $(\mathbb{F}_q^\times)^2$.

Let Q be a nondegenerate quadratic form on $V = \mathbb{F}_q^n$ and let $(\cdot,\cdot)$ be the associated bilinear form. Fix a basis $(u_1, \dots, u_n)$ for V and let $M = ((u_i, u_j))$ be the matrix of $(\cdot,\cdot)$. The *discriminant* of Q is the element of $\mathbb{F}_q^\times / (\mathbb{F}_q^\times)^2$ defined as

$$D(Q) = \det(M) \pmod{(\mathbb{F}_q^\times)^2}. \tag{2.8}$$

The discriminant $D(Q)$ is independent of the basis [43, pp.31–32] and determines the isometry type of Q [43, Propositions 2.5.4 and 2.5.10]. In particular, if $n = 2m$, then

$$D(Q) = \square \iff q^m \equiv \operatorname{sgn}(Q) \pmod 4, \tag{2.9}$$

where we interpret $\operatorname{sgn}(Q)$ as the integer 1 or -1.

Table 2.1: Finite simple classical groups

	$\mathrm{PSL}_n(q)$	$\mathrm{PSU}_n(q)$	$\mathrm{PSp}_n(q)$	$\mathrm{P}\Omega^\epsilon_n(q)$
lower bound on n	2	3	4	7
excluded (n,q)	$(2,2)$, $(2,3)$	$(3,2)$	$(4,2)$	

By a *finite simple classical group* we mean one of the groups in Table 2.1. These groups are simple and each excluded group is either not simple or coincides with another simple group [43, Theorem 2.1.3 and Proposition 2.9.1].

Remark 2.2.3. We make passing references to unitary groups, a thorough treatment of which is in [43, Section 2.3]. We adopt the convention that $\mathrm{GU}_n(q)$ and $\mathrm{CU}_n(q)$ are the isometry and similarity groups of a nondegenerate conjugate-symmetric sesquilinear form on $\mathbb{F}_{q^2}^n$ with respect to the field automorphism $\lambda \mapsto \lambda^q$. Therefore, $\mathrm{GU}_n(q)$ is naturally a subgroup of $\mathrm{GL}_n(q^2)$ (not $\mathrm{GL}_n(q)$). Write $\mathrm{SU}_n(q) = \mathrm{GU}_n(q) \cap \mathrm{SL}_n(q^2)$ and, by analogy with orthogonal groups, $\mathrm{GL}^+ = \mathrm{GL}$ and $\mathrm{GL}^- = \mathrm{GU}$.

Remark 2.2.4. Although we use notation such as $\mathrm{Sp}_{2m}(q)$ and $\mathrm{GO}^-_{2m}(q)$, the elements of these groups are linear maps on a fixed vector space V which preserve a fixed quadratic or bilinear form; the elements are not matrices. Indeed, we will use a number of different bases to specify elements in these groups.

2.2.3 Similarities

Continue to assume that F is finite or algebraically closed and has characteristic p. We use this section to record some properties of similarities in symplectic and orthogonal groups. We begin with a technical result on the similarity map τ.

Lemma 2.2.5. *Let G be $\mathrm{GSp}(V)$ or $\mathrm{GO}(V)$. For $g, h \in G$,*

(i) $\tau(gh) = \tau(g)\tau(h)$

(ii) *if $gZ(G) = hZ(G)$, then $\tau(g)\tau(h)^{-1} \in (F^\times)^2$.*

Proof. We will prove the result for $G = \mathrm{GO}(V)$ since the proof is very similar when $G = \mathrm{GSp}(V)$. Let Q be the quadratic form defining $\mathrm{GO}(V)$. Let $v \in V$. Then

$$Q(v(gh)) = Q((vg)h) = \tau(h)Q(vg) = \tau(g)\tau(h)Q(v),$$

so $\tau(gh) = \tau(g)\tau(h)$, which proves (i). Turning to (ii), assume that $gZ(G) = hZ(G)$. Then $g = \lambda h$ for some $\lambda \in F^\times$. Consequently, using part (i),

$$\tau(g)\tau(h)^{-1} = \tau(\lambda I_n)\tau(h)\tau(h)^{-1} = \tau(\lambda I_n) = \lambda^2 \in (F^\times)^2,$$

where $\tau(\lambda I_n) = \lambda^2$ since $Q(v\lambda I_n) = Q(\lambda v) = \lambda^2 Q(v)$. This completes the proof. □

For an element g of $\mathrm{PGSp}(V)$ or $\mathrm{PGO}(V)$, Lemma 2.2.5 justifies us considering $\tau(g)$ as an element of $(F^\times)/(F^\times)^2$. If F is algebraically closed or is a finite field of even characteristic, then $(F^\times)^2 = F^\times$. If F is a finite field of odd characteristic, then we will write $(F^\times)/(F^\times)^2 = \{\square, \boxtimes\}$.

Lemma 2.2.6. *Let (C, G) be $(\mathrm{GSp}(V), \mathrm{Sp}(V))$ or $(\mathrm{GO}(V), \mathrm{O}(V))$, let $Z = Z(\mathrm{GL}(V))$ and let $g \in C$. Then $gZ \in \mathrm{P}G$ if and only if $\tau(g) \in (F^\times)^2$.*

Proof. If $\tau(g) \in \lambda^2$ for some $\lambda \in F^\times$, then, by Lemma 2.2.5, $\tau(\lambda^{-1}g) = \lambda^{-2}\lambda^2 = 1$, so $\lambda^{-1}g \in G$ and $gZ = \lambda^{-1}gZ \in \mathrm{P}G$. Conversely, if $gZ \in \mathrm{P}G$, then $\lambda g \in G$, for some $\lambda \in F^\times$, so $\tau(g) = \lambda^{-2}\tau(\lambda g) = \lambda^{-2} \in (F^\times)^2$, which completes the proof. □

We conclude with a property of similarities.

Lemma 2.2.7. *Let G be $\mathrm{GSp}(V)$ or $\mathrm{GO}(V)$ and let $g \in G$. Then g and $\tau(g)g^{-1}$ are similar. In particular, if $\tau(g) = 1$, then g and g^{-1} are similar.*

Proof. We will prove the result for $G = \mathrm{GO}(V)$ since the proof is similar and easier when $G = \mathrm{GSp}(V)$. Let Q be the quadratic form defining $\mathrm{GO}(V)$ and let $(\cdot,\cdot)$ be the bilinear form associated to Q. Fix a basis $(u_1, \ldots, u_n)$ for V and let $M = (m_{ij})$ be the $n \times n$ matrix where $m_{ij} = (u_i, u_j)$. Let $g \in \mathrm{GO}(V)$. Since g is a similarity of Q, for all $u, v \in V$,

$$(ug, vg) = Q(ug+vg) - Q(ug) - Q(vg) = \tau(g)(Q(u+v) - Q(u) - Q(v)) = \tau(g)(u, v).$$

Therefore, $gMg^{\mathsf{T}} = \tau(g)M$, so $g^M = \tau(g)g^{-\mathsf{T}}$. Consequently, g is similar to $\tau(g)g^{-\mathsf{T}}$, which is evidently similar to $\tau(g)g^{-1}$. This completes the proof. □

2.2.4 Reflections

We will now introduce a particularly important class of elements in orthogonal groups. Recall that F is finite or algebraically closed and has characteristic p. Let $V = F^n$ be equipped with a nondegenerate quadratic form Q with bilinear form $(\cdot,\cdot)$.

Let $v \in V$ be nonsingular. The *reflection* in v is the map $r_v \colon V \to V$ defined for $u \in V$ as

$$ur_v = u - \frac{(u, v)}{Q(v)}v.$$

If p is odd, then reflections are always isometries. If $p = 2$, then $r_v \in \mathrm{O}(V)$ if and only if $Q(v) = 1$, in which case we may write

$$ur_v = u + (u, v)v,$$

and r_v is referred to as a *transvection*. For uniformity, following [43], we still refer to r_v as a reflection (rather than transvection) in characteristic two.

The following result is proved in [2, 22.7].

Theorem 2.2.8. *Let $G = \mathrm{O}(V)$. Then G is generated by reflections unless $G = \mathrm{O}_4^+(2)$.*

The group $\mathrm{O}_4^+(2)$ is a genuine exception and we refer the reader to [43, Proposition 2.5.9].

2.2.5 The group $\Omega(V)$

In this section, we restrict F slightly further: we will assume that F is an algebraically closed field of characteristic $p = 2$ or a finite field (of any characteristic $p > 0$). Let $V = F^n$ be equipped with a nondegenerate quadratic form Q with bilinear form $(\cdot, \cdot)$. The aim of this section is to define an important index two subgroup $\Omega(V)$ of $\mathrm{SO}(V)$. In light of Theorem 2.2.8, we assume that $(n, F, \mathrm{sgn}(Q)) \neq (4, \mathbb{F}_2, +)$ (see [43, Proposition 2.5.9] for the definition of $\Omega_4^+(2)$).

First assume that $p = 2$. By Theorem 2.2.8, every element of $\mathrm{SO}(V) = \mathrm{O}(V)$ is a product of reflections. We define $\Omega(V)$ to be the group of all elements that are a product of an even number of reflections (which is well-defined, see [2, 22.8 and 22.9]).

Remark 2.2.9. When F is an algebraically closed field of characteristic two, our definitions of $\Omega(V)$ and $\mathrm{SO}(V)$, which are the conventions of [31], are not widespread and often $\mathrm{SO}(V)$ is used to refer to the group we call $\Omega(V)$ (for example, in [53]). However, the author chose this notation since it accords more strongly with the notation for finite groups and he imagines that many readers would simply, and reasonably, assume that $\mathrm{SO}(V) = \mathrm{O}(V) \cap \mathrm{SL}(V)$.

Now assume that p is odd. Therefore, under our assumption of this section, F is finite. Write $F = \mathbb{F}_q$ where $q = p^f$. In this case, reflections have determinant -1, so the subgroup of $\mathrm{O}(V)$ containing the elements that are a product of an even number of reflections is simply $\mathrm{SO}(V)$. Therefore, we need to define $\Omega(V)$ differently in this case.

The *spinor norm* is the map $\mathrm{sp}\colon \mathrm{SO}(V) \to \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2$ defined as follows. For $g \in \mathrm{SO}(V)$, write $g = r_{v_1} \cdots r_{v_k}$ and let

$$\mathrm{sp}(g) = \prod_{i=1}^{k} (v_i, v_i) \pmod{(\mathbb{F}_q^\times)^2}. \tag{2.10}$$

By [2, 22.10], sp is well-defined, and we define $\Omega(V) = \ker(\mathrm{sp})$.

2.2.6 The group $\mathrm{DO}(V)$

We return to our usual assumption that F is finite or algebraically closed and has characteristic p. Let $n = 2m$ and equip $V = F^{2m}$ with a nondegenerate quadratic form Q. In this section, we coin a useful piece of notation for a particular subgroup of $\mathrm{GO}(V)$.

First assume that p is odd. If $g \in \mathrm{GO}(V)$, then Lemma 2.2.7 implies that g is similar to $\tau(g)g^{-1}$, so $\det(g) = \pm\tau(g)^m$. This motivates the following definition:

$$\mathrm{DO}(V) = \{g \in \mathrm{GO}(V) \mid \det(g) = \tau(g)^m\}. \tag{2.11}$$

Informally, $\mathrm{DO}(V)$ is to $\mathrm{GO}(V)$ as $\mathrm{SO}(V)$ is to $\mathrm{O}(V)$. Indeed, $\mathrm{DO}(V) \cap \mathrm{O}(V) = \mathrm{SO}(V)$.

If $p = 2$, then we simply define

$$\mathrm{DO}(V) = \Omega(V). \tag{2.12}$$

2.2.7 Automorphisms

In this section, we write $q = p^f$ and we will describe $\mathrm{Aut}(\mathrm{PSp}_n(q))$ and $\mathrm{Aut}(\mathrm{P}\Omega^\varepsilon_n(q))$ in terms of classical groups introduced throughout Section 2.2. If T is any finite simple group, then $\mathrm{Out}(T) = \mathrm{Aut}(T)/T$ is a known soluble group, where we identify T with $\mathrm{Inn}(T)$ (which we always do). We discuss automorphisms again, from the perspective of algebraic groups, in Section 2.6.6, and we provide much more detail on automorphisms in Sections 4.1 and 5.1. The results of this section are given in [43, Section 2.1].

By $H \leqslant_k G$ we mean that H is an index k subgroup of G.

Symplectic groups

Let $n \geqslant 4$ be even. Since $\mathrm{Sp}_4(2) \cong S_6$, assume that $(n, q) \neq (4, 2)$. For $d = (p-1, 2)$,

$$Z(\mathrm{Sp}_n(q)) = \langle -I_n \rangle \cong C_d.$$

In addition, we have the chain of subgroups

$$\mathrm{PSp}_n(q) \leqslant_d \mathrm{PGSp}_n(q) \leqslant_f \mathrm{P\Gamma Sp}_n(q) \leqslant_{\gamma_1} \mathrm{Aut}(\mathrm{PSp}_n(q))$$

where $\gamma_1 = 1$ unless $(n, p) = (4, 2)$ when $\gamma_1 = 2$. The group $\mathrm{Sp}_4(2^f)$ has an exceptional *graph-field automorphism*, which accounts for $\gamma_1 > 1$ (see (4.5) in Section 4.1.2).

Odd-dimensional orthogonal groups

Let $n \geqslant 7$ be odd and let p be odd. Then $Z(\Omega_n(q)) = 1$ and

$$\Omega_n(q) \leqslant_2 \mathrm{SO}_n(q) = \mathrm{PSO}_n(q) = \mathrm{PO}_n(q) = \mathrm{PGO}_n(q) \leqslant_f \mathrm{P\Gamma O}_n(q) = \mathrm{Aut}(\Omega_n(q)).$$

Even-dimensional orthogonal groups

Let $n \geqslant 8$ be even and let $\varepsilon \in \{+, -\}$. Let $\gamma_2 = 1$ unless $(n, \varepsilon) = (8, +)$ when $\gamma_2 = 3$. If $p = 2$, then $Z(\Omega^\varepsilon_n(q)) = 1$ and

$$\Omega^\varepsilon_n(q) \leqslant_2 \mathrm{SO}^\varepsilon_n(q) = \mathrm{O}^\varepsilon_n(q) = \mathrm{PO}^\varepsilon_n(q) = \mathrm{PGO}^\varepsilon_n(q) \leqslant_f \mathrm{P\Gamma O}^\varepsilon_n(q) \leqslant_{\gamma_2} \mathrm{Aut}(\Omega^\varepsilon_n(q)).$$

Now assume that p is odd. In this case, $Z(\mathrm{SO}^\varepsilon_n(q)) = \langle -I_n \rangle \cong C_2$. For $c = \frac{1}{2}(q^m - \varepsilon, 4)$,

$$Z(\Omega^\varepsilon_n(q)) \cong C_c,$$

see [43, Proposition 2.5.13], and

$$\mathrm{P}\Omega^\varepsilon_n(q) \leqslant_c \mathrm{PSO}^\varepsilon_n(q) \leqslant_2 \left\{ \begin{array}{c} \mathrm{PO}^\varepsilon_n(q) \\ \mathrm{PDO}^\varepsilon_n(q) \end{array} \right\} \leqslant_2 \mathrm{PGO}^\varepsilon_n(q) \leqslant_f \mathrm{P\Gamma O}^\varepsilon_n(q) \leqslant_{\gamma_2} \mathrm{Aut}(\mathrm{P}\Omega^\varepsilon_n(q)).$$

The group $\mathrm{P}\Omega^+_8(q)$ has an exceptional *triality graph automorphism*, which accounts for $\gamma_2 > 1$, and we discuss this group in Remark 5.1.15.

2.3 Semisimple elements in classical groups

We use Sections 2.3.1–2.3.4 to record a variety of useful information about classical groups and their actions on vector spaces. In Section 2.3.5, we apply this information to studying semisimple elements. Section 2.3.6 is more specialised and here we define certain *types* of elements, which play an important role in Chapters 4 and 5.

2.3.1 Subspaces and decompositions

In this section, $V = F^n$ where $n \geqslant 1$ and F is a field.

Let $\mathcal{D}$ be a *direct sum decomposition* $V = V_1 \oplus \cdots \oplus V_k$ or a *tensor product decomposition* $V = V_1 \otimes \cdots \otimes V_k$, where $\dim V_i > 1$ in the latter case. We say that $\mathcal{D}$ is *nontrivial* if $k > 1$. We will routinely identify $\mathcal{D}$ with the set $\{V_1, \ldots, V_k\}$, so, for $G \leqslant \mathrm{GL}(V)$, we write

(i) $G_{\mathcal{D}} = G_{\{\mathcal{D}\}}$ for the setwise stabiliser of $\mathcal{D}$ in G, which we call the *stabiliser* of $\mathcal{D}$

(ii) $G_{(\mathcal{D})}$ for the pointwise stabiliser of $\mathcal{D}$ in G, which we call the *centraliser* of $\mathcal{D}$.

If V is equipped with a form, then $V = V_1 \perp \cdots \perp V_k$ refers to a direct sum decomposition where $V_1, \ldots, V_k$ are pairwise orthogonal nondegenerate subspaces.

An element or subgroup of $\mathrm{GL}(V)$ or $\mathrm{PGL}(V)$ is *reducible* if it stabilises a proper nonzero subspace of V and *irreducible* otherwise. Moreover, an irreducible subgroup is *imprimitive* if it stabilises a nontrivial direct sum decomposition of V and *primitive* otherwise.

If an element $g \in \mathrm{GL}(V)$ centralises the decomposition $\mathcal{D}$ and acts as g_i on V_i, then we write g as $g_1 \oplus \cdots \oplus g_k$, or $g_1 \perp \cdots \perp g_k$, or $g_1 \otimes \cdots \otimes g_k$, according to the type of decomposition. This representation of g is unique if $\mathcal{D}$ is a direct sum decomposition. If $\mathcal{D}$ is a tensor product decomposition and $g_1 \otimes \cdots \otimes g_k = h_1 \otimes \cdots \otimes h_k$, then there exist $\lambda_1, \ldots, \lambda_k \in F^\times$ satisfying $\lambda_1 \cdots \lambda_k = 1$ and $h_i = \lambda_i g_i$.

We now present some representation theoretic results on direct sums. The following is entirely analogous to Goursat's Lemma from group theory (see [44, p.75] for example).

Lemma 2.3.1 (Goursat's Lemma)**.** *Let $G \leqslant \mathrm{GL}(V)$ centralise $V = V_1 \oplus V_2$. Let U be an FG-submodule of V. Then there exist FG-submodules $W_1 \leqslant U_1 \leqslant V_1$ and $W_2 \leqslant U_2 \leqslant V_2$ and an FG-isomorphism $\varphi\colon U_1/W_1 \to U_2/W_2$ such that*

$$U = \{(u_1, u_2) \in U_1 \oplus U_2 \mid \varphi(W_1 + u_1) = W_2 + u_2\}.$$

Proof. Let $\pi_i\colon U \to V_i$ be the projection map $(u_1, u_2) \mapsto u_i$ and let $U_i = \pi_i(U)$. Write $W_1 = \{u_1 \in U_1 \mid (u_1, 0) \in U\} \cong \ker \pi_2$ and $W_2 = \{u_2 \in U_2 \mid (0, u_2) \in U\} \cong \ker \pi_1$.

Let $u_1 \in U_1$. Since $U_1 = \pi_1(U)$, there exists $u_2 \in U_2$ such that $(u_1, u_2) \in U$. Now let $u_2, v_2 \in U_2$ satisfy $(u_1, u_2), (u_1, v_2) \in U$. Then $(0, u_2 - v_2) = (u_1, u_2) - (u_1, v_2) \in U$, so $u_2 - v_2 \in W_2$ and hence $W_2 + u_2 = W_2 + v_2$. Therefore, the map $\psi\colon U_1 \to U_2/W_2$ defined as $\psi(u_1) = \{u_2 \in U_2 \mid (u_1, u_2) \in U\}$ is well-defined.

Now ψ is surjective since $U_2 = \pi_2(U)$. It is straightforward to check that ψ is a FG-homomorphism. The definition of W_1 makes it clear that W_1 is the kernel of ψ. Therefore, $\varphi\colon U_1/W_1 \to U_2/W_2$ defined as $\varphi(W_1 + u_1) = \psi(u_1)$ is a well-defined FG-isomorphism. By construction,

$$U = \{(u_1, u_2) \in U_1 \oplus U_2 \mid \varphi(W_1 + u_1) = W_2 + u_2\},$$

as required. □

Corollary 2.3.2. *Let $G \leqslant \mathrm{GL}(V)$ centralise $V = V_1 \oplus V_2$. Assume that there are no nonzero FG-isomorphisms between FG-subquotients of V_1 and V_2. Let U be a FG-submodule of V. Then there exist FG-submodules $U_1 \leqslant V_1$ and $U_2 \leqslant V_2$ such that $U = U_1 \oplus U_2$.*

Proof. By Lemma 2.3.1, there exist FG-submodules $W_1 \leqslant U_1 \leqslant V_1$ and $W_2 \leqslant U_2 \leqslant V_2$ and an FG-isomorphism $\varphi\colon U_1/W_1 \to U_2/W_2$ such that

$$U = \{(u_1, u_2) \in U_1 \oplus U_2 \mid \varphi(W_1 + u_1) = W_2 + u_2\}.$$

By assumption, we must have $W_1 = U_1$ and $W_2 = U_2$. Therefore, $\varphi(W_1 + u_1) = W_2 + u_2$ for all $(u_1, u_2) \in U_1 \oplus U_2$, so we conclude that $U = U_1 \oplus U_2$. □

The following lemma, which is proved directly in [43, Lemma 2.10.11], is an immediate consequence of Corollary 2.3.2.

Lemma 2.3.3. *Let $G \leqslant \mathrm{GL}(V)$ centralise $V = V_1 \oplus \cdots \oplus V_k$. If $V_1, \ldots, V_k$ are pairwise nonisomorphic irreducible FG-modules, then they are the only irreducible FG-submodules of V.*

We use the next lemma to compute centralisers of elements in classical groups.

Lemma 2.3.4. *Let $g = g_1 \oplus \cdots \oplus g_k \in \mathrm{GL}(V)$ centralise $V = V_1 \oplus \cdots \oplus V_k$. Assume that there are no nonzero $F\langle g\rangle$-homomorphisms between V_i and V_j when $i \neq j$. Then*

$$C_{\mathrm{GL}(V)}(g) = C_{\mathrm{GL}(V_1)}(g_1) \times \cdots \times C_{\mathrm{GL}(V_k)}(g_k).$$

Proof. The $F\langle g\rangle$-endomorphism ring of V is

$$\mathrm{End}_{F\langle g\rangle}(V) = \{(\varphi_{ij}) \mid \varphi_{ij} \in \mathrm{Hom}_{F\langle g\rangle}(V_i, V_j)\}$$

under formal matrix operations. Since $\mathrm{Hom}_{F\langle g\rangle}(V_i, V_j) = 0$ if $i \neq j$,

$$\mathrm{End}_{F\langle g\rangle}(V) = \mathrm{End}_{F\langle g_1\rangle}(V_1) \oplus \cdots \oplus \mathrm{End}_{F\langle g_k\rangle}(V_k).$$

Considering the bijections in $\mathrm{End}_{F\langle g\rangle}(V)$ and forgetting the additive structure, we obtain

$$C_{\mathrm{GL}(V)}(V) = C_{\mathrm{GL}(V_1)}(\langle g_1\rangle) \times \cdots \times C_{\mathrm{GL}(V_k)}(\langle g_k\rangle),$$

as desired. □

We obtain the following immediate consequence of Lemma 2.3.4.

Corollary 2.3.5. *Let $g = g_1 \oplus \cdots \oplus g_k \in \mathrm{GL}(V)$ centralise $V = V_1 \oplus \cdots \oplus V_k$. Assume that $V_1, \ldots, V_k$ are pairwise nonisomorphic irreducible $F\langle g\rangle$-modules. Then*

$$C_{\mathrm{GL}(V)}(g) = C_{\mathrm{GL}(V_1)}(g_1) \times \cdots \times C_{\mathrm{GL}(V_k)}(g_k).$$

2.3.2 Conjugacy and semisimplicity

Continue to assume that $V = F^n$ where $n \geqslant 1$ and F is a field. Let us record some general results on $\mathrm{GL}_n(F)$, which are surely well known but are hard to find direct references for. In this section, it will be convenient to fix a basis for V and consider the elements of $\mathrm{GL}_n(F)$ as matrices with respect to this basis. In light of the notation of the previous section, we will write $g_1 \oplus \cdots \oplus g_k$ for the block diagonal matrix

$$\begin{pmatrix} g_1 & 0 & \cdots & 0 \\ 0 & g_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_k \end{pmatrix}$$

The *companion matrix* of a monic polynomial $\phi = \sum_{i=0}^{n} a_i t^i \in F[t]$ is the $n \times n$ matrix

$$C(\phi) = \left(\begin{array}{c|ccc} 0 & & & \\ \vdots & & I_{n-1} & \\ 0 & & & \\ \hline -a_0 & -a_1 & \cdots & -a_{n-1} \end{array}\right)$$

The following is the main theorem on conjugacy in $\mathrm{GL}_n(F)$ (see [39, 11.17 and 11.26], for example). We say that $g, h \in \mathrm{GL}_n(F)$ are *similar* if g and h are $\mathrm{GL}_n(F)$-conjugate.

Theorem 2.3.6. *Each element $g \in \mathrm{GL}_n(F)$ is similar to a unique block diagonal matrix*

$$C(\phi_1^{e_{11}}) \oplus \cdots \oplus C(\phi_1^{e_{1r_1}}) \oplus \cdots C(\phi_k^{e_{k1}}) \oplus \cdots \oplus C(\phi_k^{e_{kr_k}}) \tag{2.13}$$

where $\phi_i \in F[t]$ are distinct monic irreducible polynomials and $e_{i1} \geqslant \ldots \geqslant e_{ir_i} \geqslant 1$. Moreover $\prod_{i,j} \phi_i^{e_{ir_j}}$ is the characteristic polynomial of g and $\prod_i \phi_i^{e_{i1}}$ is the minimal polynomial of g.

The element in (2.13) is known as the *(primary) rational canonical form* of g. By Theorem 2.3.6, two elements of $\mathrm{GL}_n(F)$ are similar if and only if they have the same rational canonical form.

Lemma 2.3.7. *Let $g \in \mathrm{GL}_n(F)$. Then g is irreducible if and only if the characteristic polynomial of g is irreducible over F.*

Proof. Let χ be the characteristic polynomial of g. First assume that g is reducible. That is, V has an k-dimensional submodule U with $0 < k < n$. Therefore, g is similar to the block lower triangular matrix

$$\begin{pmatrix} g_1 & 0 \\ h & g_2 \end{pmatrix}$$

where g_1 is a $k \times k$ matrix. Now the characteristic polynomial ϕ of g_1 (of degree k) is a proper nonconstant divisor of χ (of degree n), so χ is reducible.

For the converse, assume that g is irreducible. From the rational canonical form of g, it is evident that the irreducibility of g implies that χ is the minimal polynomial of g. We wish to prove that χ is irreducible, so write $\chi = \phi\psi$, where ϕ and ψ are monic. Since $\chi(g) = 0$, without loss of generality, $\phi(g)$ is not invertible. Now let U be the kernel of $\phi(g)$, noting that $U \neq 0$. Let $u \in U$ and note that $(ug)\phi(g) = (u\phi(g))g = 0g = 0$, so U is a submodule of V. However, V is irreducible, so $U = V$ and, consequently, $\phi(g) = 0$. Since χ is the minimal polynomial of x, we deduce that $\chi = \phi$. Therefore, χ is irreducible. This completes the proof. □

Lemma 2.3.8. *Let $g, h \in \mathrm{GL}_n(F)$ be irreducible. Then g and h are similar if and only if they have the same characteristic polynomial.*

Proof. If g and h are similar, then g and h evidently have the same characteristic polynomial. Now assume χ is the characteristic polynomial of both g and h. By Lemma 2.3.7, χ is irreducible, so $C(\chi)$ is the rational canonical form of g and h. Now Theorem 2.3.6 implies g and h are similar. This completes the proof. □

We say that an element $g \in \mathrm{GL}_n(F)$ is *semisimple*, if g is similar to a block diagonal matrix $g_1 \oplus \cdots \oplus g_k$ where each g_i is irreducible. By Maschke's Theorem, if F is a finite field of characteristic p, then g is semisimple if and only if p does not divide the order of g.

Lemma 2.3.9. *Let $g, h \in \mathrm{GL}_n(F)$ be semisimple. Then g and h are similar if and only if they have the same characteristic polynomial.*

Proof. Let $g, h \in \mathrm{GL}_n(q)$ be semisimple. If g and h are similar, then evidently g and h have the same characteristic polynomial. Now assume that χ is the characteristic polynomial of both g and h. Since g and h are semisimple, they are similar to block diagonal matrices $g_1^{a_1} \oplus \cdots \oplus g_k^{a_k}$ and $h_1^{b_1} \oplus \cdots \oplus h_l^{b_l}$, where $g_1, \ldots, g_k$ and $h_1, \ldots, h_l$ are pairwise non-similar irreducible matrices. For each i, let ϕ_i and ψ_i be the characteristic polynomials of g_i and h_i, respectively. By Lemma 2.3.7, the polynomials ϕ_i and ψ_i are irreducible since the matrices g_i and h_i are irreducible. Now

$$\phi_1^{a_1} \cdots \phi_k^{a_k} = \chi = \psi_1^{b_1} \cdots \psi_l^{b_l}.$$

By the irreducibility of each ϕ_i and ψ_i, we conclude $k = l$ and we may assume that for each i we have $\phi_i = \psi_i$ and $a_i = b_i$. For each i, by Lemma 2.3.8, g_i and h_i are similar since g_i and h_i are irreducible and have equal characteristic polynomials. Therefore, g and h are similar, as required. □

The following result is the main result on the conjugacy of semisimple elements of odd order in finite symplectic and orthogonal groups. This was proved in in [62] (see [17, Lemmas 3.4.2 and 3.5.1] for a convenient statement).

Theorem 2.3.10. *Let G be $\mathrm{Sp}_n(q)$ or $\mathrm{O}_n^\varepsilon(q)$. Two semisimple elements of G of odd order are G-conjugate if and only if they are similar.*

2.3.3 Subfields and field extensions

Continue to assume that $V = F^n$ where $n \geqslant 1$ and F is a field. In this section, we will introduce two sorts of subgroups of classical groups: ones which arise from subfields of F and others which arise from field extensions of F. We will see that the latter provide a helpful perspective on semisimple elements. Both sorts of subgroups will feature in an important way in Section 2.5.

Let F_0 be a subfield of F and let V_0 be the F_0-span of an F-basis $\mathcal{B}$ for V. Then all F_0-linear maps on V_0 extend to F-linear maps on V. Therefore, $\mathrm{GL}(V_0) \leqslant \mathrm{GL}(V)$, and we call $\mathrm{GL}(V_0)$ a *subfield subgroup* of $\mathrm{GL}(V)$.

As explained in [43, Chapter 4.5], we can obtain subfield subgroups of other classical groups. For instance, if n is even, $\mathcal{B}$ is the basis $\mathcal{B}^+$ from (2.5) and Q_0 is a nondegenerate plus-type quadratic form on V_0, then Q_0 extends to a nondegenerate plus-type quadratic form Q on V, and we thus obtain the embedding $\mathrm{O}^+_n(F_0) \leqslant \mathrm{O}^+_n(F)$. Note that a classical group may have a subfield subgroup of a different type. For example, both $\mathrm{O}^+_{2m}(q)$ and $\mathrm{O}^-_{2m}(q)$ are subfield subgroups of $\mathrm{O}^+_{2m}(q^2)$ (see the proof of Lemma 2.6.17).

We now turn to field extensions. To avoid Galois theoretic technicalities, let us assume that $F = \mathbb{F}_q$ where $q = p^f$. The following lemma, and its proof, encapsulates field extension subgroups.

Lemma 2.3.11. *Let k divide n.*

(i) *There is an embedding $\pi\colon \mathrm{GL}_{n/k}(q^k){:}\,\mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q) \to \mathrm{GL}_n(q)$.*

(ii) *If $\lambda \in \overline{\mathbb{F}}_p$ is an eigenvalue of $g \in \mathrm{GL}_{n/k}(q^k)$, then λ is an eigenvalue of $\pi(g)$.*

(iii) *If $g \in \mathrm{GL}_{n/k}(q^k)$, then $\det(\pi(g)) = \det(g)^{q^{k-1}+\cdots+q+1}$.*

Proof. Let $V_\# = \mathbb{F}_{q^k}^{n/k}$ and fix an $\mathbb{F}_{q^k}$-basis $\mathcal{B}_\# = \{u_1, \ldots, u_{n/k}\}$ of $V_\#$. Then $V_\#$ is naturally an n-dimensional vector space over $\mathbb{F}_q$ with basis

$$\mathcal{B} = \{\mu_i u_j \mid 1 \leqslant i \leqslant k \text{ and } 1 \leqslant j \leqslant n/k\},$$

where $\{\mu_1, \ldots, \mu_k\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^k}$. In this way, we identify $V_\#$ with $V = \mathbb{F}_q^n$.

Since any $\mathbb{F}_{q^k}$-linear map is an $\mathbb{F}_q$-linear map, $\mathrm{GL}_{n/k}(q^k)$ embeds in $\mathrm{GL}_n(q)$. Moreover, any $\mathbb{F}_q$-automorphism of $\mathbb{F}_{q^k}$ is an $\mathbb{F}_q$-linear map, so, in fact, $\mathrm{GL}_{n/k}(q^k){:}\,\mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q)$ embeds in $\mathrm{GL}_n(q)$. This proves (i).

For part (ii), let $g \in \mathrm{GL}_{n/k}(q^k)$ and let $\lambda \in \overline{\mathbb{F}}_p$ be an eigenvalue of g. Let

$$v = \omega_1 u_1 + \cdots + \omega_{n/k} u_{n/k}$$

be a λ-eigenvector in the $\overline{\mathbb{F}}_p$-span of $\mathcal{B}_\#$. Then v is in the $\overline{\mathbb{F}}_p$-span of $\mathcal{B}$ and $v\pi(g) = \lambda v$, so λ is an eigenvalue of $\pi(g)$. Part (iii) is given in [43, (4.3.13)]. □

We call the images of both $\mathrm{GL}_{n/k}(q^k)$ and $\mathrm{GL}_{n/k}(q^k)\colon\mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q)$ under the embedding in Lemma 2.3.11 *field extension subgroups*. If needed, we refer to $\mathrm{GL}_{n/k}(q^k)$ as the *base* of the group $\mathrm{GL}_{n/k}(q^k)\colon\mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q)$.

In [43, Chapter 4.3], field extension subgroups of other classical groups are constructed. For instance, if $n = 2m$ and $\kappa_\#$ is a symplectic form on $\mathbb{F}_{q^k}^{2m/k}$, then $\kappa = \mathrm{T}\circ\kappa_\#$ is a symplectic form on $\mathbb{F}_q^{2m}$, where $\mathrm{T}\colon\mathbb{F}_{q^k}\to\mathbb{F}_q$ is the trace, so $\mathrm{Sp}_{2m/k}(q^k)$ embeds in $\mathrm{Sp}_{2m}(q)$.

In Lemma 2.3.12, we record some particular examples that will feature in Section 2.3.5. In this lemma, we will not concern ourselves with the embedding of the Galois group of the field extension since we will not require this for our application. Recall the definition of $\mathrm{DO}^{\pm}_{2m}(q)$ from Section 2.2.6 (see (2.11) in particular).

Lemma 2.3.12. *Let $n = 2m$ where $m \geqslant 1$ and let k divide m. Then*

(i) $\mathrm{Sp}_{2m/k}(q^k)$ *embeds in* $\mathrm{Sp}_{2m}(q)$

(ii) *if q is odd, then* $\{g \in \mathrm{GSp}_{2m/k}(q^k) \mid \tau(g) \in \mathbb{F}_q\}$ *embeds in* $\mathrm{GSp}_{2m}(q)$

(iii) $\mathrm{SO}^-_{2m/k}(q^k)$ *embeds in* $\mathrm{SO}^-_{2m}(q)$

(iv) *if q is odd, then* $\{g \in \mathrm{DO}^-_{2m/k}(q^k) \mid \tau(g) \in \mathbb{F}_q\}$ *embeds in* $\mathrm{DO}^-_{2m}(q)$.

Moreover, in (ii) *and* (iv), *τ is invariant under the embedding.*

Proof. These embeddings are given in [43, Section 4.3], see in particular [43, (4.3.8) and (4.3.11)] and the comment on τ is [43, Lemma 4.3.5(i)]. The exception is (iv), where only the embedding

$$\pi\colon \{g \in \mathrm{GO}^-_{2m/k}(q^k) \mid \tau(g) \in \mathbb{F}_q\} \to \mathrm{GO}^-_{2m}(q)$$

is established.

Let q be odd and let $g \in \mathrm{DO}^-_{2m/k}(q^k)$ with $\tau(g) \in \mathbb{F}_q$. Then $\det(g) = \tau(g)^m$. Therefore, by Lemma 2.3.11(iii) (see Remark 2.3.13 below), $\det(\pi(g)) = \det(g) = \tau(g)^m = \tau(\pi(g))^m$. Therefore, $\pi(g) \in \mathrm{DO}^-_{2m}(q)$, which gives the embedding in (iv) and completes the proof. □

Remark 2.3.13. The field extension embeddings in Lemma 2.3.12, as described in [43, Section 4.3], are simply restrictions of the embedding in Lemma 2.3.11. Therefore, parts (ii) and (iii) of Lemma 2.3.11 hold for the embeddings in Lemma 2.3.12 also.

2.3.4 Primitive prime divisors

For positive integers a, b such that $a \geqslant 2$, we say that a positive integer r is a *primitive divisor* of $a^b - 1$ if r divides $a^b - 1$ but r does not divide $a^k - 1$ for any $k < b$. Write $\mathrm{ppd}(a, b)$ for the set of *primitive prime divisors* of $a^b - 1$.

The following useful theorem is due to Zsigmondy [65] (see also [17, Theorem 3.1.5]).

Theorem 2.3.14. *Let (a, b) be a pair of positive integers satisfying*

$$a \geqslant 2 \text{ and } (a, b) \neq (2, 6) \text{ and } a + 1 \text{ is not a power of 2 if } b = 2. \tag{2.14}$$

Then there exists a primitive prime divisor of $a^b - 1$.

For the following lemma see [4, Lemma 6.1], for example.

Lemma 2.3.15. *Let a be a prime power and let $b \geqslant 3$. Assume that $(a, b) \neq (2, 6)$.*

(i) *If $r \in \mathrm{ppd}(a, b)$, then $r \equiv 1 \pmod{b}$.*

(ii) *If $\mathrm{ppd}(a, b) = \{b + 1\}$, then a is prime and $a^b \in \{2^4, 2^{10}, 2^{12}, 2^{18}, 3^4, 3^6, 5^6\}$.*

(iii) *If $\mathrm{ppd}(a, b) \subseteq \{b + 1, 2b + 1\}$, then $a = 2$ and $b \in \{2, 8, 20\}$, or $a = 4$ and $b \in \{3, 6\}$.*

Remark 2.3.16. Let us make some number theoretic comments.

(i) A primitive divisor is defined in terms of the expression "$a^b - 1$" and not the numerical value of $a^b - 1$: for instance, 7 is the only primitive prime divisor of $4^3 - 1$ and 3 is the only primitive prime divisor of $8^2 - 1$, but $4^3 - 1 = 8^2 - 1$.

(ii) Numbers a such that $a + 1$ is a power of two are said to be *Mersenne*. Although we do not use this, we note that if a is a prime power and $a + 1$ is a power of two, then Catalan's Conjecture (which is a theorem [54]) implies that a is a Mersenne prime.

2.3.5 Irreducible elements of classical groups

For this section, $V = \mathbb{F}_q^n$ where $n \geqslant 1$ and $q = p^f$. Write $\mathbb{F}_q^\times = \langle \alpha \rangle$. For a field extension E/F and $\lambda \in E$, recall that the *minimal polynomial* of λ over F is the monic polynomial ϕ over F of least degree such that $\phi(\lambda) = 0$ (so, ϕ is irreducible over F).

Lemma 2.3.17. *Let r be a primitive (not necessarily prime) divisor of $q^n - 1$. Let $g \in \mathrm{GL}_n(q)$ and assume that g has an eigenvalue over $\overline{\mathbb{F}}_p$ of order r. Then g is irreducible on $\mathbb{F}_q^n$ and the eigenvalues of g over $\overline{\mathbb{F}}_p$ are $\lambda, \lambda^q, \ldots, \lambda^{q^{n-1}}$, which are all distinct.*

Proof. Let $\lambda \in \overline{\mathbb{F}}_p$ be an eigenvalue of g of order r and let ϕ be the minimal polynomial of λ over $\mathbb{F}_q$. Since r is a primitive divisor of $q^n - 1$, the element λ is contained in $\mathbb{F}_{q^n}$ and is not contained in any proper subfield of $\mathbb{F}_{q^n}$. Therefore, ϕ is a polynomial of degree n. However, the characteristic polynomial of g is a monic polynomial χ of degree n such that $\chi(\lambda) = 0$. Therefore, $\chi = \phi$. In particular, χ is irreducible over $\mathbb{F}_q$. Now Lemma 2.3.7 implies that g is irreducible on $\mathbb{F}_q^n$. Moreover, the eigenvalues of g are the roots of χ, which are the n distinct Galois conjugates $\lambda, \lambda^q, \ldots, \lambda^{q^{n-1}}$. This completes the proof. □

The following result provides irreducible elements of $\mathrm{GL}_n(q)$.

Lemma 2.3.18. *Let r be a primitive divisor of $q^n - 1$ and let $\lambda \in \mathbb{F}_{q^n}^\times$ have order r. Then $\mathrm{GL}_n(q)$ contains an irreducible element of order r and with eigenvalues $\lambda, \lambda^q, \ldots, \lambda^{q^{n-1}}$.*

Proof. By Lemma 2.3.11(i), there is a field extension embedding $\pi\colon \mathrm{GL}_1(q^n) \to \mathrm{GL}_n(q)$. Now $g = \pi((\lambda)) \in G$ has order r. Lemma 2.3.11(ii) implies that λ is an eigenvalue of g, so, by Lemma 2.3.17, g is irreducible and has eigenvalues $\lambda, \lambda^q, \ldots, \lambda^{q^{n-1}}$. □

For the remainder of Section 2.3.5 write $n = 2m$.

Lemma 2.3.19. *Let G be $\mathrm{Sp}_{2m}(q)$ or $\mathrm{SO}^-_{2m}(q)$. Let r be a primitive divisor of $q^{2m}-1$ that divides q^m+1 and let $\lambda \in \mathbb{F}^\times_{q^{2m}}$ have order r. Then G contains an irreducible element of order r and eigenvalues $\lambda, \lambda^q, \ldots, \lambda^{q^{2m-1}}$.*

Proof. First assume that $G = \mathrm{Sp}_{2m}(q)$. By Lemma 2.3.12(i), there is a field extension embedding $\pi_1\colon \mathrm{Sp}_2(q^m) \to \mathrm{Sp}_{2m}(q^m)$. Now $\mathrm{Sp}_2(q^m) = \mathrm{SL}_2(q^m)$, so Lemma 2.3.11 gives an embedding $\pi_2\colon H \to \mathrm{Sp}_2(q^m)$, where

$$H = \{(\mu) \in \mathrm{GL}_1(q^{2m}) \mid \mu^{q^m+1} = 1\} \cong C_{q^m+1}.$$

Now $g = \pi_1(\pi_2((\lambda))) \in G$ has order r. By Lemma 2.3.11(ii), λ is an eigenvalue of g. Since λ has order r, by Lemma 2.3.17, g is irreducible and has eigenvalues $\lambda, \lambda^q, \ldots, \lambda^{q^{2m-1}}$.

Now assume that $G = \mathrm{SO}^-_{2m}(q)$. Lemma 2.3.12(iii) gives $\pi\colon \mathrm{SO}^-_2(q^m) \to \mathrm{SO}^-_{2m}(q)$. Since $\mathrm{SO}^-_2(q^m) \cong C_{q^m+1}$, we may fix $h \in \mathrm{SO}^-_2(q^m)$ of order r. Without loss of generality, the eigenvalues of h are λ and λ^{-1}. As in the previous case, $\pi(h) \in G$ has order r and Lemma 2.3.11(ii) implies that λ is an eigenvalue of g, so g is irreducible with eigenvalues $\lambda, \lambda^q, \ldots, \lambda^{q^{2m-1}}$. □

For the following result, recall that $\mathbb{F}_q^\times = \langle \alpha \rangle$.

Lemma 2.3.20. *Let q be odd and let G be either $\mathrm{GSp}_{2m}(q)$ or $\mathrm{DO}^-_{2m}(q)$. Let r be a divisor of q^m+1 that is divisible by $(q^m+1)_2$. Assume that $r/2$ is a primitive divisor of $q^{2m}-1$. Then G contains an element g of order $(q-1)r$ such that $\tau(g) = \alpha$ and g^{q-1} is irreducible.*

Proof. First assume that $G = \mathrm{GSp}_{2m}(q)$. Let $\lambda \in \mathbb{F}^\times_{q^{2m}}$ have order $(q-1)r$. The order of λ^{q^m+1} is $(q-1)r/(q^m+1,(q-1)r)$. Since r divides q^m+1, we may write

$$(q^m+1,\ (q-1)r) = r\ \left(\tfrac{1}{r}(q^m+1),\ q-1\right) = r,$$

where the second equality holds since $(q^m+1, q-1) = 2$ and $(q^m+1)_2$ divides r. Therefore, λ^{q^m+1} has order $q-1$. Consequently, we may choose λ such that $\lambda^{q^m+1} = \alpha$.

We now proceed as in the proof of Lemma 2.3.19. By Lemma 2.3.12(ii), there is a field extension embedding $\pi_1\colon H \to \mathrm{GSp}_{2m}(q)$, where

$$H = \{h \in \mathrm{GSp}_2(q^m) \mid \tau(h) \in \mathbb{F}_q\} = \{h \in \mathrm{GL}_2(q^m) \mid \det(h) \in \mathbb{F}_q\},$$

where the second equality holds since $\mathrm{GSp}_2(q^m) = \mathrm{GL}_2(q^m)$ and $\tau(h) = \det(h)$ for all $h \in \mathrm{GSp}_2(q^m)$ (see [43, Lemma 2.4.5], for example). By Lemma 2.3.11, there is a field extension embedding $\pi_2\colon K \to H$, where

$$K = \{(\mu) \in \mathrm{GL}_1(q^{2m}) \mid \mu^{q^m+1} \in \mathbb{F}_q\}.$$

Now $g = \pi_1(\pi_2((\lambda))) \in G$ has order $(q-1)r$. Moreover,

$$\tau(g) = \tau(\pi_2((\lambda)) = \det(\pi_2((\lambda))) = \lambda^{q^m+1} = \alpha.$$

By Lemma 2.3.11(ii), λ is an eigenvalue of g, so λ^{q-1} is an eigenvalue of g^{q-1}. Since λ^{q-1} has order r, by Lemma 2.3.17, g^{q-1} is irreducible.

Now assume that $G = \mathrm{DO}^-_{2m}(q)$. In this case, let $\lambda \in \mathbb{F}^\times_{q^{2m}}$ have order r. Lemma 2.3.12(iv) implies that there is a field extension embedding $\pi\colon H \to \mathrm{DO}^-_{2m}(q)$, where

$$H = \{h \in \mathrm{DO}^-_2(q^m) \mid \tau(h) \in \mathbb{F}_q\} \cong C_{(q^m+1)(q-1)}.$$

Now fix $h \in \mathrm{DO}^-_2(q^m)$ of order $(q-1)r$ and $\tau(h) = \alpha$. Without loss of generality, the eigenvalues of h are λ and $\alpha\lambda^{-1}$. Let $g = \pi(h)$. Then g has order $(q-1)r$ and $\tau(g) = \tau(h) = \alpha$. Moreover, λ^{q-1} is an eigenvalue of g^{q-1} of order $r/(r, q-1) = r/2$, so Lemma 2.3.17 implies that g^{q-1} is irreducible. This completes the proof. □

Let (G, C) be $(\mathrm{Sp}_{2m}(q), \mathrm{GSp}_{2m}(q))$ or $(\mathrm{O}^+_{2m}(q), \mathrm{GO}^+_{2m}(q))$ and let $V = \mathbb{F}_q^{2m}$ be the natural module for G. Then V admits a decomposition $\mathcal{D}(V)$

$$V = V_1 \oplus V_2 \quad \text{where} \quad V_1 = \langle e_1, \ldots, e_m\rangle \text{ and } V_2 = \langle f_1, \ldots, f_m\rangle, \tag{2.15}$$

noting that V_1 and V_2 are totally singular m-spaces (with respect to the bases in (2.4) and (2.5)). The following describes the centraliser of the decomposition $\mathcal{D}(V)$ in (2.15).

Lemma 2.3.21. *Let (G, C) be $(\mathrm{Sp}_{2m}(q), \mathrm{GSp}_{2m}(q))$ or $(\mathrm{O}^+_{2m}(q), \mathrm{GO}^+_{2m}(q))$. Then*

(i) $G_{(\mathcal{D}(V))} = \{g \oplus g^{-\mathsf{T}} \mid g \in \mathrm{GL}_m(q)\}$

(ii) $C_{(\mathcal{D}(V))} = \{\lambda g \oplus g^{-\mathsf{T}} \mid g \in \mathrm{GL}_m(q) \text{ and } \lambda \in \mathbb{F}_q^\times\}$

(iii) *If $g \in \mathrm{GL}_m(q)$ and $\lambda \in \mathbb{F}_q^\times$, then $\tau(\lambda g \oplus g^{-\mathsf{T}}) = \lambda$.*

Proof. The matrix of the underlying bilinear form with respect to $(e_1, \ldots, e_m, f_1, \ldots, f_m)$ is

$$M = \begin{pmatrix} 0 & I_m \\ I_m & 0 \end{pmatrix}.$$

Let $x = g \oplus h \in \mathrm{GL}(V)$ centralise $\mathcal{D}(V)$. If x is a similarity of the form, then, for some $\lambda \in \mathbb{F}_q^\times$, we have $xMx^{-\mathsf{T}} = \lambda M$ and consequently $g = \lambda h^{-\mathsf{T}}$. It is straightforward to see that all such elements are indeed similarities. This proves (ii). Now let $\lambda \in \mathbb{F}_q^\times$ and $g \in \mathrm{GL}(V)$. Write $x = \lambda g \oplus g^{-\mathsf{T}}$. Then $xMx^{-\mathsf{T}} = \lambda M$, so $\tau(x) = \lambda$. This proves (iii) and consequently (i). □

Remark 2.3.22. Assume that q is odd. Let $x = \lambda g \oplus g^{-\mathsf{T}} \in \mathrm{GO}^+_{2m}(q)$ centralise $\mathcal{D}(V)$, where $g \in \mathrm{GL}_m(q)$ and $\lambda \in \mathbb{F}_q^\times$. Evidently $\det(x) = \lambda^m$, which equals $\tau(x)^m$, by Lemma 2.3.21(iii). Thus, $x \in \mathrm{DO}^+_{2m}(q)$. This implies that $(\mathrm{GO}^+_{2m}(q))_{(\mathcal{D}(V))} \leqslant \mathrm{DO}^+_{2m}(q)$ and consequently $(\mathrm{O}^+_{2m}(q))_{(\mathcal{D}(V))} \leqslant \mathrm{SO}^+_{2m}(q)$.

Remark 2.3.23. For two maximal totally singular subspaces $U, W \leqslant V$, write $U \sim W$ if and only if $m - \dim U \cap W$ is even. Then $\sim$ is an equivalence relation with exactly two equivalence classes $\mathcal{U}^1$ and $\mathcal{U}^2$ [2, 22.13]. Now $\mathrm{PDO}^+_{2m}(q)$ is the stabiliser in $\mathrm{PGO}^+_{2m}(q)$ of each of $\mathcal{U}^1$ and $\mathcal{U}^2$ (see [17, p.56]). In particular, $(\mathrm{PGO}^+_{2m}(q))_{\mathcal{D}(V)} \leqslant \mathrm{PDO}^+_{2m}(q)$ if and only if m is even.

Lemma 2.3.24. *Let G be $\mathrm{Sp}_{2m}(q)$ or $\mathrm{SO}^+_{2m}(q)$. Let r be a primitive divisor of $q^m - 1$. Then G contains an element of order r that centralises $\mathcal{D}(V)$ and acts irreducibly on both V_1 and V_2.*

Proof. By Lemma 2.3.18, there exists an irreducible element $g \in \mathrm{GL}_m(q)$ of order r. The corresponding element $g \oplus g^{-\mathsf{T}} \in G_{(\mathcal{D}(V))}$ satisfies the statement of the corollary. □

The following straightforward lemma is [17, Lemma 3.1.13].

Lemma 2.3.25. *Let $k > 1$, let r be a primitive prime divisor of $q^k - 1$, let $\lambda \in \mathbb{F}^\times_{q^k}$ have order r and let $\Lambda = \{\lambda^{q^j} \mid 0 \leqslant j < k\}$. Then $\Lambda^{-1} = \Lambda$ if and only if k is even.*

Proof. Since r is a primitive divisor of $q^k - 1$, we know $|\Lambda| = k$. Now $r \neq 2$, since $k > 1$, so $\mu \neq \mu^{-1}$ for all $\mu \in \Lambda$. Therefore, if $\Lambda^{-1} = \Lambda$, then k is necessarily even. Now assume that k is even and write $k = 2l$. Since r is a primitive prime divisor of $q^{2l} - 1$ it must be that r divides $q^l + 1$. Therefore, $\lambda^{q^l+1} = \lambda$, so $\lambda^{q^l} = \lambda^{-1}$, which proves that $\Lambda^{-1} = \Lambda$. □

2.3.6 Types of semisimple elements

Continue to write $V = \mathbb{F}_q^{2m}$ and $\mathbb{F}^\times_q = \langle \alpha \rangle$. Using the results of the previous sections, we define several *types* of semisimple elements in symplectic and orthogonal groups. The general idea that motivates these definitions is that we are interested in elements that stabilise few subspaces, whose orders have few prime divisors and which are contained in particular cosets of $\mathrm{Sp}_{2m}(q)$ in $\mathrm{GSp}_{2m}(q)$ or $\Omega^\pm_{2m}(q)$ in $\mathrm{GO}^\pm_{2m}(q)$.

Definition 2.3.26. Let m be odd and let G be $\mathrm{Sp}_{2m}(q)$ or $\mathrm{SO}^+_{2m}(q)$. An element $g \in G$ has *type* $(2m)^+_q$ if $|g| \in \mathrm{ppd}(q, m)$ and g centralises a decomposition $V = V_1 \oplus V_2$ where V_1 and V_2 are totally singular nonisomorphic irreducible $\mathbb{F}_q\langle g \rangle$-modules.

Lemma 2.3.27. *Let G be $\mathrm{Sp}_{2m}(q)$ or $\mathrm{SO}^+_{2m}(q)$ and assume that m is odd. Then G contains an element of type $(2m)^+_q$.*

Proof. Theorem 2.3.14 implies that $q^m - 1$ has a primitive prime divisor r and Lemma 2.3.24 establishes that G contains an element $g \oplus g^{-\mathsf{T}}$ of order r that centralises $\mathcal{D}(V)$ and acts irreducibly on both V_1 and V_2. By Lemma 2.3.25, since m is odd, the eigenvalue sets of g and $g^{-\mathsf{T}}$ are distinct, so g and $g^{-\mathsf{T}}$ are nonisomorphic. Therefore, $g \oplus g^{-\mathsf{T}}$ has type $(2m)^+_q$. □

Definition 2.3.28. Let G be $\mathrm{Sp}_{2m}(q)$ or $\mathrm{SO}^-_{2m}(q)$. An element $g \in G$ has *type* $(2m)^-_q$ if g is irreducible on V and either $|g| \in \mathrm{ppd}(q, 2m)$, or q is Mersenne, $m = 1$ and $|g| = q + 1$.

Lemma 2.3.29. *Let G be $\mathrm{Sp}_{2m}(q)$ or $\mathrm{SO}^-_{2m}(q)$ and assume that $(m,q) \neq (3,2)$. Then G contains an element of type $(2m)^-_q$.*

Proof. If q is Mersenne and $m = 1$, then let $r = q+1$. Otherwise, Theorem 2.3.14 implies that $q^{2m}-1$ has a primitive prime divisor r. Now Lemma 2.3.19 implies that G contains an irreducible element of order r, as claimed. □

Lemma 2.3.30. *Let $g \in \mathrm{SO}^\varepsilon_{2m}(q)$ have type $(2m)^\varepsilon_q$. Then $g \notin \Omega^\varepsilon_{2m}(q)$ if and only if $\varepsilon = -$, $m = 1$ and q is Mersenne.*

Proof. First assume that $\varepsilon = -$, $m = 1$ and q is Mersenne. Then $|g| = q+1$ and $|\Omega^-_2(q)| = \frac{1}{2}(q+1)$, so $g \notin \Omega^-_2(q)$. Now assume otherwise. Therefore, g has odd prime order, so $g \in \Omega^\varepsilon_{2m}(q)$. □

Lemma 2.3.31. *Let g be an element of $\mathrm{Sp}_{2m}(q)$ or $\mathrm{SO}^\varepsilon_{2m}(q)$ of type $(2m)^\varepsilon_q$. Then the eigenvalues of g (over $\overline{\mathbb{F}}_p$) are distinct.*

Proof. If $\varepsilon = -$, then g is irreducible, so the characteristic polynomial of g over $\mathbb{F}_q$ is irreducible and the eigenvalues of g are distinct. Now assume that $\varepsilon = +$. Then $g = x \oplus x^{-\mathsf{T}}$, centralising the decomposition $\mathcal{D}(V)$ (see (2.15)) where x and $x^{-\mathsf{T}}$ act irreducibly on V_1 and V_2. Therefore, the characteristic polynomial of x is irreducible. Moreover, V_1 and V_2 are nonisomorphic $\mathbb{F}_q\langle x\rangle$-modules, so the characteristic polynomials of x and $x^{-\mathsf{T}}$ are distinct irreducible polynomials. Consequently, g has distinct eigenvalues in this case too. This completes the proof. □

Now assume that q is odd. Fix $\beta \in \mathbb{F}_q^\times$ with $|\beta| = (q-1)_2$. Note that $\alpha, \beta \notin (\mathbb{F}_q^\times)^2$. We will define some variants on the types of elements defined above, which have a very similar action on the natural module. Consequently, in the first instance the reader is encouraged to think of elements of type $(2m)^\pm_q$ upon encountering ${}^\Delta(2m)^\pm_q$ and ${}^\Sigma(2m)^\pm_q$.

Definition 2.3.32. Let q be odd, let $\varepsilon \in \{+,-\}$ and let G be $\mathrm{GSp}_{2m}(q)$ or $\mathrm{DO}^\varepsilon_{2m}(q)$. An element $g \in G$ has *type* ${}^\Delta(2m)^\varepsilon_q$ if $\tau(g) = \beta$ and g^k has type $(2m)^\varepsilon_q$ where

$$k = \begin{cases} (q^m+1)_2(q-1)_2 & \text{if } \varepsilon = - \text{ and either } m \geqslant 3 \text{ or } q \text{ is not Mersenne} \\ (q-1)_2 & \text{otherwise.} \end{cases}$$

Lemma 2.3.33. *Let q be odd, let $\varepsilon \in \{+,-\}$ and let G be $\mathrm{GSp}_{2m}(q)$ or $\mathrm{DO}^\varepsilon_{2m}(q)$.*

(i) *If $\varepsilon = +$ and $m > 1$ is odd, then G contains an element of type ${}^\Delta(2m)^+_q$.*

(ii) *If $\varepsilon = -$, then G contains an element of type ${}^\Delta(2m)^-_q$*

Proof. First assume that $\varepsilon = +$. By Lemma 2.3.27, G contains an element $g \oplus g^{-\mathsf{T}}$ of type $(2m)^+_q$. Let $h = \beta g \oplus g^{-\mathsf{T}}$, noting that $h \in G$ (see Lemma 2.3.21(ii) and Remark 2.3.22). We claim that h has type ${}^\Delta(2m)^+_q$. By Lemma 2.3.21(iii), $\tau(h) = \beta$. Now $|g|$ is odd, since $|g| \in \mathrm{ppd}(q,m)$, and $|\beta| = (q-1)_2$, so $h^{(q-1)_2} = g^{(q-1)_2} \oplus (g^{(q-1)_2})^{-\mathsf{T}}$ has order $|g|$. Therefore, $h^{(q-1)_2}$ has type $(2m)^+_q$ and, consequently, h has type ${}^\Delta(2m)^+_q$.

Now assume that $\varepsilon = -$. For now assume further that $m \geqslant 3$ or q is not Mersenne. Then Theorem 2.3.16 implies that we may fix $r \in \mathrm{ppd}(2m, q)$. By Lemma 2.3.19, there exists an element $g \in G$ of order $r(q^m+1)_2(q-1)$ such that $\tau(g) = \alpha$ and $g^{(q-1)}$ is irreducible. Let $h = g^{(q-1)_{2'}}$. Then $h^{(q^m+1)_2(q-1)_2}$ has type $(2m)_q^-$ and $\tau(h)$ has order $(q-1)_2$, so without loss of generality is $\tau(h) = \beta$. Therefore, h has type ${}^{\Delta}(2m)_q^-$.

It remains to assume that $\varepsilon = -$, $m = 1$ and q is Mersenne. Then Lemma 2.3.19 implies that there exists $g \in G$ of order $(q+1)(q-1)$ such that $\tau(g) = \alpha$ and g^{q-1} is irreducible. As before, $g^{(q-1)_{2'}}$ has type ${}^{\Delta}(2)_q^-$. We have completed the proof. □

Definition 2.3.34. Let q be odd. An element $g \in \mathrm{SO}^{\varepsilon}_{2m}(q) \setminus \Omega^{\varepsilon}_{2m}(q)$ has *type* ${}^{\Sigma}(2m)^{\varepsilon}_q$ if g^k has type $(2m)^{\varepsilon}_q$ where $k = (q^m - \varepsilon)_2$.

Lemma 2.3.35. *Let q be odd.*

(i) *If $m > 1$ is odd, then $\mathrm{SO}^+_{2m}(q)$ contains an element of type ${}^{\Sigma}(2m)^+_q$.*

(ii) *If $m > 1$, then $\mathrm{SO}^-_{2m}(q)$ contains an element of type ${}^{\Sigma}(2m)^-_q$.*

Proof. First assume that $\varepsilon = +$ and $m > 1$ is odd. By Theorem 2.3.14, we may fix $r \in \mathrm{ppd}(m, q)$. Let $\lambda \in \mathbb{F}^{\times}_{q^{2m}}$ have order $r(q^m-1)_2$. By Lemma 2.3.18, $\mathrm{GL}_m(q)$ contains an element of $r(q^m-1)$ and determinant $\lambda^{q^{m-1}+\cdots+q+1}$. Let $h = g \oplus g^{-\mathsf{T}}$. By Lemma 2.3.21(i), $h \in \mathrm{SO}^+_{2m}(q)$. We know that $\lambda \notin (\mathbb{F}^{\times}_{q^m})^2$ since $(q^m-1)_2$ divides the order of λ. Therefore, $\det(g) = \lambda^{q^{m-1}+\cdots+q+1} \notin (\mathbb{F}^{\times}_q)^2$. Consequently, $h \notin \Omega^+_{2m}(q)$ by [43, Lemma 4.1.9]. Now $h^{(q^m-1)_2}$ has type $(2m)^+_q$, so h has type ${}^{\Sigma}(2m)^+_q$.

Now assume that $\varepsilon = -$ and $m > 1$. By Theorem 2.3.14, we may fix $r \in \mathrm{ppd}(2m, q)$. By Lemma 2.3.19, $\mathrm{SO}^-_{2m}(q)$ contains an irreducible element h of order $r(q^m+1)_2$. By [22, Theorem 4], $(q^m+1)_2$ does not divide the order of a maximal torus of $\Omega^-_{2m}(q)$, so $g \notin \Omega^-_{2d}(q)$. Since $h^{(q^m+1)_2}$ has type $(2m)^-_q$, h has type ${}^{\Sigma}(2d)^-_q$, completing the proof. □

For all of the elements introduced in this section, if the field size q is clear from the context, then we omit the subscript of q from the notation. However, in general, the field size is pertinent, as Lemma 2.3.36 demonstrates.

Lemma 2.3.36. *Let $m > 1$ and $q = q_0^e$. Let G be $\mathrm{Sp}_{2m}(q)$ or $\mathrm{SO}^{\eta}_{2m}(q)$. Let $g \in G$ have odd order and type $(2m)^{\eta}_{q_0}$, where we assume that m is odd if $\eta = +$. Then g is similar to $g_1 \oplus \cdots \oplus g_t$ where each of $g_1, \ldots, g_t$ has type $\left(\frac{2m}{t}\right)^{\varepsilon}_q$ where $t = (m, e)$ and $\varepsilon = \eta^{e/t}$.*

Proof. First assume that $\varepsilon = +$. Then $|g| \in \mathrm{ppd}(q_0, m)$ and the eigenvalue set of g is $\Lambda \cup \Lambda^{-1}$ where $\Lambda = \{\lambda, \lambda^{q_0}, \ldots, \lambda^{q_0^{m-1}}\}$. There are $t = (m, e)$ distinct $\mu \mapsto \mu^q$ orbits on Λ, say $\Lambda_1, \ldots, \Lambda_t$, each of size m/t. Fix $1 \leqslant j \leqslant t$ and $\lambda_j \in \Lambda_j$. By Lemma 2.3.17, there exists an irreducible element $x_j \in \mathrm{GL}_{m/t}(q)$ with eigenvalue set Λ_j. Then $g_j = x_j \oplus x_j^{-\mathsf{T}}$ has type $\left(\frac{2m}{t}\right)^+_q$ and eigenvalue set $\Lambda_j \cup \Lambda_j^{-1}$. Therefore, g has the same eigenvalues as $g_1 \oplus \cdots \oplus g_t$. Noting that g is a semisimple element of odd order, Lemma 2.3.9 implies that g is similar to $g_1 \oplus \cdots \oplus g_t$. This proves the claim in this case.

Now assume that $\varepsilon = -$. Then $|g| \in \mathrm{ppd}(q_0, 2m)$ and $\Lambda = \{\lambda, \lambda^{q_0}, \ldots, \lambda^{q_0^{2m-1}}\}$ is the eigenvalue set of g. There are $k = (2m, e)$ distinct $\mu \mapsto \mu^q$ orbits of Λ, say $\Lambda_1, \ldots, \Lambda_k$, each of size $2m/k$. Assume for now that $2m/k$ is odd. Then $k = (2m, e) = 2(m, e) = 2t$ and we may assume that $\Lambda_{t+j} = \Lambda_j^{-1}$ for each $1 \leqslant j \leqslant t$. As we argued in the previous case, there exists an element g_j of type $\left(\frac{2m}{t}\right)_q^+$ whose eigenvalue set is $\Lambda_i \cup \Lambda_i^{-1}$ and g is similar to $g_1 \oplus \cdots \oplus g_t$.

It remains to assume that $2m/k$ is even. In this case, $k = (2m, e) = (m, e) = t$. Fix $1 \leqslant j \leqslant t$ and let $\lambda_j \in \Lambda_j$. Lemma 2.3.19 implies that there exists an irreducible element $g_j \in \mathrm{SO}^-_{2m/t}(q)$ with eigenvalue set Λ_j. Therefore, g_j has type $\left(\frac{2m}{t}\right)_q^-$. Lemma 2.3.9 now implies that g is similar to $g_1 \oplus \cdots \oplus g_t$, which completes the proof. □

We conclude with a comment on centralisers.

Lemma 2.3.37. *Let G be $\mathrm{PGSp}_{2m}(q)$ or $\mathrm{PDO}^\varepsilon_{2m}(q)$. Let $g \in G$ lift to an element of type ${}^*(2m)^\varepsilon_q$, where $*$ is the empty symbol, Δ (q odd) or Σ (q odd and $T = \mathrm{P}\Omega^\varepsilon_{2m}(q)$). Then*

$$|C_G(g)| \leqslant q^m - \varepsilon.$$

Proof. A suitable power h of g has type $(2m)^\varepsilon_q$. For $x \in \mathrm{GL}_{2m}(q)$, write $\overline{x}$ for the image in $\mathrm{PGL}_{2m}(q)$. First assume that $\varepsilon = +$. Then $h = h_1 \oplus h_1^{-\mathsf{T}}$ and $|h| \in \mathrm{ppd}(q, m)$. Therefore, by [17, Appendix B] (see Lemma 2.4.4(ii) later), $|C_G(\overline{h})| = q^m - 1$, so $|C_G(\overline{g})| \leqslant q^m - 1$.

Next assume that $\varepsilon = -$. If $m > 1$ or q is not Mersenne, then $|h| \in \mathrm{ppd}(q, 2m)$ and from [17, Appendix B] (see Lemma 2.4.4(i)), $|C_G(\overline{h})| = q^m + 1$, so $|C_G(\overline{g})| \leqslant q^m + 1$. It is straightforward to verify the claim in the very special case where $\varepsilon = -$, $m = 1$ and q is Mersenne, where $|h| = q + 1$ and G is either $\mathrm{PGSp}_2(q)$ or $\mathrm{PDO}^-_2(q)$. □

2.4 Conjugacy in classical groups

To apply our probabilistic method, especially when we compute fixed point ratios in Chapter 3, we will need an understanding of the conjugacy of prime order elements in the relevant almost simple groups. This section provides a short guide to this topic. Let T be a finite simple classical group. The conjugacy classes of elements of prime order in $\mathrm{Aut}(T)$, and the centralisers thereof, are known. This topic is presented in great detail in [17, Chapter 3], which we closely follow in this section.

Let $q = p^f$ where p is prime. With a view towards our applications, we focus on the case where T is $\mathrm{PSp}_n(q)$ (with $n \geqslant 4$) or $\mathrm{P}\Omega_n^\varepsilon(q)$ (with $n \geqslant 7$ and $\varepsilon \in \{+, \circ, -\}$). In this section, we will consider prime order elements contained in $\mathrm{PGSp}_n(q)$ and $\mathrm{PGO}_n^\varepsilon(q)$, and we defer the discussion of prime order elements in $\mathrm{Aut}(\mathrm{PSp}_n(q)) \setminus \mathrm{PGSp}_n(q)$ and $\mathrm{Aut}(\mathrm{P}\Omega_n^\varepsilon(q)) \setminus \mathrm{PGO}_n^\varepsilon(q)$ to Section 2.6.6.

Recall from Section 2.3.1, that an element $g \in \mathrm{GL}_n(q)$ is *semisimple* if $|g|$ is coprime to p. We say that $g \in \mathrm{GL}_n(q)$ is *unipotent* if p divides $|g|$.

2.4.1 Semisimple elements

Let g be an element of $\mathrm{PGSp}_n(q)$ or $\mathrm{PGO}_n^\varepsilon(q)$ of prime order r. Then g is either semisimple or unipotent. In this section, we assume that g is semisimple (so $r \neq p$); unipotent elements will be covered in Section 2.4.2. Much of the work in this section is best attributed to Wall [62]. We will heavily draw on the results of Section 2.3.

Background

We begin with a general discussion of $\mathrm{GL}_n(q)$ before turning to $\mathrm{PGSp}_n(q)$ and $\mathrm{PGO}_n^\varepsilon(q)$.

Let us fix some notation.

Let i be the least positive integer such that r divides $q^i - 1$.

Let $\mathcal{S}_r$ be the set of elements of order r in $\mathbb{F}_{q^i}^\times$.

Let $\sigma \colon \mathbb{F}_{q^i} \to \mathbb{F}_{q^i}$ be the field automorphism defined as $\lambda \mapsto \lambda^q$.

Let $\Lambda_1, \ldots, \Lambda_t$ be the orbits of σ on $\mathcal{S}_r$.

Let λ_j be an element of Λ_j.

Notice that $t = (r-1)/i$ and for each $1 \leqslant j \leqslant t$ we have $|\Lambda_j| = i$. By Lemma 2.3.18, there exists an irreducible element $A_j \in \mathrm{GL}_n(q)$ of order r and whose eigenvalue set is Λ_j.

Define the following set of t-tuples of nonnegative integers:

$$\mathcal{I} = \left\{ (a_1, \ldots, a_t) \mid 0 < i \sum_{j=1}^{t} a_j \leqslant n \right\}.$$

Let $(a_1, \dots, a_t) \in \mathcal{I}$. Write $e = n - i\sum_{j=1}^{t} a_j$ and consider the element

$$A = [A_1^{a_1}, \dots, A_t^{a_t}, I_e] = \underbrace{A_1 \oplus \cdots \oplus A_1}_{a_1 \text{ terms}} \oplus \cdots \oplus \underbrace{A_t \oplus \cdots \oplus A_t}_{a_t \text{ terms}} \oplus I_e$$

that centralises the decomposition

$$U_{1,1} \oplus \cdots \oplus U_{1,a_1} \oplus \cdots \oplus U_{t,1} \oplus \cdots \oplus U_{t,a_t} \oplus W$$

where the restriction of A to $U_{j,k}$ is A_j and W is the 1-eigenspace of A. In particular, A acts irreducibly on each $U_{j,k}$ and the order of A is r.

The eigenvalue multiset of A is

$$\Lambda = \Lambda_1^{a_1} \cup \cdots \cup \Lambda_t^{a_t} \cup \{1\}^e,$$

where superscripts denote multiplicities in a multiset. We often abuse notation and write $A = [\Lambda_1^{a_1}, \dots, \Lambda_t^{a_t}, I_e]$.

The following result [17, Lemma 3.1.7] is a consequence of Theorem 2.3.6.

Lemma 2.4.1. *Each semisimple element of prime order in* $\mathrm{GL}_n(q)$ *is* $\mathrm{GL}_n(q)$*-conjugate to* $[\Lambda_1^{a_1}, \dots, \Lambda_t^{a_t}, I_e]$ *for a unique sequence* $(a_1, \dots, a_t) \in \mathcal{I}$.

Example 2.4.2. We will determine the conjugacy classes of elements of order 5 in $\mathrm{GL}_4(4)$. Since 5 divides $4^2 - 1 = 15$ but not $4 - 1 = 3$, we conclude that $i = 2$. Write

$$\mathcal{S}_5 = \{\lambda, \lambda^2, \lambda^3, \lambda^4\} = \Lambda_1 \cup \Lambda_2$$

where $\Lambda_1 = \{\lambda, \lambda^4\}$ and $\Lambda_2 = \{\lambda^2, \lambda^3\}$ are the orbits of $\sigma\colon (a_{ij}) \mapsto (a_{ij}^4)$ on $\mathcal{S}_5$. Now

$$\mathcal{I} = \{(1,0), (0,1), (2,0), (1,1), (0,2)\}.$$

Therefore, there are five conjugacy classes of elements of order 5 in $\mathrm{GL}_4(4)$, which are represented by the elements

$$[\Lambda_1, I_2] \quad [\Lambda_2, I_2] \quad [\Lambda_1^2] \quad [\Lambda_1, \Lambda_2] \quad [\Lambda_2^2].$$

Write $\langle \alpha \rangle = \mathbb{F}_4^\times$. The minimal polynomials of λ_1 and λ_2 over $\mathbb{F}_4$ are $\chi_1 = X^2 + \alpha X + 1$ and $\chi_2 = X^2 + \alpha^2 X + 1$. Choosing A_j to be the companion matrix of χ_j, we obtain the conjugacy class representatives

$$\begin{pmatrix} 0 & 1 & & \\ 1 & \alpha & & \\ & & 1 & 0 \\ & & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & & \\ 1 & \alpha^2 & & \\ & & 1 & 0 \\ & & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & & \\ 1 & \alpha & & \\ & & 0 & 1 \\ & & 1 & \alpha \end{pmatrix} \begin{pmatrix} 0 & 1 & & \\ 1 & \alpha & & \\ & & 0 & 1 \\ & & 1 & \alpha^2 \end{pmatrix} \begin{pmatrix} 0 & 1 & & \\ 1 & \alpha^2 & & \\ & & 0 & 1 \\ & & 1 & \alpha^2 \end{pmatrix}$$

Semisimple elements of odd prime order

Let $(T, G, \widehat{G})$ be $(\mathrm{PSp}_n(q), \mathrm{PGSp}_n(q), \mathrm{GSp}_n(q))$ or $(\mathrm{P}\Omega^\varepsilon_n(q), \mathrm{PGO}^\varepsilon_n(q), \mathrm{GO}^\varepsilon_n(q))$ and let $Z = Z(\widehat{G}) \cong \mathbb{F}_q^\times$. Let $g \in G$ have odd prime order r. Since $|G : T|$ is a power of two, $r \in T$. By [17, Lemma 3.1.3], there is a unique element $\hat{g} \in \widehat{G}$ of order r such that $\hat{g}Z = g$.

By Lemma 2.2.7, $\hat{g}$ is similar to $\hat{g}^{-1}$, so the multiset of eigenvalues of $\hat{g}$ over $\overline{\mathbb{F}}_p$ must be closed under inversion. Recall the notation established in the previous section. By Lemma 2.3.25, $\Lambda_j^{-1} = \Lambda_j$ if and only if $i = |\Lambda_j|$ is even. If i is odd, then t is even and we will assume that $\Lambda_j^{-1} = \Lambda_{t/2+j}$.

Define two variants on $\mathcal{I}$, both of which are sets of sequences of nonnegative integers

$$\mathcal{I}_{\mathsf{even}} = \left\{ (a_1, \ldots, a_t) \mid 0 < i \sum_{j=1}^{t} a_j \leqslant n \ \text{ and } \ i \sum_{j=1}^{t} a_j < n \text{ if } \varepsilon = (-)^{n/i+1} \right\}$$
$$\mathcal{I}_{\mathsf{odd}} = \left\{ (a_1, \ldots, a_{t/2}) \mid 0 < 2i \sum_{j=1}^{t/2} a_j \leqslant n \ \text{ and } \ 2i \sum_{j=1}^{t/2} a_j < n \text{ if } \varepsilon = - \right\}$$

where $\varepsilon = \circ$ if $T = \mathrm{PSp}_n(q)$ (so the second condition can be ignored in this case).

First assume that i is even and let $(a_1, \ldots, a_t) \in \mathcal{I}_{\mathsf{even}}$ and $e = n - i\sum_{j=1}^{t} a_j$. Lemma 2.3.19 implies that there exists an element $A = [A_1^{a_1}, \ldots, A_t^{a_t}, I_e] \in \widehat{G}$ of order r, which centralises the decomposition

$$U_{1,1} \perp \cdots \perp U_{1,a_1} \perp \cdots \perp U_{t,1} \perp \cdots \perp U_{t,a_t} \perp W$$

where A acts (irreducibly) as A_j on $U_{j,k}$. Moreover, each $U_{j,k}$ is a nondegenerate i-space and W is the 1-eigenspace of A. If $T = \mathrm{P}\Omega^\varepsilon_n(q)$, then each $U_{j,k}$ is minus-type.

Now assume that i is odd and let $(a_1, \ldots, a_{t/2}) \in \mathcal{I}_{\mathsf{odd}}$ and $e = n - 2i\sum_{j=1}^{t/2} a_j$. By Lemma 2.3.24 there exists an element $A = [(A_1 \oplus A_1^{-1})^{a_1}, \ldots, (A_{t/2} \oplus A_{t/2}^{-1})^{a_{t/2}}, I_e] \in \widehat{G}$ of order r, which centralises the decomposition

$$\begin{aligned}(U_{1,1} \oplus U_{1,1}^*) \perp \cdots \perp (U_{1,a_1} \oplus U_{1,a_1}^*) \perp \cdots \\ \perp (U_{t/2,1} \oplus U_{t/2,1}^*) \perp \cdots \perp (U_{t/2,a_{t/2}} \oplus U_{t/2,a_{t/2}}^*) \perp W\end{aligned}$$

where A acts (irreducibly) as A_j on $U_{j,k}$ and $A_j^{-\mathsf{T}}$ on $U_{j,k}^*$. Moreover, each $U_{j,k} \oplus U_{j,k}^*$ is a nondegenerate $2i$-space of which $U_{j,k}$ and $U_{j,k}^*$ are maximal totally singular subspaces, and W is the 1-eigenspace of A.

The following result combines [17, Propositions 3.4.3 and 3.5.4].

Lemma 2.4.3. *Let G be $\mathrm{PGSp}_n(q)$ or $\mathrm{PGO}^\varepsilon_n(q)$. Each semisimple element of odd prime order in G is G-conjugate to*

(i) $[\Lambda_1^{a_1}, \ldots, \Lambda_t^{a_t}, I_e]Z$ *for a sequence $(a_1, \ldots, a_t) \in \mathcal{I}_{\mathsf{even}}$ if i is even*

(ii) $[(\Lambda_1 \cup \Lambda_1^{-1})^{a_1}, \ldots, (\Lambda_{t/2} \cup \Lambda_{t/2}^{-1})^{a_{t/2}}, I_e]Z$ *for a sequence $(a_1, \ldots, a_{t/2}) \in \mathcal{I}_{\mathsf{odd}}$ if i is odd.*

We now record the order of the centraliser in G of a semisimple element of odd prime order (see [17, Appendix B]).

Lemma 2.4.4. *Let G be $\mathrm{PGSp}_n(q)$ or $\mathrm{PGO}^\varepsilon_n(q)$. Let $g \in G$ be a semisimple element of odd prime order. Let Σ be Sp if $G = \mathrm{PGSp}_n(q)$ and O if $G = \mathrm{PGO}^\varepsilon_n(q)$.*

(i) *If i is even and $g = [\Lambda_1^{a_1}, \dots, \Lambda_t^{a_t}, I_e]Z$, then*

$$|C_G(g)| = |\Sigma_e(q)| \cdot \prod_{i=1}^{t} |\mathrm{GU}_{a_i}(q^{i/2})|.$$

(ii) *If i is odd and $g = [(\Lambda_1 \cup \Lambda_1^{-1})^{a_1}, \dots, (\Lambda_{t/2} \cup \Lambda_{t/2}^{-1})^{a_{t/2}}, I_e]Z$, then*

$$|C_G(g)| = |\Sigma_e(q)| \cdot \prod_{i=1}^{t/2} |\mathrm{GL}_{a_i}(q^i)|.$$

Semisimple involutions

Assume that p is odd and let G be $\mathrm{PGSp}_n(q)$ or $\mathrm{PGO}^\varepsilon_n(q)$. The involutions in G are given in [31, Table 4.5.1] and are discussed in detail in [17, Sections 3.4.2 and 3.5.2]. Moreover, the orders of the centralisers in G of these semisimple involutions are given in [17, Appendix B]. The details are rather technical and we will not provide them here.

2.4.2 Unipotent elements

We now consider unipotent elements. As in Section 2.4.1, we will first discuss the general situation in $\mathrm{GL}_n(q)$ before considering the groups $\mathrm{PGSp}_n(q)$ and $\mathrm{PGO}^\varepsilon_n(q)$. Much of the work on unipotent elements is due to Liebeck and Seitz [50].

Background

For $i \geqslant 1$, let J_i be the $i \times i$ (lower triangular) Jordan block with eigenvalues 1. Let $\mathcal{J}$ be the set of nontrivial partitions of n into parts of size at most p; that is,

$$\mathcal{J} = \left\{ (p^{a_p}, \dots, 1^{a_1}) \mid \sum_{i=1}^{p} i a_i = n \text{ and } a_1 < n \right\}.$$

The next result [17, Lemma 3.1.14] is another consequence of Theorem 2.3.6.

Lemma 2.4.5. *Each element of $\mathrm{GL}_n(q)$ of order p is $\mathrm{GL}_n(q)$-conjugate to $[J_p^{a_p}, \dots, J_2^{a_2}, J_1^{a_1}]$ for a unique partition $(p^{a_p}, \dots, 1^{a_1}) \in \mathcal{J}$.*

The following result, which describes the centraliser of a unipotent element of prime order, is proved in [50, Theorem 7.1].

Lemma 2.4.6. *Let $g \in \mathrm{GL}_n(q)$ be the unipotent element $[J_p^{a_p}, \dots, J_2^{a_2}, J_1^{a_1}]$. Then*

$$C_{\mathrm{GL}_n(q)}(g) = Q \prod_{i=1}^{p} \mathrm{GL}_{a_i}(q)$$

where $|Q| = q^\gamma$ and $\gamma = 2\sum_{i<j} i a_i a_j + \sum_{i=1}^{p} (i-1) a_i^2$.

Unipotent elements of odd order

Assume that p is odd. Let $(G, \widehat{G})$ be $(\mathrm{PGSp}_n(q), \mathrm{GSp}_n(q))$ or $(\mathrm{PGO}^\varepsilon_n(q), \mathrm{GO}^\varepsilon_n(q))$ and let $Z = Z(\widehat{G}) \cong \mathbb{F}_q^\times$. In the previous section, we saw that conjugacy of elements of order p in $\mathrm{GL}_n(q)$ is determined by the Jordan form over $\overline{\mathbb{F}}_p$, so the set of conjugacy classes of elements of order p in $\mathrm{GL}_n(q)$ is in bijection with $\mathcal{J}$. However, the Jordan form is not enough to determine conjugacy of elements of order p in $\widehat{G}$. Therefore, a technical modification has to be made, and we summarise how this is done. We will define two variants on $\mathcal{J}$. In both definitions, it should be understood that $\sum_{i=1}^p ia_i = n$ and $a_1 < n$.

First assume that $G = \mathrm{PGSp}_n(q)$. Define the following set of signed partitions of n

$$\mathcal{J}_\mathsf{s} = \left\{ (p^{a_p}, \varepsilon_{p-1}(p-1)^{a_{p-1}}, \dots, \varepsilon_2 2^{a_2}, 1^{a_1}) \mid a_i \text{ even if } i \text{ odd}, \ \ \varepsilon_i = \pm \right\}.$$

Let $(p^{a_p}, \varepsilon_{p-1}(p-1)^{a_{p-1}}, \dots, \varepsilon_2 2^{a_2}, 1^{a_1}) \in \mathcal{J}_\mathsf{s}$. In [17, Section 3.4.3], a particular element $[J_p^{a_p}, J_{p-1}^{\varepsilon_{p-1}, a_{p-1}}, \dots, J_2^{\varepsilon_2, a_2}, J_1^{a_1}] \in \widehat{G}$ is defined which has Jordan form $[J_p^{a_p}, J_{p-1}^{a_{p-1}}, \dots, J_2^{a_2}, J_1^{a_1}]$.

Now assume that $G = \mathrm{PGO}^\varepsilon_n(q)$ and let δ be the discriminant of the quadratic form defining G (see Remark 2.2.2). Define the following set of labelled partitions of n

$$\mathcal{J}_\mathsf{o} = \left\{ (\delta_p p^{a_p}, (p-1)^{a_{p-1}}, \dots, 2^{a_2}, \delta_1 1^{a_1}) \mid a_i \text{ even if } i \text{ even}, \ \ \delta_i \in \{\square, \boxtimes\}, \ \ \prod_{i \text{ odd}} \delta_i = \delta \right\}.$$

Let $(\delta_p p^{a_p}, (p-1)^{a_{p-1}}, \dots, 2^{a_2}, \delta_1 1^{a_1}) \in \mathcal{J}_\mathsf{o}$. An element $[J_p^{\delta_p, a_p}, J_{p-1}^{a_{p-1}}, \dots, J_2^{a_2}, J_1^{\delta_1, a_1}] \in \widehat{G}$ is defined in [17, Section 3.5.3], which has Jordan form $[J_p^{a_p}, J_{p-1}^{a_{p-1}}, \dots, J_2^{a_2}, J_1^{a_1}]$.

The signs and discriminants indicate the types of nondegenerate subspaces stabilised by these elements, see [17, Sections 3.4.3 and 3.5.3] for a precise statement.

Lemma 2.4.7. *Let $q = p^f$ be odd. Let G be $\mathrm{PGSp}_n(q)$ or $\mathrm{PGO}^\varepsilon_n(q)$. Each element of G of order p is G-conjugate to*

(i) $[J_p^{a_p}, \dots, J_2^{\varepsilon_2, a_2}, J_1^{a_1}]Z$ *for a unique* $(p^{a_p}, \dots, \varepsilon_2 2^{a_2}, 1^{a_1}) \in \mathcal{J}_\mathsf{s}$ *if* $G = \mathrm{PGSp}_n(q)$

(ii) $[J_p^{\delta_p, a_p}, \dots, J_2^{a_2}, J_1^{\delta_1, a_1}]Z$ *for a unique* $(\delta_p p^{a_p}, \dots, 2^{a_2}, \delta_1 1^{a_1}) \in \mathcal{J}_\mathsf{o}$ *if* $G = \mathrm{PGO}^\varepsilon_n(q)$.

We refer the reader to [17, Lemmas 3.4.11 and 3.5.13] for a description of the centraliser in G of an element of order p, which is somewhat similar to Lemma 2.4.6.

Unipotent involutions

Now let $p = 2$. Let n be even and let G be $\mathrm{Sp}_n(q)$ or $\mathrm{O}^\pm_n(q)$. Again, the Jordan form does not determine conjugacy of elements of order p in G, and we will adopt the notation of Aschbacher and Seitz [3, Section 7]. For each $1 \leqslant s \leqslant n/2$, Aschbacher and Seitz define elements a_s and c_s if s is even and b_s if s is odd, all of which have Jordan form $[J_2^s, J_1^{n-2s}]$. These elements are described explicitly in [17, Sections 3.4.4 and 3.5.4].

Lemma 2.4.8. *Let n be even and let $q = 2^f$. Let G be $\mathrm{Sp}_n(q)$ or $\mathrm{O}^\pm_n(q)$. Each involution in G with Jordan form $[J_2^s, J_1^{n-2s}]$ is conjugate to b_s if s is odd, or exactly one of a_s or c_s if s is even.*

2.5 Maximal subgroups of classical groups

Determining the maximal subgroups of almost simple groups is a problem with a long history, with the classification of the maximal subgroups of $\mathrm{PSL}_2(q)$ typically attributed to Dickson [25] in 1901. The Classification added impetus to this project and this remains an active area of research in its own right. This section is dedicated to the subgroup structure of almost simple classical groups, since an understanding of this topic will be essential in Chapters 4 and 5.

Theorem 2.5.1, due to Aschbacher, is one of the most important theorems in this thesis, since it provides a framework for describing the maximal subgroups of classical groups. Roughly, it states that if H is a maximal subgroup of an almost simple classical group G, then either H is the stabiliser of a natural geometric structure on the natural module V for $\mathrm{soc}(G)$, or H is an almost simple group and the embedding $\mathrm{soc}(H) \leqslant \mathrm{PGL}(V)$ is afforded by an absolutely irreducible representation on V of a cover of $\mathrm{soc}(H)$. This is analogous to the description of the maximal subgroups of symmetric groups by the O'Nan–Scott Theorem (see [63, Theorem 2.4] and also [48]).

2.5.1 Aschbacher's theorem

Let G be an almost simple classical group and let $V = \mathbb{F}_q^n$ be the natural module for $\mathrm{soc}(G)$. Theorem 2.5.1 was proved by Aschbacher [1], but Aschbacher excluded the case when $\mathrm{soc}(G) = \mathrm{P}\Omega_8^+(q)$ and G contains a triality automorphism, and the theorem was proved in this special case by Kleidman [42].

Theorem 2.5.1 (Aschbacher's Subgroup Theorem)**.** *Let G be an almost simple classical group and let H be a maximal subgroup of G not containing* $\mathrm{soc}(G)$*. Then H belongs to one of the subgroup collections $\mathcal{C}_1, \ldots, \mathcal{C}_8, \mathcal{S}, \mathcal{N}$.*

Regarding Theorem 2.5.1, notice that the subgroups of G that contain $\mathrm{soc}(G)$ correspond to subgroups of $G/\mathrm{soc}(G) \leqslant \mathrm{Out}(\mathrm{soc}(G))$, which is a well-known soluble group. This explains our focus on maximal subgroups not containing $\mathrm{soc}(G)$.

Geometric subgroups

The collections $\mathcal{C}_1, \ldots, \mathcal{C}_8$ contain the *geometric subgroups*, and each such collection corresponds to a different geometric structure on the natural module for $\mathrm{soc}(G)$. We adopt the definition of each $\mathcal{C}_i$ given in [43, Section 4.i], which differs slightly from Aschbacher's original definition. These eight collections are summarised in Table 2.2 and a brief discussion of $\mathcal{C}_i$ is given [17, Section 2.6.2.i]. (The $\mathcal{C}_6$ subgroups, which do not relate to geometric structures that we have already introduced, will hardly feature in what follows.)

Each $\mathcal{C}_i$ collection is a union of *types* of geometric subgroup. The type of a subgroup is a rough indication of both its group theoretic structure and the geometric structure it stabilises; this notion is formally introduced in [43, p.58].

Table 2.2: Geometric subgroups

	structure stabilised	rough description in $\mathrm{GL}_n(q)$
$\mathcal{C}_1$	nondegenerate or tot. sing. subspace	maximal parabolic
$\mathcal{C}_2$	$V = \bigoplus_{i=1}^k V_i$ where $\dim V_i = a$	$\mathrm{GL}_a(q) \wr S_k$ with $n = ak$
$\mathcal{C}_3$	prime degree field extension of $\mathbb{F}_q$	$\mathrm{GL}_a(q^k).k$ with $n = ak$ for prime k
$\mathcal{C}_4$	tensor product $V = V_1 \otimes V_2$	$\mathrm{GL}_a(q) \circ \mathrm{GL}_b(q)$ with $n = ab$
$\mathcal{C}_5$	prime degree subfield of $\mathbb{F}_q$	$\mathrm{GL}_n(q_0)$ with $q = q_0^k$ for prime k
$\mathcal{C}_6$	symplectic-type r-group	$(C_{q-1} \circ r^{1+2a}).\mathrm{Sp}_{2a}(r)$ with $n = r^a$
$\mathcal{C}_7$	$V = \bigotimes_{i=1}^k V_i$ where $\dim V_i = a$	$(\mathrm{GL}_a(q) \circ \cdots \circ \mathrm{GL}_a(q)).S_k$ with $n = a^k$
$\mathcal{C}_8$	nondegenerate classical form	$\mathrm{GSp}_n(q)$, $\mathrm{GO}_n^\varepsilon(q)$, $\mathrm{GU}_n(q^{\frac{1}{2}})$

The Main Theorem in [43, Chapter 3] establishes the structure, conjugacy and, when $n \geqslant 13$, maximality of each geometric subgroup of each almost simple classical group. If $n \leqslant 12$, then complete information on the maximal subgroups of almost simple classical groups is given in the very useful book [7] (and the foreword to this book tells an interesting story about this topic).

Let us present an example.

Example 2.5.2. The $\mathcal{C}_2$ subgroups are the irreducible imprimitive subgroups. Here we study them for almost simple groups G with socle $\mathrm{PSp}_{14}(q)$ using [43, Main Theorem]. Fix the basis $\mathcal{B} = (e_1, f_1, \ldots, e_7, f_7)$ from (2.4).

(i) The group G has exactly two types of $\mathcal{C}_2$ subgroups. One is $\mathrm{Sp}_2(q) \wr S_7$, where the summands in the stabilised decomposition are nondegenerate 2-spaces, say $\langle e_i, f_i \rangle$ for $1 \leqslant i \leqslant 7$. The other is $\mathrm{GL}_7(q)$, where the summands are maximal totally singular subspaces, say $\langle e_1, \ldots, e_7 \rangle$ and $\langle f_1, \ldots, f_7 \rangle$.

(ii) The exact structure of the geometric subgroups is given in [43, Chapter 4]. For example, [43, Proposition 4.2.10] implies that if q is odd, $G = \mathrm{PGSp}_{14}(q)$ and H has type $\mathrm{Sp}_2(q) \wr S_7$, then $H = ((\mathrm{Sp}_2(q)^7{:}\langle\delta\rangle)/\langle -I_{14}\rangle){:}S_7$, where δ is the diagonal matrix $[\alpha, 1, \ldots, \alpha, 1]$ for a generator α of $\mathbb{F}_q^\times$ and where S_7 permutes the $\mathrm{Sp}_2(q)$ factors and centralises δ.

We now turn to conjugacy of geometric subgroups. Write $T = \mathrm{soc}(G)$ and let H be a maximal geometric subgroup of G. Let $\mathcal{H} = \{H_1, \ldots, H_c\}$ be a set of representatives of the c distinct T-classes of subgroups of T of the same type as H. In the terminology of [43, Chapter 3], for each $1 \leqslant i \leqslant c$, let $H_{G,i}$ be the G-associate of H_i. In particular, $H_{G,i}$ is a geometric subgroup of G of the same type as H_i and $H_i \leqslant H_{G,i}$. See [43, Section 3.1] for a precise definition.

For $x \in \mathrm{Aut}(T)$ write $\ddot{x}$ for $Tx \in \mathrm{Out}(T)$, and for $X \subseteq \mathrm{Aut}(T)$ write $\ddot{X} = \{\ddot{x} \mid x \in X\}$. There is a natural action of $\mathrm{Out}(T)$ on the set $\mathcal{H}$, and the permutation representation $\pi\colon \mathrm{Out}(T) \to S_c$ associated to this action is described in [43, Tables 3.5.A–3.5.G]. As a consequence of the proof of [43, Lemma 3.2.2(iii)], for $G \leqslant A \leqslant \mathrm{Aut}(T)$, the groups $H_{G,i}$ and $H_{G,j}$ are A-conjugate if and only if H_i and H_j are in the same $\pi(\ddot{A})$-orbit.

The following example highlights the key ideas.

Example 2.5.3. The $\mathcal{C}_5$ subgroups are the subfield subgroups, which we now study for $T = \mathrm{PSp}_n(q)$ and $G = \mathrm{PGSp}_n(q)$ when $n \geqslant 6$ and $q = p^f$.

A subfield subgroup of G or T has type $\mathrm{Sp}_n(q^{1/r})$ for a prime r dividing f. Inspecting [43, Table 3.5C], we see that $c = 1$, unless q is odd and $r = 2$, in which case $c = 2$. If $c = 1$, then there is a unique T-class of subgroups of type $\mathrm{Sp}_n(q^{1/r})$, so there is certainly a unique G-class.

Now assume that q is odd and $r = 2$. In this case, $c = 2$. This means that there are exactly two T-classes of subgroups of T of type $\mathrm{Sp}_n(q^{1/2})$, represented by H_1 and H_2, but $H_1^g = H_2$ for some $g \in \mathrm{Aut}(T)$. Inspecting [43, Table 3.5G], we see that $\ddot{g} \in \ker \pi$ if and only if $g \in \mathrm{PSp}_n(q)$. Therefore, H_1 and H_2 are in the same $\pi(\ddot{G})$-orbit, so there is a unique G-class of subgroups of G of type $\mathrm{Sp}_n(q^{1/2})$. This completes our example.

The following example highlights the two main types of obstacles to maximality.

Example 2.5.4. These two examples continue Examples 2.5.2 and 2.5.3, respectively.

(i) Let G be an almost simple group with socle $\mathrm{PSp}_{14}(q)$. Let H be a subgroup of G of type $\mathrm{Sp}_2(q) \wr S_7$. Then it turns out that H is a maximal subgroup of G unless $q = 2$. If $q = 2$, then $G = \mathrm{Sp}_{14}(2)$ and $H = \mathrm{Sp}_2(2) \wr S_7 = \mathrm{O}_2^-(2) \wr S_7$, and in this case H is contained in $\mathrm{O}_{14}^-(2)$ which is a maximal $\mathcal{C}_8$ subgroup of G.

(ii) Let $T = \mathrm{PSp}_n(q)$ and $G = \mathrm{PGSp}_n(q)$ for $n \geqslant 14$ and $q = p^f$, where p is odd and f is even. It turns out that a subgroup of either T or G of type $\mathrm{Sp}_n(q^{1/2})$ is isomorphic to $\mathrm{PGSp}_n(q^{1/2})$ (this is related to the fact that $c = 2$ in this case). The subgroups of this type are maximal in T, but evidently any subgroup of G of this type is contained in T and is consequently not maximal in G.

Non-geometric subgroups

We will now introduce the families $\mathcal{S}$ and $\mathcal{N}$ of *non-geometric subgroups* that feature in Theorem 2.5.1. If $H \leqslant G$ is contained in the collection $\mathcal{S}$, then H is almost simple with socle H_0 and the embedding $H_0 \leqslant G$ is afforded by an absolutely irreducible representation $\rho\colon \widehat{H}_0 \to \mathrm{GL}(V)$ for some quasisimple extension $\widehat{H}_0$ of H_0. The full definition of $\mathcal{S}$ involves further conditions, which ensure that $\mathcal{S}$ is disjoint from $\bigcup_{i=1}^{8} \mathcal{C}_i$ and this can be found on [43, p.3]. It is critical to realise that the particular subgroups which arise is $\mathcal{S}$ are in general not known.

When $\mathrm{soc}(G)$ is $\mathrm{PSL}_n(q)$ (with $n \geqslant 3$), $\mathrm{Sp}_4(q)$ (with $p = 2$) or $\mathrm{P\Omega}_8^+(q)$, then $\mathrm{Aut}(\mathrm{soc}(G))$ is not contained in $\mathrm{P\Gamma L}(V)$. Consequently, there are more exotic almost simple groups with these socles and the subgroup structure of these groups is accordingly more intricate. More precisely, when $H \leqslant G$ and $H \cap \mathrm{soc}(G)$ is not maximal in $\mathrm{soc}(G)$, then H is said to be a *novelty subgroup*. If $G \not\leqslant \mathrm{P\Gamma L}(V)$, then there may exist a maximal subgroup $H \leqslant G$ such that $H \cap \mathrm{soc}(G)$ is not only non-maximal but is not contained in $\cup_{i=1}^{8} \mathcal{C}_i \cup \mathcal{S}$. The definition of $\mathcal{C}_1$ was adapted in [43] to avoid this issue when $\mathrm{soc}(G) = \mathrm{PSL}_n(q)$. However, when $\mathrm{soc}(G)$ is $\mathrm{Sp}_4(q)$ or $\mathrm{P\Omega}_8^+(q)$, these additional novelty subgroups arise in a final collection $\mathcal{N}$, which is described in [17, Table 5.9.1].

2.5.2 Elements of maximal subgroups

For this section, write $V = \mathbb{F}_q^n$ and $\overline{V} = V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_p$, where $q = p^f$. The main theorem of [35] classifies the maximal subgroups of $\mathrm{GL}_n(q)$ that contain an element whose order is divisible by a primitive prime divisor of $q^k - 1$ for $k > \frac{n}{2}$. The following version is a special case of [34, Theorem 2.2] (the exceptions in part (iv) are given in [34, Table 1]).

Theorem 2.5.5. *Let $n \geqslant 3$ and $k > \frac{n}{2}$. Let $g \in \mathrm{GL}(V)$ with $|g| \in \mathrm{ppd}(q, k)$ and $|g| > 2k + 1$. Let $H \leqslant \mathrm{GL}(V)$ be an irreducible subgroup containing g. Then one of the following holds*

(i) *H is a subfield subgroup*

(ii) *H is a field extension subgroup of degree dividing (n, k)*

(iii) *H contains $\mathrm{SL}(V)$, $\mathrm{SU}(V)$, $\mathrm{Sp}(V)$ or $\Omega(V)$*

(iv) *$n \leqslant 9$ and H is one of a small number of exceptions.*

A wealth of practical information on elements of geometric subgroups can be found in [17, Chapter 5]. We present some here, beginning with $\mathcal{C}_2$ subgroups [17, Lemma 5.2.6].

Lemma 2.5.6. *Let r be prime and let $\mathcal{D}$ be $\overline{V} = V_1 \oplus \cdots \oplus V_r$ where $\dim V_i = a$ for $1 \leqslant i \leqslant r$. Assume that $x \in \mathrm{GL}(\overline{V})_{\mathcal{D}}$ has order r and transitively permutes the subspaces in $\mathcal{D}$.*

(i) *If $r \neq p$, then each rth root of unity occurs as an eigenvalue of x with multiplicity a.*

(ii) *If $r = p$, then x has Jordan form $[J_p^a]$.*

The next result [17, Lemma 5.3.2] concerns field extension $\mathcal{C}_3$ subgroups.

Lemma 2.5.7. *Let k be a prime divisor of n, let $a = n/k$ and let $\pi\colon \mathrm{GL}_a(q^k).k \to \mathrm{GL}_n(q)$ be a field extension embedding. Let $r \neq p$ be prime and let $x \in \mathrm{GL}_a(q^k).k$ have order r.*

(i) *If $x \in \mathrm{GL}_a(q^k)$ and has eigenvalues $\lambda_1, \ldots, \lambda_a$ over $\overline{\mathbb{F}}_p$, then $\pi(x)$ has eigenvalues $\Lambda_1 \cup \cdots \cup \Lambda_a$ where $\Lambda_i = \{\lambda_i^{q^j} \mid 0 \leqslant j < k\}$.*

(ii) *If $x \notin \mathrm{GL}_a(q^k)$, then $r = k$ and each rth root of unity occurs as an eigenvalue of $\pi(x)$ with multiplicity a.*

Let us record some consequences of Lemma 2.5.7.

Corollary 2.5.8. *Let G be $\mathrm{PSp}_{2m}(q)$ or $\mathrm{PSO}^{\pm}_{2m}(q)$ and let g lift to $g_1 \oplus \cdots \oplus g_t \oplus I_\ell$ where $g_1, \ldots, g_t$ have type $(2d)^{\varepsilon}_q$ for $d > 1$ and have distinct eigenvalues.*

(i) *If d is odd, then g is not contained in the base of a subgroup of type $\mathrm{Sp}_m(q^2)$ (where m is even) or $\mathrm{O}^{v}_m(q^2)$ (where $v \in \{+,-\}$ if m is even and $v = \circ$ if m is odd).*

(ii) *If $\varepsilon \neq (-)^d$, then g is not contained in the base of a subgroup of type $\mathrm{GU}_m(q)$.*

Proof. Let $\pi\colon H = B.2 \to G$ be the field extension embedding in question, where B is the base of H. Write $|g| = r$. For a contradiction, suppose that $g \in B$.

First assume that $\varepsilon = +$, so we may assume that d is odd. Let Λ be the set of nontrivial eigenvalues of g. If $g = \pi(x)$ for $x \in B$, then, by Lemma 2.5.7(i), $\Lambda = \Lambda_0 \cup \Lambda_0^q$, where Λ_0 is the set of eigenvalues of x. Since x is an element defined over $\mathbb{F}_{q^2}$ we know that $\Lambda_0^{q^2} = \Lambda_0$. However, the elements of Λ_0 have order r, where $r \in \mathrm{ppd}(q,d)$. Since d is odd, $\Lambda_0^{q^2} = \Lambda_0^q$. Thus, every eigenvalue of g occurs with multiplicity at least two, which contradicts the distinctness of the eigenvalues of g.

Next assume that $\varepsilon = -$. Let Λ_i be the set of $2d$ distinct eigenvalues of g_i. For now consider part (i), so we may assume that d is odd. Then $r \in \mathrm{ppd}(q,2d)$ and there are two $\mu \mapsto \mu^{q^2}$ orbits on Λ_i, say Λ_{i1} and $\Lambda_{i2} = \Lambda_{i1}^q = \Lambda_{i1}^{-1}$. By Lemma 2.5.7(i), without loss of generality, the eigenvalues of g as an element of $\mathrm{GL}_m(q^2)$ are $\cup_{i=1}^t \Lambda_{i1}$, which is not closed under inversion (see Lemma 2.3.25), which is a contradiction to Lemma 2.2.7(i).

Continuing to assume $\varepsilon = -$, now consider part (ii). We may now assume that d is even. Therefore, $r \in \mathrm{ppd}(q,d)$ and again write Λ_{i1} and $\Lambda_{i2} = \Lambda_{i1}^{-q}$ for the two $\mu \mapsto \mu^{q^2}$ orbits on Λ_i. Then, by Lemma 2.5.7(i), without loss of generality, the eigenvalues of g as an element of $\mathrm{GU}_m(q)$ are $\cup_{i=1}^t \Lambda_{i1}$, which is not closed under the map $\mu \mapsto \mu^{-q}$, which is a contradiction to [17, Proposition 3.3.1]. This completes the proof. □

Combining Corollary 2.5.8 with Lemma 2.3.36 gives the following.

Corollary 2.5.9. *Let G be $\mathrm{PSp}_{2m}(q)$ or $\mathrm{PSO}^{\pm}_{2m}(q)$. Let $g \in G$ have type $(2d)^{\eta}_{q_0} \perp I_\ell$ for $q_0^e = q$.*

(i) *If d is odd, then g is not contained in the base of a subgroup of type $\mathrm{Sp}_m(q^2).2$ or $\mathrm{O}^{v}_m(q^2).2$.*

(ii) *If d is odd and $\eta = +$; or d is even, $\eta = -$ and e is odd; or d is odd, $\eta = -$ and e is even, then g is not contained in the base of a subgroup of type $\mathrm{GU}_m(q)$.*

The following straightforward result concerns tensor product decompositions.

Lemma 2.5.10. *Let $x = x_1 \otimes x_2 \in \mathrm{GL}(\overline{V})$ centralise a decomposition $\overline{V} = V_1 \otimes V_2$. Assume that x has order coprime to p, and let $\lambda_1, \ldots, \lambda_a$ and $\mu_1, \ldots, \mu_b$ be the eigenvalues of x_1 on V_1 and x_2 on V_2. Then the eigenvalues of x on $\overline{V}$ are $\lambda_i\mu_j$ for $1 \leqslant i \leqslant a$ and $1 \leqslant j \leqslant b$.*

Table 2.3: Exceptions in Theorem 2.5.14 when $q > p$

T	$H \cap T$	conditions
$P\Omega_8^+(q)$	$\Omega_7(q)$	$p > 2$
$\Omega_8^+(q)$	$Sp_6(q)$	$p = 2$
$\Omega_7(q)$	$G_2(q)$	$p > 2$
$Sp_6(q)$	$G_2(q)$	$p = 2$
$PSp_6(p^2)$	J_2	$p > 2$
$PSL_6^\varepsilon(q)$	$PSL_3^\varepsilon(q)$	$p > 2$

The next result on $\mathcal{C}_7$ subgroups [17, Lemma 5.7.2] is analogous to Lemma 2.5.6.

Lemma 2.5.11. *Let r be prime and let $\mathcal{D}$ be $\overline{V} = V_1 \otimes \cdots \otimes V_r$ where $\dim V_i = a$ for $1 \leqslant i \leqslant r$. Assume that $x \in \mathrm{GL}(\overline{V})_{\mathcal{D}}$ has order r and transitively permutes the subspaces in $\mathcal{D}$.*

(i) *If $r \neq p$, then each nontrivial rth root of unity occurs as an eigenvalue of x with multiplicity $\frac{n-a}{r}$ and 1 occurs with multiplicity $\frac{n-a}{r} + a$.*

(ii) *If $r = p$, then x has Jordan form $[J_p^{(n-a)/p}, J_1^a]$.*

For the final results of this section, we introduce the following standard piece of notation.

Notation 2.5.12. For $x \in \mathrm{PGL}(V)$, let $\hat{x}$ be a preimage of x in $\mathrm{GL}(V)$ and define $\nu(x)$ as the codimension of the largest eigenspace of $\hat{x}$ on $\overline{V}$.

The following is [52, Lemma 3.7].

Lemma 2.5.13. *Let $x = x_1 \otimes x_2 \in \mathrm{GL}(\overline{V})$ have prime order and centralise a decomposition $\overline{V} = V_1 \otimes V_2$. Then $\nu(x) \geqslant \max\{\nu(x_2)\dim V_1, \nu(x_1)\dim V_2\}$.*

We conclude this section by presenting a theorem of Guralnick and Saxl [36, Theorem 7.1], which provides valuable information about the groups in the collection $\mathcal{S}$.

Theorem 2.5.14. *Let G be an almost simple classical group with socle T and natural module $V = \mathbb{F}_q^n$ satisfying $n \geqslant 6$. Let $H \leqslant G$ be contained in $\mathcal{S}$. Then one of the following holds*

(i) *$\nu(x) > \max\{2, \frac{\sqrt{n}}{2}\}$ for all $x \in H \cap \mathrm{PGL}(V)$*

(ii) *q is prime, $H \cap T$ is an alternating group and V is the fully deleted permutation module*

(iii) *$n \leqslant 10$ and $H \cap T$ is one of a small number of exceptions.*

A convenient list of the exceptions in part (iii) is given in [14, Table 2.3]. We record in Table 2.3 the exceptions in (iii) when q is not prime. See [43, p.185–187] for a good account of the fully deleted permutation module appearing in part (ii).

2.6 Algebraic groups

The finite simple groups of Lie type arise as the fixed points of algebraic groups under Steinberg endomorphisms. This section briefly introduces how, and for a full account we refer the reader to [31, Chapters 1 and 2] and [53]. This perspective allows us to exploit Shintani descent, which is described in Section 2.7.

2.6.1 Simple algebraic groups

We begin by establishing terminology. Fix a prime number p. By an *algebraic group* we always mean a linear algebraic group over $\overline{\mathbb{F}}_p$. Moreover, by a *simple algebraic group* we mean an algebraic group which is simple as an algebraic group (see [31, Definition 1.7.1] for a definition); any such group is connected but need not be simple as an abstract group. A morphism $\pi\colon X \to Y$ of algebraic groups is an *isogeny* if π is surjective and $\ker\pi$ is finite; if π is an isogeny and X is connected, then $\ker\pi \leqslant Z(X)$. We say that X and Y are *isogenous* if there exists an isogeny $X \to Y$ or $Y \to X$.

The following theorem, which is a special case of Chevalley's classification of semisimple algebraic groups (see [31, Theorem 1.10.4]), establishes that simple algebraic groups are characterised, up to isogeny, by their associated root system. It is therefore useful to recall that the indecomposable root systems are labelled

$$\mathsf{A}_m\,(m \geqslant 1), \quad \mathsf{B}_m\,(m \geqslant 2), \quad \mathsf{C}_m\,(m \geqslant 2), \quad \mathsf{D}_m\,(m \geqslant 4), \quad \mathsf{E}_6,\ \mathsf{E}_7,\ \mathsf{E}_8, \quad \mathsf{F}_4, \quad \mathsf{G}_2.$$

Theorem 2.6.1 (Classification of Simple Algebraic Groups)**.** *Let Φ be an indecomposable root system. Then there exist simple algebraic groups Φ^{sc} and Φ^{ad}, unique up to isomorphism of algebraic groups, such that*

(i) *Φ is the root system of Φ^{sc} and Φ^{ad}*

(ii) *$Z(\Phi^{\mathsf{sc}})$ is finite and $Z(\Phi^{\mathsf{ad}}) = 1$*

(iii) *if X is any simple algebraic group with root system Φ, then there exist isogenies*

$$\Phi^{\mathsf{sc}} \to X \to \Phi^{\mathsf{ad}}$$

(iv) *if X, Y are isogenous simple algebraic groups, then the root systems of X and Y are isomorphic, or $\mathrm{char}(F) = 2$ and the root systems of X and Y are B_m and C_m.*

The exception featured in Theorem 2.6.1(iv) is genuine, see Lemma 2.6.2.

For an indecomposable root system Φ, the groups Φ^{sc} and Φ^{ad} (from Theorem 2.6.1) are called the *simply connected* and *adjoint* groups of type Φ. Moreover, for a simple algebraic group X with root system Φ, we say that the *simply connected* and *adjoint* versions of X are $X^{\mathsf{sc}} = \Phi^{\mathsf{sc}}$ and $X^{\mathsf{ad}} = \Phi^{\mathsf{ad}}$.

Table 2.4: Simple classical algebraic groups

Φ	Φ^{sc}	Φ^{ad}	$Z(\Phi^{\mathsf{sc}})$	p	m
A_m $(m \geqslant 1)$	SL_{m+1}	PSL_{m+1}	$C_{(m+1)_{p'}}$		
B_m $(m \geqslant 2)$	SO_{2m+1}	SO_{2m+1}	1	2	
	Spin_{2m+1}	SO_{2m+1}	C_2	odd	
C_m $(m \geqslant 2)$	Sp_{2m}	PSp_{2m}	$C_{(p-1,2)}$		
D_m $(m \geqslant 4)$	Ω_{2m}	Ω_{2m}	1	2	
	Spin_{2m}	PSO_{2m}	C_4	odd	odd
			$C_2 \times C_2$	odd	even

2.6.2 Simple classical algebraic groups

The simple classical algebraic groups are described in Table 2.4 (see [31, Theorem 1.10.7]), where we adopt the notation introduced in Section 2.2 (but we omit reference to the ambient field $\overline{\mathbb{F}}_p$). Recall that $\mathrm{SO}_n = \mathrm{O}_n \cap \mathrm{SL}_n$, and when n and p are even Ω_n is the subgroup of SO_n containing the products of an even number of reflections (equivalently, Ω_n is the connected component of the identity of SO_n).

The groups of type B_m and D_m merit further attention in odd characteristic. Accordingly, assume that $p \neq 2$ and let $(\Phi, n) \in \{(\mathsf{B}_m, 2m+1), (\mathsf{D}_m, 2m)\}$. In this case, the simply connected group Φ^{sc} is the *spin group* Spin_n and there is an isogeny $\mathrm{Spin}_n \to \mathrm{SO}_n$ with a kernel $K \leqslant Z(\mathrm{Spin}_n)$ of order two. We will not require any further information about spin groups, but for completeness we record that if m is even, then there exists the *half-spin group* HSpin_{2m} such that if $Z \leqslant Z(\mathrm{Spin}_{2m})$ is one of the two order two subgroups other than K, then Spin_{2m}/K and HSpin_{2m} are isomorphic as algebraic groups.

Let us now address the exception in Theorem 2.6.1(iv). The groups $\mathrm{SO}_{2m+1}(\overline{\mathbb{F}}_2)$ and $\mathrm{Sp}_{2m}(\overline{\mathbb{F}}_2)$ are nonisomorphic algebraic groups, but the following lemma demonstrates that they are isogenous. We will exploit this isogeny in Proposition 4.3.13.

Lemma 2.6.2. *There exists a bijective isogeny* $\mathrm{SO}_{2m+1}(\overline{\mathbb{F}}_2) \to \mathrm{Sp}_{2m}(\overline{\mathbb{F}}_2)$.

Proof. Let $W = \overline{\mathbb{F}}_2^{2m+1}$ be equipped with the nonsingular quadratic form Q, with bilinear form $(\cdot,\cdot)$, defined in (2.7) with respect to the basis $(e_1, f_1, \ldots, e_m, f_m, x)$. Let $Y \cong \mathrm{SO}_{2m+1}(\overline{\mathbb{F}}_2)$ be the isometry group of Q. The restriction of $(\cdot,\cdot)$ to $V = \langle e_1, \ldots, f_m \rangle$ is the symplectic form defined in (2.4); let X be the isometry group of this restriction. With respect to the bases in (2.4) and (2.7), define $\pi\colon X \to Y$ as

$$\pi((a_{ij})) = \begin{pmatrix} a_{11} & \cdots & a_{1(2m)} & \sum_{j=1}^{m} (a_{1(2j-1)} a_{1(2j)})^{\frac{1}{2}} \\ \vdots & \ddots & \vdots & \vdots \\ a_{(2m)1} & \cdots & a_{(2m)(2m)} & \sum_{j=1}^{m} (a_{(2m)(2j-1)} a_{(2m)(2j)})^{\frac{1}{2}} \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

Notice that for $1 \leqslant i \leqslant 2m$

$$\sum_{j=1}^{m} a_{i(2j-1)}a_{i(2j)} = Q\left(\sum_{j=1}^{m}(a_{i(2j-1)}e_j + a_{i(2j)}f_j)\right).$$

To see that π is well-defined, let $u, v \in \{e_1, \ldots, f_m\}$ and $g \in X$, and note that for $h = \pi(g)$

$$\begin{aligned}
(uh, vh) &= (ug + Q(ug)^{\frac{1}{2}}x, vg + Q(vg)^{\frac{1}{2}}x) = (ug, vg) = (u, v)\\
(uh, xh) &= (ug + Q(ug)^{\frac{1}{2}}x, x) = 0 = (u, x)\\
Q(uh) &= Q(ug + Q(ug)^{\frac{1}{2}}x) = Q(ug) + Q(ug)^{\frac{1}{2}}(ug, x) + Q(ug)Q(x) = 0 = Q(u)\\
Q(xh) &= Q(x).
\end{aligned}$$

Evidently π is injective. For surjectivity, let $h \in Y$. Then there exists $g \in X$ such that for all $u \in \{e_1, \ldots, f_m\}$ there exists $\lambda_u \in \overline{\mathbb{F}}_2$ satisfying $uh = ug + \lambda_u x$. Now

$$Q(u) = Q(uh) = Q(ug + \lambda_u x) = Q(ug) + \lambda_u^2,$$

so $\lambda_u = (Q(u) + Q(ug))^{\frac{1}{2}}$. Therefore, $uh = u(\pi(g))$. Moreover, since $\langle x \rangle$ is the radical of $(\cdot, \cdot)$ (see (2.2)), $xh = \lambda x$ and $\lambda = 1$ since

$$1 = Q(x) = Q(xh) = Q(\lambda x) = \lambda^2 Q(x).$$

Therefore, $h = \pi(g)$. Consequently, π is a well-defined bijection.

Let us now show that π is an abstract group homomorphism. Let $A = (a_{ij})$ and $B = (b_{ij})$ be elements of X. It is a matter of routine to show that

$$\pi(AB) = \begin{pmatrix} AB & C \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \pi(A)\pi(B) = \begin{pmatrix} AB & D \\ 0 & 1 \end{pmatrix}$$

where $C = (c_i)$ and $D = (d_i)$ are the $2m \times 1$ matrices defined as

$$\begin{aligned}
c_i &= \sum_{j=1}^{m}\sum_{s=1}^{2m} a_{is}(b_{s(2j-1)}b_{s(2j)})^{\frac{1}{2}} + \sum_{j=1}^{m}(a_{i(2j-1)}a_{i(2j)})^{\frac{1}{2}}\\
d_i &= \sum_{j=1}^{m}\sum_{s=1}^{2m} a_{is}(b_{s(2j-1)}b_{s(2j)})^{\frac{1}{2}} + \sum_{\{s,t\}\in S}(a_{is}a_{it})^{\frac{1}{2}}\sum_{k=1}^{m}(b_{s(2k-1)}b_{t(2k)} + b_{t(2k-1)}b_{s(2k)})^{\frac{1}{2}}
\end{aligned}$$

and S is the set of 2-subsets of $\{1, \ldots, 2m\}$. Write $(u_1, \ldots, u_{2m}) = (e_1, f_1, \ldots, e_m, f_m)$. For all $\{s, t\} \in S$,

$$\sum_{k=1}^{m}(b_{s(2k-1)}b_{t(2k)} + b_{t(2k-1)}b_{s(2k)}) = (u_sB, u_tB).$$

Since B is an isometry of $(\cdot, \cdot)$,

$$(u_sB, u_tB) = (u_s, u_t) = \begin{cases} 1 & \text{if } \{s, t\} = \{2j-1, 2j\} \text{ for some } 1 \leqslant j \leqslant m \\ 0 & \text{otherwise.} \end{cases}$$

Together with the above expressions for c_i and d_i, this proves that $C = D$ and consequently that π is a homomorphism.

In summary, π is an abstract group isomorphism. Although π is not a morphism of algebraic groups, evidently π^{-1} is. Therefore, $\pi^{-1}\colon Y \to X$ is a bijective isogeny. □

2.6.3 Finite simple groups of Lie type

A *Steinberg endomorphism* of an algebraic group X is a bijective morphism $\sigma\colon X \to X$ whose fixed point subgroup

$$X_\sigma = \{x \in X \mid x^\sigma = x\}$$

is finite. Now assume that X is a simple algebraic group. By a theorem of Steinberg [59, Theorem 10.13] an endomorphism σ of X is a Steinberg endomorphism if and only if σ is not an automorphism of X as an algebraic group. In particular, we may consider the semidirect product $X{:}\langle\sigma\rangle$ where $\sigma^{-1}x\sigma = x^\sigma = \sigma(x)$ for all $x \in X$.

Theorem 2.6.3 captures how the finite simple groups of Lie type are obtained from simple algebraic groups and Steinberg endomorphisms (see [31, Theorem 2.2.6]). Example 2.6.11, and Section 2.6.5 more generally, provides concrete applications of this theorem. Here, we write $O^{p'}(G)$ for the smallest normal subgroup N of G such that G/N is a p'-group (equivalently, $O^{p'}(G)$ is the subgroup of G generated by the p-elements).

Theorem 2.6.3. *Let X be a simple algebraic group and let σ be a Steinberg endomorphism of X. Write $G = O^{p'}(X_\sigma)$ and similarly define $G^{\mathsf{sc}} = O^{p'}((X^{\mathsf{sc}})_\sigma)$ and $G^{\mathsf{ad}} = O^{p'}((X^{\mathsf{ad}})_\sigma)$. Then*

(i) *there exist surjective homomorphisms $G^{\mathsf{sc}} \to G \to G^{\mathsf{ad}}$ with central kernels*

(ii) *$G^{\mathsf{sc}}/Z(G^{\mathsf{sc}}) \cong G^{\mathsf{ad}}$ and $Z(G^{\mathsf{ad}}) = 1$*

(iii) *$G^{\mathsf{sc}} = (X^{\mathsf{sc}})_\sigma$.*

The group G^{ad} defined in Theorem 2.6.3 is typically a finite simple group (see [31, Theorem 2.2.7(a)]) and these are the *finite simple groups of Lie type*.

With the notation from Theorem 2.6.3, define the *innerdiagonal group* of G^{ad} as

$$\mathrm{Inndiag}(G^{\mathsf{ad}}) = (X^{\mathsf{ad}})_\sigma. \tag{2.16}$$

It is interesting that $\mathrm{Inndiag}(G^{\mathsf{ad}})/G^{\mathsf{ad}} \cong Z(G^{\mathsf{sc}})$ (see [31, Theorem 2.5.12]).

Remark 2.6.4. Different authors use the term Steinberg endomorphism differently. In [31], the term is used more generally to refer to any surjective endomorphism with a finite fixed point subgroup; injectivity is not assumed. However, if X is a simple algebraic group, then any surjective endomorphism of X is bijective [31, Proposition 1.15.3], so our terminology agrees in this case. In contrast, in [53] the term is used in a more restrictive manner (for what is known as a Frobenius endomorphism in [31]), but again the terminology is consistent for simple algebraic groups (see [31, Theorem 2.1.11] and [53, Theorem 21.5]).

2.6.4 The Lang–Steinberg Theorem

We now record the key theorem that allows one to transfer information from algebraic groups to the finite simple groups of Lie type [59, Theorem 10.13].

Theorem 2.6.5 (Lang–Steinberg Theorem)**.** *Let X be a connected algebraic group and let σ be a Steinberg endomorphism of X. The map $L\colon X \to X$ defined as $L(x) = xx^{-\sigma}$ is surjective.*

The following observation will be used repeatedly in the following section.

Corollary 2.6.6. *Let X be a connected algebraic group and let σ be a Steinberg endomorphism of X. The map $L'\colon X \to X$ defined as $L'(x) = xx^{-\sigma^{-1}}$ is surjective.*

Proof. Let $g \in X$. By Theorem 2.6.5, there exists $x \in X$ such that $g^{-\sigma} = xx^{-\sigma}$. Consequently, $g = xx^{-\sigma^{-1}}$ and L' is surjective. □

Let us record some applications of Theorem 2.6.5, which highlight its significance.

Proposition 2.6.7. *Let X be a connected algebraic group and let σ be a Steinberg endomorphism of X. The coset $X\sigma$ of $X{:}\langle\sigma\rangle$ is exactly the conjugacy class σ^X.*

Proof. For all $g \in X$ we have $\sigma^g = g^{-1}\sigma g = g^{-1}g^{\sigma^{-1}}\sigma$, so $\sigma^X \subseteq X\sigma$. For the reverse inclusion, fix $y \in X$. Corollary 2.6.6 implies that there exists $x \in X$ such that $y = xx^{-\sigma^{-1}}$. Consequently, $\sigma^{x^{-1}} = xx^{-\sigma^{-1}}\sigma = y\sigma$. This implies that $X\sigma = \sigma^X$. □

We refer the reader to [46, Section 1.3] for a proof of the following important consequence of Theorem 2.6.5, together with several applications. Here, for a group G and $\sigma \in \mathrm{Aut}(G)$, two elements $g, h \in G$ are σ-conjugate if there exists $x \in G$ such that $g = x^{-1}hx^{\sigma}$.

Theorem 2.6.8. *Let X be a connected algebraic group and let σ be a Steinberg endomorphism of X. Let $X{:}\langle\sigma\rangle$ act on a nonempty set Ω and assume that X acts transitively on Ω.*

(i) *The set $\Omega_\sigma = \{\omega \in \Omega \mid \omega\sigma = \omega\}$ is nonempty.*

(ii) *If G_α is closed for some $\alpha \in \Omega$, then for all $\omega \in \Omega_\sigma$, there exists a bijection between the X_σ-orbits on Ω_σ and the σ-conjugacy classes in $G_\omega / G_\omega^\circ$.*

2.6.5 Finite simple classical groups

We now identify classical finite simple groups of Lie type with classical groups introduced in Section 2.2. We follow the account in [31, Section 2.7]. For this section, we fix $f \geqslant 1$ and $q = p^f$.

Definition 2.6.9. The *standard Frobenius endomorphism* with respect to the basis $\mathcal{B}$ for $\overline{\mathbb{F}}_p^n$ is the endomorphism $\varphi_{\mathcal{B}}$ of $\mathrm{GL}_n(\overline{\mathbb{F}}_p)$ defined as $(a_{ij}) \mapsto (a_{ij}^p)$, where the elements of $\mathrm{GL}_n(\overline{\mathbb{F}}_p)$ are written as matrices with respect to $\mathcal{B}$.

Remark 2.6.10. Regarding Definition 2.6.9, if the basis $\mathcal{B}$ is understood, then we omit reference to it. We will identify φ with the map induced on φ-stable subgroups of $\mathrm{GL}_n(\overline{\mathbb{F}}_p)$ and quotients of such subgroups by φ-stable normal subgroups.

The following example gives a detailed discussion of linear groups.

Example 2.6.11. Let $m \geqslant 1$ and consider the groups of type $\Phi = \mathsf{A}_m$. Write $n = m + 1$, fix a basis $\mathcal{B}$ for $\overline{\mathbb{F}}_p^n$ and write $\sigma = \varphi_{\mathcal{B}}^f$. If $n = 2$ and $f = 1$, then assume that $p \geqslant 5$, since $\mathrm{PSL}_2(2) \cong S_3$ and $\mathrm{PSL}_2(3) \cong A_4$ are not simple.

Let $X^{\mathsf{sc}} = \Phi^{\mathsf{sc}} = \mathrm{SL}_n(\overline{\mathbb{F}}_p)$. Evidently

$$(X^{\mathsf{sc}})_\sigma = \{(a_{ij}) \in \mathrm{SL}_n(\overline{\mathbb{F}}_p) \mid (a_{ij}^q) = (a_{ij})\} = \mathrm{SL}_n(q).$$

If N is a proper normal subgroup of $\mathrm{SL}_n(q)$, then $N \leqslant Z(\mathrm{SL}_n(q))$, so the order of N divides $(n, q-1)$ and therefore $\mathrm{SL}_n(q)/N$ is not a p'-group. This implies that

$$G^{\mathsf{sc}} = O^{p'}((X^{\mathsf{sc}})_\sigma) = O^{p'}(\mathrm{SL}_n(q)) = \mathrm{SL}_n(q) = (X^{\mathsf{sc}})_\sigma,$$

as claimed in Theorem 2.6.3(iii). (Alternatively, note that $\mathrm{SL}_n(q)$ is generated by the set of transvections [2, 13.7], which have order p, so $O^{p'}(\mathrm{SL}_n(q)) = \mathrm{SL}_n(q)$.)

Let $X^{\mathsf{ad}} = \Phi^{\mathsf{ad}} = \mathrm{PSL}_n(\overline{\mathbb{F}}_p)$. Write $Z = Z(\mathrm{GL}_n(\overline{\mathbb{F}}_p))$. For each $\mu \in \overline{\mathbb{F}}_p$, there exists $\lambda \in \overline{\mathbb{F}}_p$ such that $\lambda^n = \mu$ and hence there exists $\lambda I_n \in Z$ such that $\det(\lambda I_n) = \mu$. Consequently,

$$X^{\mathsf{ad}} = \mathrm{PSL}_n(\overline{\mathbb{F}}_p) = (\mathrm{SL}_n(\overline{\mathbb{F}}_p)Z)/Z = \mathrm{GL}_n(\overline{\mathbb{F}}_p)/Z = \mathrm{PGL}_n(\overline{\mathbb{F}}_p).$$

Moreover,

$$(X^{\mathsf{ad}})_\sigma = \{(a_{ij})Z \mid (a_{ij}) \in \mathrm{GL}_n(\overline{\mathbb{F}}_p) \text{ and } (a_{ij}^q) = (a_{ij})\} = \mathrm{PGL}_n(q).$$

Every nontrivial normal subgroup of $\mathrm{PGL}_n(q)$ contains $\mathrm{PSL}_n(q)$. Since $\mathrm{PGL}_n(q)/\mathrm{PSL}_n(q)$ has order $(n, q-1)$, and is therefore a p'-group, $O^{p'}(\mathrm{PGL}_n(q)) = \mathrm{PSL}_n(q)$, which is a finite simple group.

Now $Z(G^{\mathsf{ad}}) = Z(\mathrm{PSL}_n(q)) = 1$ and

$$G^{\mathsf{sc}}/Z(G^{\mathsf{sc}}) = \mathrm{SL}_n(q)/Z(\mathrm{SL}_n(q)) \cong \mathrm{PSL}_n(q) = G^{\mathsf{ad}},$$

as claimed in Theorem 2.6.3(ii).

Finally, we record that

$$\mathrm{Inndiag}(\mathrm{PSL}_n(q)) = \mathrm{Inndiag}(G^{\mathsf{ad}}) = (X^{\mathsf{ad}})_\sigma = \mathrm{PGL}_n(q).$$

This completes the example on groups of type A_m.

The following results on symplectic groups and odd-dimensional orthogonal groups can be proved as in Example 2.6.11 and we omit the proofs. In the statements, we refer to the bases $\mathcal{B}$ in (2.4) and (2.7).

Lemma 2.6.12. *Let $n \geqslant 4$ be even and $\varphi = \varphi_{\mathcal{B}}$.*

(i) *If $X = \mathrm{Sp}_n(\overline{\mathbb{F}}_p)$, then $X_{\varphi^f} = \mathrm{Sp}_n(q)$.*

(ii) *If $X = \mathrm{PSp}_n(\overline{\mathbb{F}}_p)$, then $X_{\varphi^f} = \mathrm{PGSp}_n(q)$.*

Therefore, for even $n \geqslant 4$,

$$\mathrm{Inndiag}(\mathrm{PSp}_n(q)) = \mathrm{PGSp}_n(q). \tag{2.17}$$

Lemma 2.6.13. *Let $n \geqslant 7$ be odd, p be odd and $\varphi = \varphi_{\mathcal{B}}$. If $X = \mathrm{SO}_n(\overline{\mathbb{F}}_p)$, then $X_{\varphi^f} = \mathrm{SO}_n(q)$.*

Therefore, for odd $n \geqslant 7$ and odd q,

$$\mathrm{Inndiag}(\Omega_n(q)) = \mathrm{SO}_n(q). \tag{2.18}$$

We now turn to even-dimensional orthogonal groups. Here we will see the significance of the groups $\mathrm{PDO}_n^{\pm}(q)$ introduced in Section 2.2.6. Lemma 2.6.14 concerns plus-type groups (see (2.5) for the basis $\mathcal{B}^+$).

Lemma 2.6.14. *Let $n \geqslant 8$ be even and $\varphi = \varphi_{\mathcal{B}^+}$.*

(i) *If $p = 2$ and $X = \Omega_n(\overline{\mathbb{F}}_2)$, then $X_{\varphi^f} = \Omega_n^+(q)$.*

(ii) *If p is odd and $X = \mathrm{SO}_n(\overline{\mathbb{F}}_p)$, then $X_{\varphi^f} = \mathrm{SO}_n^+(q)$.*

(iii) *If p is odd and $X = \mathrm{PSO}_n(\overline{\mathbb{F}}_p)$, then $X_{\varphi^f} = \mathrm{PDO}_n^+(q)$.*

Proof. First assume that $p = 2$. Since $X = \Omega_n(\overline{\mathbb{F}}_2) \leqslant \mathrm{O}_n(\overline{\mathbb{F}}_2)$, we have $X_{\varphi^f} \leqslant \mathrm{O}_n^+(q)$. Since $\Omega_n(\overline{\mathbb{F}}_2)$ does not contain any reflections, we must have $X_{\varphi^f} \leqslant \Omega_n^+(q)$. However, $|\,\mathrm{O}_n(\overline{\mathbb{F}}_2) : \Omega_n(\overline{\mathbb{F}}_2)| = 2$, so $|\,\mathrm{O}_n^+(q) : X_{\varphi^f}| \leqslant 2$. Therefore, $X_{\varphi^f} = \Omega_n^+(q)$. This proves (i).

Now assume that p is odd. Part (ii) is clear. For (iii), let $X = \mathrm{PSO}_{2m}(\overline{\mathbb{F}}_p)$ and write $Z = Z(\mathrm{GO}_n(\overline{\mathbb{F}}_p)) = \{\lambda I_n \mid \lambda \in \overline{\mathbb{F}}_p^{\times}\}$. Since $\det(\lambda I_n) = \lambda^n = \tau(\lambda I_n)^{n/2}$, we have $Z \leqslant \mathrm{DO}_n(\overline{\mathbb{F}}_p)$. Moreover, for each $\mu \in \overline{\mathbb{F}}_p$, there exists $\lambda \in \overline{\mathbb{F}}_p$ such that $\lambda^2 = \mu$ and hence there exists $\lambda I_n \in Z$ such that $\tau(\lambda I_n) = \mu$ and $\det(\lambda I_n) = \mu^{n/2}$. Consequently, $\mathrm{SO}_n(\overline{\mathbb{F}}_p)Z = \mathrm{DO}_n(\overline{\mathbb{F}}_p)$ and

$$X = \mathrm{PSO}_n(\overline{\mathbb{F}}_p) = (\mathrm{SO}_n(\overline{\mathbb{F}}_p)Z)/Z = \mathrm{DO}_n(\overline{\mathbb{F}}_p)/Z = \mathrm{PDO}_n(\overline{\mathbb{F}}_p), \tag{2.19}$$

whence $X_{\varphi^f} = \mathrm{PDO}_n^+(q)$. □

For minus-type groups, we need to consider a different sort of Steinberg endomorphism.

Definition 2.6.15. Let n be even. With respect to $\mathcal{B}^+$, define $r \in \mathrm{O}_n^+(p)$ as the element

$$r = I_{2m-2} \perp \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

that centralises the decomposition $\langle e_1, \ldots, f_{m-1}\rangle \perp \langle e_m, f_m\rangle$.

Remark 2.6.16. Regarding Definition 2.6.15, note that $r \in \mathrm{O}_n(\overline{\mathbb{F}}_p) \setminus \Omega_n(\overline{\mathbb{F}}_p)$. We routinely identify r with the involutory automorphism of the algebraic group $\Omega_n(\overline{\mathbb{F}}_p)$ it induces by conjugation. We will write r for the image of r in $\mathrm{PO}_n(\overline{\mathbb{F}}_p)$.

Lemma 2.6.17. *Let $n \geqslant 8$ be even and $\varphi = \varphi_{\mathcal{B}^+}$. Then there exists an inner automorphism Ψ of $\mathrm{GL}_n(\overline{\mathbb{F}}_p)$ such that the following hold.*

(i) *If $p = 2$ and $X = \Omega_n(\overline{\mathbb{F}}_2)$, then $\Psi(X_{r\varphi^f}) = \Omega_n^-(q)$.*

(ii) *If p is odd and $X = \mathrm{SO}_n(\overline{\mathbb{F}}_p)$, then $\Psi(X_{r\varphi^f}) = \mathrm{SO}_n^-(q)$.*

(iii) *If p is odd and $X = \mathrm{PSO}_n(\overline{\mathbb{F}}_p)$, then $\Psi(X_{r\varphi^f}) = \mathrm{PDO}_n^-(q)$.*

Proof. Let $V = \overline{\mathbb{F}}_p^n$ be equipped with the quadratic form Q, with bilinear form $(\cdot,\cdot)$, defined in (2.5) with respect to the basis $\mathcal{B}^+ = (e_1, f_1, \ldots, e_m, f_m)$, where $n = 2m$. Let Ψ be the endomorphism of $\mathrm{GL}_n(\overline{\mathbb{F}}_p)$ induced by conjugation by the element $A = I_{n-2} \perp A'$ that centralises $\langle e_1, \ldots, f_{m-1}\rangle \perp \langle e_m, f_m\rangle$, where

$$A' = \begin{pmatrix} \xi & \xi^{-1} \\ \xi^{-1} & \xi \end{pmatrix}$$

and where $\xi \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ satisfies $\xi^q = \xi^{-1}$.

Write $u_m = e_m A$ and $v_m = f_m A$. It is straightforward to check that $Q(u_m) = Q(v_m) = 1$ and $(u_m, v_m) = \xi^2 + \xi^{-2}$, so, without loss of generality, we may assume that $\mathcal{B}^+ A$ is the basis $\mathcal{B}^-$ defined in (2.6).

Let $\sigma_\varepsilon = (\varphi_{\mathcal{B}^\varepsilon})^f$. A straightforward calculation yields $AA^{-(q)} = r$ where $A = (a_{ij})$ and $A^{(q)} = (a_{ij}^q)$. Consequently, $\Psi(X_{r\sigma_+}) = A^{-1}X_{r\sigma_+}A = X_{\sigma_-}$ for any subgroup $X \leqslant \mathrm{GL}_n(\overline{\mathbb{F}}_p)$. Let V^ε be the $\mathbb{F}_q$-span of $\mathcal{B}^\varepsilon$. Then (V^ε, Q) is the ε-type formed space from (2.5) or (2.6). Therefore, if $X = \mathrm{SO}_n(\overline{\mathbb{F}}_p)$, then $X_{\sigma_+} = \mathrm{SO}_n^+(q)$ and $\Psi(X_{r\sigma_+}) = X_{\sigma_-} = \mathrm{SO}_n^-(q)$.

We are now in the position to prove the main claims of the lemma.

First assume that $p = 2$ and $X = \Omega_n(\overline{\mathbb{F}}_2)$. We know that $\Psi(Y_{r\varphi^f}) = \mathrm{O}_n^-(q)$, where $Y = \mathrm{O}_n(\overline{\mathbb{F}}_2)$. Since Ψ^{-1} maps the reflections in $\mathrm{O}_n^-(q)$ to reflections in $Y_{r\varphi^f}$ and X contains no reflections, we conclude that $\Psi(X_{r\varphi^f}) = \Omega_n^-(q)$. This proves (i).

Now assume that p is odd. We have already proved (ii). For (iii), let $X = \mathrm{PSO}_n(\overline{\mathbb{F}}_p)$. We recorded in (2.19) that $X = \mathrm{PSO}_n(\overline{\mathbb{F}}_p) = \mathrm{PDO}_n(\overline{\mathbb{F}}_p)$. The above discussion now implies that $\Psi(X_{r\varphi^f}) = \mathrm{PDO}_n^-(q)$. This completes the proof. □

In light of Lemmas 2.6.14 and 2.6.17, with a slight abuse of notation for minus-type groups, for even $n \geqslant 8$,

$$\mathrm{Inndiag}(\mathrm{P}\Omega_n^\pm(q)) = \mathrm{PDO}_n^\pm(q). \tag{2.20}$$

Let us conclude this section by recording our notation for finite spin groups. Assume that p is odd and $X = \mathrm{Spin}_n(\overline{\mathbb{F}}_p)$. If $n \geqslant 8$ is even, then we write $X_{\varphi^f} = \mathrm{Spin}_n^+(q)$ and $X_{r\varphi^f} = \mathrm{Spin}_n^-(q)$. Similarly, if $n \geqslant 7$ is odd, then we write $X_{\varphi^f} = \mathrm{Spin}_n(q)$.

2.6.6 Automorphisms

Let $q = p^f$ where p is prime and $f \geqslant 1$. In this section, we describe the automorphism groups of the finite simple symplectic and orthogonal groups. This should be compared with the brief discussion in Section 2.2.7 and the detailed analysis in Sections 4.1 and 5.1. In particular, we tie up a loose end from Section 2.4 by discussing the conjugacy classes of elements of prime order in $\mathrm{Aut}(\mathrm{PSp}_n(q)) \setminus \mathrm{PGSp}_n(q)$ and $\mathrm{Aut}(\mathrm{P}\Omega^\epsilon_n(q)) \setminus \mathrm{PGO}^\epsilon_n(q)$.

Viewing the finite simple groups of Lie type from the perspective of algebraic groups provides a uniform means of describing their automorphisms. This is described in full generality in [31, Section 2.5]. In Lemmas 2.6.18, 2.6.21 and 2.6.25, we record the consequences of [31, Theorem 2.5.12] for the groups we are interested in. The terminology that we introduce follows [31, Definition 2.5.13].

In this section, φ is the standard Frobenius endomorphism $(a_{ij}) \mapsto (a_{ij}^p)$ with respect to the appropriate basis from (2.4), (2.5) or (2.7).

Lemma 2.6.18.

(i) *If $T = \mathrm{PSp}_n(q)$ where $n \geqslant 4$ is even and $(n, p) \neq (4, 2)$, then*

$$\mathrm{Aut}(T) = \mathrm{Inndiag}(T){:}\langle\varphi\rangle = \mathrm{P\Gamma Sp}_n(q).$$

(ii) *If $T = \Omega_n(q)$ where $n \geqslant 7$ is odd, then*

$$\mathrm{Aut}(T) = \mathrm{Inndiag}(T){:}\langle\varphi\rangle = \mathrm{P\Gamma O}_n(q).$$

(iii) *If $T = \mathrm{P}\Omega^+_n(q)$ where $n \geqslant 10$ is even, then*

$$\mathrm{Aut}(T) = \mathrm{Inndiag}(T){:}(\langle r\rangle \times \langle\varphi\rangle) = \mathrm{P\Gamma O}^+_n(q).$$

Definition 2.6.19. Let T be a simple group featured in Lemma 2.6.18.

(i) A *field automorphism* of T is an $\mathrm{Aut}(T)$-conjugate of an element of $\langle\varphi\rangle$.

(ii) If $T = \mathrm{P}\Omega^+_n(q)$, then a *graph automorphism* of T is an $\mathrm{Aut}(T)$-conjugate of an element of $\mathrm{Inndiag}(T){:}\langle r\rangle \setminus \mathrm{Inndiag}(T) = \mathrm{PGO}^+_n(q) \setminus \mathrm{PDO}^+_n(q)$.

(iii) If $T = \mathrm{P}\Omega^+_n(q)$, then a *graph-field automorphism* of T is an $\mathrm{Aut}(T)$-conjugate of an element of $\langle r, \varphi\rangle \setminus (\langle r\rangle \cup \langle\varphi\rangle)$.

The next result follows from [17, Propositions 3.4.15, 3.5.20 and 3.5.21].

Lemma 2.6.20. *Let (G, Γ) be $(\mathrm{PGSp}_n(q), \mathrm{P\Gamma Sp}_n(q))$ for $n \geqslant 4$, $(\mathrm{PGO}_n(q)\ \mathrm{P\Gamma O}_n(q))$ for $n \geqslant 7$ or $(\mathrm{PGO}^+_n(q), \mathrm{P\Gamma O}^+_n(q))$ for $n \geqslant 10$. A prime order element in $\Gamma \setminus G$ is G-conjugate to*

(i) *a field automorphism φ^i for some $1 \leqslant i \leqslant f$, or*

(ii) *the graph-field automorphism $r\varphi^{f/2}$ (assuming that $G = \mathrm{PGO}^+_n(q)$ and f is even).*

We now turn to minus-type orthogonal groups. Let $n \geqslant 8$. Recall from Lemma 2.6.17 that $\mathrm{PDO}_n^-(q) = \Psi(X_{r\varphi^f})$, where $X = \mathrm{PSO}_n(\overline{\mathbb{F}}_p)$ and Ψ is an inner automorphism of $\mathrm{GL}_n(\overline{\mathbb{F}}_p)$. Define $\psi\colon \Psi(X) \to \Psi(X)$ as

$$\psi = \Psi \circ \varphi \circ \Psi^{-1}. \tag{2.21}$$

Lemma 2.6.21. *Let $T = \mathrm{P}\Omega_n^-(q)$ where $n \geqslant 8$. Then*

$$\mathrm{Aut}(T) = \mathrm{PDO}_n^-(q){:}\langle\psi\rangle = \mathrm{P\Gamma O}_n^-(q).$$

Definition 2.6.22. Let $T = \mathrm{P}\Omega_n^-(q)$ where $n \geqslant 8$.

(i) A *field automorphism* of T is an $\mathrm{Aut}(T)$-conjugate of an odd order element of $\langle\psi\rangle$.

(ii) A *graph automorphism* of T is an element $g \in \mathrm{Aut}(T)$ such that $\pi(g)$ has even order, where $\pi\colon \mathrm{Aut}(T) \to \mathrm{Aut}(T)/\mathrm{Inndiag}(T)$ is the natural quotient map.

Lemma 2.6.23. *Let $T = \mathrm{P}\Omega_n^-(q)$ where $n \geqslant 8$. Then ψ is an order $2f$ graph automorphism of T satisfying $\psi^f = r$.*

Proof. Write $X = \mathrm{PSO}_n(\overline{\mathbb{F}}_p)$. Evidently, φ is an automorphism of $X_{r\varphi^f}$ of order $2f$ and φ^f induces conjugation by r. Consequently, $\psi = \Psi \circ \varphi \circ \Psi^{-1}$ is an order $2f$ automorphism of $\Psi(X_{r\varphi^f}) = \mathrm{PDO}_n^-(q)$ and hence also of $T = \mathrm{P}\Omega_n^-(q)$. Moreover, $\psi^f = \Psi \circ \varphi^f \circ \Psi^{-1}$ induces conjugation by $\Psi(r) = r$ on T. This proves the result. □

The following is a special case of [17, Proposition 3.5.20].

Lemma 2.6.24. *Let $n \geqslant 8$ be even. Each prime order element in $\mathrm{P\Gamma O}_n^-(q) \setminus \mathrm{PGO}_n^-(q)$ is $\mathrm{PGO}_n^-(q)$-conjugate to a field automorphism ψ^i for some $1 \leqslant i \leqslant 2f$.*

It remains to consider $T = \mathrm{Sp}_4(2^f)$ and $T = \mathrm{P}\Omega_8^+(q)$. We will not discuss the latter case in detail since we will not prove our main theorems for almost simple groups with socle $\mathrm{P}\Omega_8^+(q)$, but we refer the reader to Remark 5.1.15 for some further details.

Now let $T = \mathrm{Sp}_4(2^f)$. The group T has an exceptional automorphism ρ, which satisfies $\rho^2 = \varphi$ (see [23, Proposition 12.3.3]).

Lemma 2.6.25. *Let $T = \mathrm{Sp}_4(2^f)$. Then $\mathrm{Aut}(T) = \langle T, \rho\rangle$.*

Definition 2.6.26. Let $T = \mathrm{Sp}_4(2^f)$ where $n \geqslant 4$.

(i) A *field automorphism* of T is an $\mathrm{Aut}(T)$-conjugate of an element of $\langle\varphi\rangle$.

(ii) A *graph-field automorphism* of T is an $\mathrm{Aut}(T)$-conjugate of ρ^i for odd $0 < i < 2f$.

Lemma 2.6.27. *Let $T = \mathrm{Sp}_4(2^f)$. Each prime order element in $\mathrm{Aut}(T) \setminus T$ is T-conjugate to*

(i) *a field automorphism φ^i for some $1 \leqslant i \leqslant f$, or*

(ii) *the graph-field automorphism ρ^f (assuming that f is even).*

2.7 Shintani descent

We now describe Shintani descent. We begin with the basic setup in Section 2.7.1, where we follow the account given in [18, Section 2.6]. In Section 2.7.2 we present three new technical lemmas, which are crucial to how we manipulate Shintani maps in our proofs, and Section 2.7.3 records some further applications. Section 2.7.4 introduces a new result (Lemma 2.7.13) that allows us to use Shintani descent more flexibly.

2.7.1 Introduction

Let X be a connected algebraic group and let σ be a Steinberg endomorphism of X. We consider the semidirect product $X{:}\langle\sigma\rangle$ where $\sigma^{-1}x\sigma = x^{\sigma} = \sigma(x)$ for all $x \in X$. For $e > 1$ the subgroup X_{σ^e} is σ-stable, so σ restricts to an automorphism $\widetilde{\sigma} = \sigma|_{X_{\sigma^e}}$ of X_{σ^e}. Therefore, we may also consider the finite semidirect product $X_{\sigma^e}{:}\langle\widetilde{\sigma}\rangle$, where $g^{\widetilde{\sigma}} = \widetilde{\sigma}(g) = \sigma(g)$ for all $g \in X_{\sigma^e}$, noting that $|\widetilde{\sigma}| = e$.

A *Shintani map* of (X, σ, e) is a map of conjugacy classes of the form

$$F\colon \{(g\widetilde{\sigma})^{X_{\sigma^e}} \mid g \in X_{\sigma^e}\} \to \{x^{X_\sigma} \mid x \in X_\sigma\} \quad (g\widetilde{\sigma})^{X_{\sigma^e}} \mapsto (a^{-1}(g\widetilde{\sigma})^e a)^{X_\sigma}$$

where $a \in X$ satisfies $g = aa^{-\sigma^{-1}}$ (which exists by Corollary 2.6.6). We often abuse notation by writing $F(g\widetilde{\sigma})$ for a representative of the X_σ-class $F((g\widetilde{\sigma})^{X_{\sigma^e}})$.

The following theorem establishes the main properties of the Shintani map. This result was first proved in this form by Kawanaka in [41, Lemma 2.2], building on the work of Shintani who introduced the key ideas in [58, Lemmas 2.1 and 2.6]. We follow the proof given in [18, Lemma 2.13].

Theorem 2.7.1 (Shintani Descent)**.** *Let X be a connected algebraic group, let σ be a Steinberg endomorphism of X and let $e > 1$. Let F be a Shintani map of (X, σ, e).*

(i) *The map F is a well-defined bijection, which does not depend on the choice of $a \in X$.*

(ii) *If $g \in X_{\sigma^e}$ then $C_{X_\sigma}(F(g\widetilde{\sigma})) = a^{-1}C_{X_{\sigma^e}}(g\widetilde{\sigma})a$.*

Proof. Let $g \in X_{\sigma^e}$ and write $g = aa^{-\sigma^{-1}}$. First note that

$$a^{-1}(g\sigma)^e a = a^{-1}gg^{\sigma^{-1}}\cdots g^{\widetilde{\sigma}^{-(e-1)}}a = a^{-1}(aa^{-\sigma^{-1}})(a^{\sigma^{-1}}a^{-\sigma^{-2}})\cdots(a^{\sigma^{-(e-1)}}a^{-\sigma^{-e}})a = a^{-\sigma^{-e}}a.$$

Since $g = aa^{-\sigma^{-1}} \in X_{\sigma^e}$ we know that $aa^{-\sigma^{-1}} = (aa^{-\sigma^{-1}})^{\sigma^{-e}} = a^{\sigma^{-e}}a^{-\sigma^{-(e+1)}}$, whence $a^{-\sigma^{-e}}a = a^{-\sigma^{-(e+1)}}a^{\sigma^{-1}} = (a^{-\sigma^{-e}}a)^{\sigma^{-1}}$, so $a^{-\sigma^{-e}}a \in X_\sigma$.

Let $h\widetilde{\sigma}$ be X_{σ^e}-conjugate to $g\widetilde{\sigma}$. Fix $k \in X_{\sigma^e}$ such that $h\widetilde{\sigma} = k^{-1}(g\widetilde{\sigma})k$ and consequently $h = k^{-1}gk^{-\sigma^{-1}}$. Writing $g = aa^{-\sigma^{-1}}$, we obtain $h = (k^{-1}a)(k^{-1}a)^{-\sigma^{-1}}$, whence

$$(k^{-1}a)^{-1}(h\widetilde{\sigma})^e(k^{-1}a) = a^{-1}k(h\widetilde{\sigma})^e k^{-1}a = a^{-1}(g\widetilde{\sigma})^e a.$$

Therefore, F does not depend on the choice of representative of the X_{σ^e}-class.

Write $g = aa^{-\sigma^{-1}} = bb^{-\sigma^{-1}}$. Then $a^{-1}b = a^{-\sigma^{-1}}b^{\sigma^{-1}} = (a^{-1}b)^{\sigma^{-1}}$, so $a^{-1}b \in X_\sigma$ and

$$b^{-1}(g\widetilde{\sigma})^e b = (a^{-1}b)^{-1}(a^{-1}(g\widetilde{\sigma})^e a)(a^{-1}b),$$

so F is independent of the choice of a. Therefore, F is a well-defined function.

To see that F is surjective, let $x \in X_\sigma$ and write $x^{-1} = bb^{-\sigma^{-e}}$. Then $x = a^{-\sigma^{-e}}a$ where $a = b^{-1}$. As we argued in the first paragraph, $a^{-1}(aa^{-\sigma^{-1}}\widetilde{\sigma})^e a = x$ and $aa^{-\sigma^{-1}} \in X_{\sigma^e}$ since $a^{-\sigma^{-e}}a \in X_\sigma$. We will complete the proof that F is bijective after proving (ii).

Turning to (ii), let $z \in C_{X_{\sigma^e}}(g\widetilde{\sigma})$. Then $a^{-1}za$ centralises $a^{-1}(g\widetilde{\sigma})^e a$. Since $z \in C_{X_{\sigma^e}}(g\widetilde{\sigma})$, we know that $zg\widetilde{\sigma} = g\widetilde{\sigma}z$, which implies that $z^{\sigma^{-1}} = g^{-1}zg$. Therefore,

$$(a^{-1}za)^{\sigma^{-1}} = a^{-\sigma^{-1}}g^{-1}zga^{\sigma^{-1}} = a^{-1}gg^{-1}zgg^{-1}a = a^{-1}za.$$

Therefore, $a^{-1}za \in X_\sigma$, so $a^{-1}za \in C_{X_\sigma}(a^{-1}(g\widetilde{\sigma})^e a) = C_{X_\sigma}(F(g\widetilde{\sigma}))$. This proves that $a^{-1}C_{X_{\sigma^e}}(g\widetilde{\sigma})a \subseteq C_{X_\sigma}(F(g\widetilde{\sigma}))$. For the reverse inclusion, let $w \in C_{X_\sigma}(F(g\widetilde{\sigma}))$. Then

$$awa^{-1} = (g\widetilde{\sigma})^{-e}(awa^{-1})(g\widetilde{\sigma})^e = (aa^{-\sigma^{-1}}\sigma)^{-e}(awa^{-1})(aa^{-\sigma^{-1}}\sigma)^e = (awa^{-1})^{\sigma^{-e}},$$

which implies that $awa^{-1} \in X_{\sigma^e}$. Moreover,

$$(g\widetilde{\sigma})^{-1}(awa^{-1})(g\widetilde{\sigma}) = (\sigma^{-1}a^{\sigma^{-1}}a^{-1})awa^{-1}(aa^{-\sigma^{-1}}\sigma) = aw^{\sigma^{-1}}a^{-1} = awa^{-1},$$

so $awa^{-1} \in C_{X_{\sigma^e}}(g\widetilde{\sigma})$. This implies that $a^{-1}C_{X_{\sigma^e}}(g\widetilde{\sigma})a = C_{X_\sigma}(F(g\widetilde{\sigma}))$, as claimed.

We may now prove that F is bijective. Let $\{c_1, \ldots, c_t\}$ be representatives of the X_σ-classes in X_σ. Then there exist X_{σ^e}-classes $C_1, \ldots, C_t$ in $X_{\sigma^e}\widetilde{\sigma}$ such that $F(C_i) = c_i$ for each i, by the surjectivity of F. By (ii), $|C_i| = |c_i||X_{\sigma^e} : X_\sigma|$. This implies that

$$\sum_{i=1}^{t} |C_i| = |X_{\sigma^e} : X_\sigma| \sum_{i=1}^{t} |c_i| = |X_{\sigma^e}| = |X_{\sigma^e}\widetilde{\sigma}|,$$

so $\{C_1, \ldots, C_t\}$ is a complete set of G-classes in $X_{\sigma^e}\widetilde{\sigma}$, which proves that F is bijective. □

The following concrete example highlights how we apply Shintani descent.

Example 2.7.2. Let $e \geqslant 2$, let $m \geqslant 4$ and let $q = 2^e$. Write $X = \Omega_{2m}(\overline{\mathbb{F}}_2)$. Let $\varphi = \varphi_{\mathcal{B}^+}$ be the standard Frobenius endomorphism $(a_{ij}) \mapsto (a_{ij}^2)$ of X.

Let F be the Shintani map of (X, φ, e). Note that $X_\varphi = \Omega_{2m}^+(2)$ and $X_{\varphi^e} = \Omega_{2m}^+(q)$. Now

$$F\colon \{(g\varphi)^{\Omega_{2m}^+(q)} \mid g \in \Omega_{2m}^+(q)\} \to \{x^{\Omega_{2m}^+(2)} \mid x \in \Omega_{2m}^+(2)\}.$$

Therefore, we can specify a conjugacy class in the coset $\Omega_{2m}^+(q)\varphi$ of the almost simple group $\langle \Omega_{2m}^+(q), \varphi \rangle$ as the preimage under F of a conjugacy class in $\Omega_{2m}^+(2)$.

Recall the element r from Definition 2.6.15. Let E be the Shintani map of $(X, r\varphi, e)$. Then $X_{r\varphi} \cong \Omega_{2m}^-(2)$ and $X_{(r\varphi)^e} \cong \Omega_{2m}^\varepsilon(q)$ where $\varepsilon = (-)^e$. Therefore, the map

$$E\colon \{(gr\varphi)^{\Omega_{2m}^\varepsilon(q)} \mid g \in \Omega_{2m}^\varepsilon(q)\} \to \{x^{\Omega_{2m}^-(2)} \mid x \in \Omega_{2m}^-(2)\}$$

allows us, for example, to specify elements in the coset $\Omega_{2m}^+(q)r\varphi$ of $\langle \Omega_{2m}^+(q), r\varphi \rangle$ when e is even; however, this setup does not shed light on this coset when e is odd.

2.7.2 Properties

In this section, we will highlight three properties of the Shintani map, which justify techniques that we repeatedly employ. Each of these properties relies on the fact that the Shintani map does not depend on the choice of element afforded by the Lang–Steinberg Theorem (see Theorem 2.7.1(i)). Throughout, we assume that X is a connected algebraic group, σ is a Steinberg endomorphism of X and $e > 1$. Moreover, let F be the Shintani map of (X, σ, e) and let $\widetilde{\sigma} = \sigma|_{X_{\sigma^e}}$.

We begin with a preliminary observation. If Y is a closed σ-stable subgroup of X, then the restriction σ_Y of σ to Y is a Steinberg endomorphism. Similarly, if $\pi\colon X \to Y$ is an isogeny with a σ-stable kernel, then σ induces a Steinberg endomorphism σ_Y on Y such that $\sigma_Y \circ \pi = \pi \circ \sigma$. For ease of notation, in both cases we write σ for σ_Y.

The first property concerns subgroups of X (see Proposition 4.3.9 for an application).

Lemma 2.7.3. *Let Y be a closed connected σ-stable subgroup of X and let E be the Shintani map of (Y, σ, e).*

(i) *For all $g \in Y_{\sigma^e}$, any representative of $E((g\widetilde{\sigma})^{Y_{\sigma^e}})$ is a representative of $F((g\widetilde{\sigma})^{X_{\sigma^e}})$.*

(ii) *For all $x \in Y_\sigma$, any representative of $E^{-1}(x^{Y_\sigma})$ is a representative of $F^{-1}(x^{X_\sigma})$.*

Proof. We prove only (i) since (ii) is very similar. Let $g \in Y_{\sigma^e}$ and let x be a representative of $E((g\widetilde{\sigma})^{Y_{\sigma^e}})$. Then $x = a^{-1}(g\widetilde{\sigma})^e a$ for an element $a \in Y$ such that $aa^{-\sigma^{-1}} = g$. Since $Y \leqslant X$, the element $a^{-1}(g\widetilde{\sigma})^e a = x$ is a valid representative of $F((g\widetilde{\sigma})^{X_{\sigma^e}})$, as required. □

The second property concerns quotients of X.

Lemma 2.7.4. *Let $\pi\colon X \to Y$ be an isogeny with a σ-stable kernel and let E be the Shintani map of (Y, σ, e).*

(i) *For all $h \in \pi(X_{\sigma^e}) \leqslant Y_{\sigma^e}$, there exists $y \in \pi(X_\sigma) \leqslant Y_\sigma$ that represents $E(h\widetilde{\sigma})$.*

(ii) *For all $y \in \pi(X_\sigma) \leqslant Y_\sigma$, there exists $h \in \pi(X_{\sigma^e}) \leqslant Y_{\sigma^e}$ such that $h\widetilde{\sigma}$ represents $E^{-1}(y)$.*

Moreover, if $\langle \pi(X_{\sigma^e}), \widetilde{\sigma}\rangle \trianglelefteqslant \langle Y_{\sigma^e}, \widetilde{\sigma}\rangle$ and $\pi(X_\sigma) \trianglelefteqslant Y_\sigma$, then E restricts to a bijection

$$E_1\colon \{(h\widetilde{\sigma})^{Y_{\sigma^e}} \mid h \in \pi(X_{\sigma^e})\} \to \{y^{Y_\sigma} \mid y \in \pi(X_\sigma)\}.$$

Proof. For (i), let $g \in X_{\sigma^e}$ and let x be a representative of $F(g\widetilde{\sigma})$. Then $x = a^{-1}(g\widetilde{\sigma})^e a$ for an element $a \in X$ such that $aa^{-\sigma^{-1}} = g$. Therefore, $\pi(x) = \pi(a)^{-1}(\pi(g)\widetilde{\sigma})^e \pi(a)$. Note that $\pi(x) \in \pi(X_\sigma) \leqslant Y_\sigma$. Moreover, $\pi(a) \in Y$ and $\pi(a)\pi(a)^{-\sigma^{-1}} = \pi(g)$, so $\pi(a)^{-1}(\pi(g)\widetilde{\sigma})^e \pi(a) = \pi(x)$ is a valid representative of $E(\pi(g)\widetilde{\sigma})$, as required. As with Lemma 2.7.3, (ii) is similar to (i).

If $\langle \pi(X_{\sigma^e}), \widetilde{\sigma}\rangle \trianglelefteqslant \langle Y_{\sigma^e}, \widetilde{\sigma}\rangle$ and $\pi(X_\sigma) \trianglelefteqslant Y_\sigma$, then for all $h \in \pi(X_{\sigma^e})$ and $y \in \pi(X_\sigma)$ we have $(h\widetilde{\sigma})^{Y_{\sigma^e}} \subseteq \pi(X_{\sigma^e})\widetilde{\sigma}$ and $y^{Y_\sigma} \subseteq \pi(X_\sigma)$, which implies, given (i) and (ii), that E restricts to the bijection E_1. □

The following concrete example elucidates the utility of Lemma 2.7.4.

Example 2.7.5. Let $m \geqslant 2$, let p be an odd prime and let $q = q_0^e = p^f$, where $e \geqslant 2$ divides f. Write $X = \mathrm{Sp}_{2m}(\overline{\mathbb{F}}_q)$ and $Y = \mathrm{PSp}_{2m}(\overline{\mathbb{F}}_q)$. Note that the natural quotient map $\pi\colon X \to Y$ is an isogeny. Let $\sigma = \varphi^{f/e}$ where $\varphi = \varphi_{\mathcal{B}^+}$ is the standard Frobenius endomorphism $(a_{ij}) \mapsto (a_{ij}^p)$ of X and also the induced endomorphism of Y.

Then $X_{\sigma^e} = \mathrm{Sp}_{2m}(q)$, so $\pi(X_{\sigma^e}) = \mathrm{PSp}_{2m}(q)$, which is a subgroup of $Y_{\sigma^e} = \mathrm{PGSp}_{2m}(q)$ (see Lemma 2.6.12). Since $\mathrm{PSp}_{2m}(q) \trianglelefteqslant \mathrm{PGSp}_{2m}(q)$ and $\langle \mathrm{PSp}_{2m}(q), \widetilde{\sigma}\rangle \trianglelefteqslant \langle \mathrm{PGSp}_{2m}(q), \widetilde{\sigma}\rangle$, by Lemma 2.7.4, the Shintani map

$$E\colon \{(g\widetilde{\sigma})^{\mathrm{PGSp}_{2m}(q)} \mid g \in \mathrm{PGSp}_{2m}(q)\} \to \{x^{\mathrm{PGSp}_{2m}(q_0)} \mid x \in \mathrm{PGSp}_{2m}(q_0)\}$$

restricts to the bijection

$$E_1\colon \{(g\widetilde{\sigma})^{\mathrm{PGSp}_{2m}(q)} \mid g \in \mathrm{PSp}_{2m}(q)\} \to \{x^{\mathrm{PGSp}_{2m}(q_0)} \mid x \in \mathrm{PSp}_{2m}(q_0)\}.$$

We conclude with a property that relates Shintani maps to taking powers (see Proposition 4.4.5 for an application).

Lemma 2.7.6. *Let d be a proper divisor of e and let E be the Shintani map of $(X, \sigma^d, e/d)$. Let $x \in X_\sigma$. If $F(g\widetilde{\sigma}) = x^{X_\sigma}$, then $E((g\widetilde{\sigma})^d) = x^{X_{\sigma^d}}$.*

Proof. Assume that $g \in X_{\sigma^e}$ satisfies $F(g\widetilde{\sigma}) = x$. Let $a \in X$ satisfy $a^{-1}(g\widetilde{\sigma})^e a = x$ and $aa^{-\sigma^{-1}} = g$. Write

$$h = gg^{\sigma^{-1}} \cdots g^{\sigma^{-(d-1)}}.$$

Then $(g\widetilde{\sigma})^d = h\widetilde{\sigma}^d$ and $h = aa^{-\sigma^{-d}}$. Therefore,

$$E((g\widetilde{\sigma})^d) = E(h\widetilde{\sigma}^d) = a^{-1}(h\widetilde{\sigma}^d)^{e/d}a = a^{-1}(g\widetilde{\sigma})^e a = x,$$

which completes the proof. □

Remark 2.7.7. Let $g, h \in X_{\sigma^e}$. If $g\widetilde{\sigma}$ and $h\widetilde{\sigma}$ are $\langle X_{\sigma^e}, \widetilde{\sigma}\rangle$-conjugate, then there exist $k \in X_{\sigma^e}$ and an integer i such that

$$h\widetilde{\sigma} = (k\widetilde{\sigma}^i)^{-1} g\widetilde{\sigma}(k\widetilde{\sigma}^i) = (h\widetilde{\sigma})^i (k\widetilde{\sigma}^i)^{-1} g\widetilde{\sigma}(k\widetilde{\sigma}^i)(h\widetilde{\sigma})^{-i},$$

but $(k\widetilde{\sigma}^i)(h\widetilde{\sigma})^{-i} \in X_{\sigma^e}$, so $g\widetilde{\sigma}$ and $h\widetilde{\sigma}$ are X_{σ^e}-conjugate. In particular,

$$|C_{\langle X_{\sigma^e}, \widetilde{\sigma}\rangle}(g\widetilde{\sigma})| = e|C_{X_{\sigma^e}}(g\widetilde{\sigma})|. \tag{2.22}$$

2.7.3 Applications

Theorem 2.7.1(ii) highlights that Shintani maps preserve important group theoretic data. We now exploit this by providing three applications of Shintani descent to determining maximal overgroups of elements, a key aspect of our probabilistic approach. We continue to assume that X is a connected algebraic group, σ is a Steinberg endomorphism of X, $e > 1$, F is the Shintani map of (X, σ, e) and $\widetilde{\sigma} = \sigma|_{X_{\sigma^e}}$.

We begin with an important general theorem of Shintani descent [18, Theorem 2.14].

Theorem 2.7.8. *Let Y be a closed connected σ-stable subgroup of X. For all $g \in X_{\sigma^e}$,*

$$\mathrm{fix}(g\widetilde{\sigma}, X_{\sigma^e}/Y_{\sigma^e}) = \mathrm{fix}(F(g\widetilde{\sigma}), X_\sigma/Y_\sigma).$$

The first application is essentially [18, Corollary 2.15].

Lemma 2.7.9. *Let Y be a closed connected σ-stable subgroup of X such that $N_{X_\sigma}(Y_\sigma) = Y_\sigma$ and $N_{X_{\sigma^e}}(Y_{\sigma^e}) = Y_{\sigma^e}$. For $g \in X_{\sigma^e}$, the number of X_{σ^e}-conjugates of Y_{σ^e} normalised by $g\widetilde{\sigma}$ equals the number of X_σ-conjugates of Y_σ containing $F(g\widetilde{\sigma})$.*

Proof. Since Y_{σ^e} is σ-stable and $N_{X_{\sigma^e}}(Y_{\sigma^e}) = Y_{\sigma^e}$, the conjugation action of $\langle X_{\sigma^e}, \widetilde{\sigma}\rangle$ on the set of X_{σ^e}-conjugates of Y_{σ^e} is equivalent to the action of $\langle X_{\sigma^e}, \widetilde{\sigma}\rangle$ on cosets of Y_{σ^e} in X_{σ^e}. Therefore, the number of X_{σ^e}-conjugates of Y_{σ^e} normalised by $g\widetilde{\sigma}$ is $\mathrm{fix}(g\widetilde{\sigma}, X_{\sigma^e}/Y_{\sigma^e})$. Similarly, the number of X_σ-conjugates of Y_σ containing $F(g\widetilde{\sigma})$ is $\mathrm{fix}(F(g\widetilde{\sigma}), X_\sigma/Y_\sigma)$. The result now follows from Theorem 2.7.8. □

The following example demonstrates a typical application of Lemma 2.7.9.

Example 2.7.10. Let $n \geqslant 2$ and let $q = q_0^e = p^f$ where $e \geqslant 2$ divides f. Let $X = \mathrm{SL}_n(\overline{\mathbb{F}}_p)$ and let $\sigma = \varphi^{f/e}$, where φ is the standard Frobenius endomorphism $(a_{ij}) \mapsto (a_{ij}^p)$ of X, with respect to some fixed basis $\mathcal{B} = (u_1, \ldots, u_n)$ for $\overline{\mathbb{F}}_p^n$. Let F be the Shintani map of (X, σ, e). Note that $X_\sigma = \mathrm{SL}_n(q_0)$ and $X_{\sigma^e} = \mathrm{SL}_n(q)$.

Let $1 \leqslant k < n$. We may fix a σ-stable maximal P_k parabolic subgroup $Y \leqslant X$; for example, let $Y = X_{\langle u_1, \ldots, u_k\rangle}$ (see [53, Section 12] for a discussion of parabolic subgroups). In particular, Y is a closed connected subgroup of X. Moreover, $N_{X_\sigma}(Y_\sigma) = Y_\sigma$ and $N_{X_{\sigma^e}}(Y_{\sigma^e}) = Y_{\sigma^e}$, so we are in a position to apply Lemma 2.7.9.

Let $g \in X_{\sigma^e}$. By Lemma 2.7.9, the number of $\mathrm{SL}_n(q)$-conjugates of Y_{σ^e} normalised by $g\widetilde{\sigma}$ equals the number of $\mathrm{SL}_n(q_0)$-conjugates of Y_σ containing $F(g\widetilde{\sigma})$.

There is a unique $\mathrm{SL}_n(q)$-class of maximal subgroups of $G = \langle \mathrm{SL}_n(q), \widetilde{\sigma}\rangle$ of type P_k and this class is represented by $H = \langle Y_{\sigma^e}, \widetilde{\sigma}\rangle$ (see, for example, [43, Proposition 4.1.17]). In addition, for each $x \in \mathrm{SL}_n(q)$, the element $g\widetilde{\sigma}$ is contained in H^x if and only if $g\widetilde{\sigma}$ normalises $Y_{\sigma^e}^x$. Therefore, the number of G-conjugates of H containing $g\widetilde{\sigma}$ equals the number of $\mathrm{SL}_n(q_0)$-conjugates of Y_σ containing $F(g\widetilde{\sigma})$.

Example 2.7.10 highlights the key idea of Shintani descent: we can deduce information about $g\widetilde{\sigma}$ from information about $F(g\widetilde{\sigma})$.

Our second application is a minor generalisation of [18, Proposition 2.16(i)]. Here we write $\widetilde{G} = X_{\sigma^e}{:}\langle\widetilde{\sigma}\rangle$.

Lemma 2.7.11. *Let $g \in \widetilde{G}$ and let $H \leqslant \widetilde{G}$. Then $g\widetilde{\sigma}$ is contained in at most $|C_{X_\sigma}(F(g\widetilde{\sigma}))|$ $\widetilde{G}$-conjugates of H.*

Proof. By Lemma 2.1.3, the number of $\widetilde{G}$-conjugates of H that contain $g\widetilde{\sigma}$ is

$$N = \frac{|(g\widetilde{\sigma})^{\widetilde{G}} \cap H|}{|(g\widetilde{\sigma})^{\widetilde{G}}|} \cdot \frac{|\widetilde{G}|}{|N_{\widetilde{G}}(H)|} = \frac{|(g\widetilde{\sigma})^{\widetilde{G}} \cap H||C_{\widetilde{G}}(g\widetilde{\sigma})|}{|N_{\widetilde{G}}(H)|}.$$

First note that $(g\widetilde{\sigma})^{\widetilde{G}} \subseteq X_{\sigma^e} g\widetilde{\sigma}$, and for $0 \leqslant i < e$, the cosets $(X_{\sigma^e} \cap H)(g\widetilde{\sigma})^i$ in H are distinct. Therefore, $|(g\widetilde{\sigma})^{\widetilde{G}} \cap H| \leqslant |H|/e$. Next, by (2.22) and Theorem 2.7.1(ii),

$$|C_{\widetilde{G}}(g\widetilde{\sigma})| = |C_{X_{\sigma^e}}(g\widetilde{\sigma})|e = |C_{X_\sigma}(F(g\widetilde{\sigma}))|e.$$

Together these observations give

$$N \leqslant \frac{|H||C_{X_\sigma}(F(g\widetilde{\sigma}))|e}{e|N_{\widetilde{G}}(H)|} \leqslant |C_{X_\sigma}(F(g\widetilde{\sigma}))|. \qquad \square$$

The third application is based on [18, Proposition 2.16(ii)] and is more specialised than the previous two. In this case, assume that X is an adjoint simple classical algebraic group with natural module V and $\sigma = \gamma\varphi^i$, where φ is a standard Frobenius endomorphism of X and either γ is trivial or X has type D_m and $\gamma = r$ (see Section 2.6.3).

Lemma 2.7.12. *Let $q = q_0^e = p^f$ where e is a prime divisor of f. Let $g \in X_{\sigma^e}$ such that $F(g\widetilde{\sigma})$ is $A_1 \oplus \cdots \oplus A_k$, where each A_i is either irreducible on a d_i-space or is $A_i = B_i \oplus B_i^{-\mathsf{T}}$ where B_i is irreducible on a d_i-space and B_i is not similar to $B_i^{-\mathsf{T}}$. Assume that $(d_i, d_j) = 1$ when $i \neq j$. Then the number of X_{σ^e}-conjugates of X_σ normalised by $g\widetilde{\sigma}$ is at most e^k.*

Proof. Write $H = X_\sigma$ and $\widetilde{H} = N_{\widetilde{G}}(H)$, noting that $\widetilde{H} = H \times \langle\widetilde{\sigma}\rangle$ since H is adjoint. The restrictions on $F(g\widetilde{\sigma})$ in the statement imply that the eigenvalue multiset (over $\overline{\mathbb{F}}_p$) of $F(g\widetilde{\sigma})$ is $S_1 \cup \cdots \cup S_k$ where S_i is either Λ_i or $\Lambda_i \cup \Lambda_i^{-1}$ where $\Lambda_i = \{\lambda_i, \ldots, \lambda_i^{q_0^{d_i-1}}\}$, and $\Lambda_i \neq \Lambda_i^{-1}$ in the latter case (compare with Lemma 2.3.17).

Let $h\widetilde{\sigma} \in \widetilde{H}$ be $\widetilde{G}$-conjugate to $g\widetilde{\sigma}$. Then $F(h\widetilde{\sigma})$ is X_σ-conjugate to $F(g\widetilde{\sigma})$. Let the eigenvalue multiset of $h \in H$ be $\{\alpha_1, \ldots, \alpha_n\}$. Therefore, the eigenvalue multiset of $F(h\widetilde{\sigma})$ is the eigenvalue multiset of $(h\widetilde{\sigma})^e = h^e$, which is $\{\alpha_1^e, \ldots, \alpha_n^e\}$. Therefore, without loss of generality, $\alpha_i^e = \lambda_i$ for each $1 \leqslant i \leqslant k$. Now note that $\alpha_1, \ldots, \alpha_k$ determine all of the eigenvalues of h. Thus, there are e^k choices for the eigenvalues of h and consequently e^k choices for h and, hence, $h\widetilde{\sigma}$ up to H-conjugacy. Therefore, $(g\widetilde{\sigma})^{\widetilde{G}} \cap \widetilde{H}$ splits into e^k H-classes. Since $(d_i, d_j) = 1$ for $i \neq j$, we know that h stabilises the same type of decomposition of $\mathbb{F}_{q_0}^n$ as g, acting irreducibly on the corresponding summands. Therefore, $|C_{X_\sigma}(h\widetilde{\sigma})| = |C_{X_\sigma}(h)| = |C_{X_\sigma}(F(g\widetilde{\sigma}))|$. Consequently, the H-classes into which $g\widetilde{\sigma}^{\widetilde{G}} \cap \widetilde{H}$ splits have size $|F(g\widetilde{\sigma})^H|$.

By Lemma 2.1.3, the number of $\widetilde{G}$-conjugates of $\widetilde{H}$ which contain $g\widetilde{\sigma}$ is

$$\frac{|(g\widetilde{\sigma})^{\widetilde{G}} \cap \widetilde{H}|}{|(g\widetilde{\sigma})^{\widetilde{G}}|} \frac{|\widetilde{G}|}{|\widetilde{H}|} \leqslant \frac{e^k |F(g\widetilde{\sigma})^{X_\sigma}||C_{\widetilde{G}}(g\widetilde{\sigma})|}{|\widetilde{H}|} = \frac{e^k |X_\sigma||C_{\widetilde{G}}(g\widetilde{\sigma})|}{|\widetilde{H}||C_{X_\sigma}(F(g\widetilde{\sigma}))|} \leqslant e^k. \qquad \square$$

2.7.4 Generalisation

In situations where we are unable to apply Shintani descent directly (see Section 5.3.2), the following new result is a very useful substitute. We continue to assume that X is a connected algebraic group, σ is a Steinberg endomorphism of X and $e > 1$.

Lemma 2.7.13. *Let γ be an order d automorphism of X as an algebraic group. Let Z be a closed connected σ-stable subgroup of X contained in $C_X(\gamma)$. Let $G = X_{\gamma\sigma^e}{:}\langle\widetilde{\gamma},\widetilde{\sigma}\rangle$ where $\widetilde{\sigma} = \sigma|_{X_{\gamma\sigma^e}}$ and $\widetilde{\gamma} = \gamma|_{X_{\gamma\sigma^e}}$.*

(i) *Let $x \in Z_\sigma \leqslant X_{\gamma\sigma^e}$. There exists $g \in X_{\gamma\sigma^e}$ such that $(g\widetilde{\sigma})^e$ and $x\widetilde{\gamma}^{-1}$ are X-conjugate elements of G.*

(ii) *Moreover, if $(\gamma\sigma^e)^d = \sigma^{ed}$, then, for all x and g in (i) and $H \leqslant \langle X_{\gamma\sigma^e}, \widetilde{\sigma}\rangle$, the number of $X_{\gamma\sigma^e}$-conjugates of H containing $g\widetilde{\sigma}$ is at most $|C_{X_\sigma}(x^d)|$.*

Proof. Let F be the Shintani map of (Z,σ,e) and fix $x \in Z_\sigma$. Let $\widehat{\sigma} = \sigma|_{Z_{\sigma^e}}$, noting that $\widehat{\sigma}^e = 1$. By Theorem 2.7.1 applied to F, there exists $g \in Z_{\sigma^e}$ such that

$$a^{-1}(g\widehat{\sigma})^e a = a^{-1}(gg^{\sigma^{e-1}}g^{\sigma^{e-2}}\cdots g^{\sigma})a = x$$

as elements of $Z_{\sigma^e}{:}\langle\widehat{\sigma}\rangle$, where $a \in Z \leqslant X$ satisfies $aa^{-\sigma^{-1}} = g$. Note that $g \in Z_{\sigma^e} \leqslant X_{\gamma\sigma^e}$ and $\widetilde{\sigma}^e = \widetilde{\gamma}^{-1}$ as an element of $G = X_{\gamma\sigma^e}{:}\langle\widetilde{\sigma},\widetilde{\gamma}\rangle$. Therefore, as elements of G,

$$a^{-1}(g\widetilde{\sigma})^e a = a^{-1}(gg^{\sigma^{e-1}}g^{\sigma^{e-2}}\cdots g^{\sigma})\widetilde{\sigma}^e a = a^{-1}(gg^{\sigma^{e-1}}g^{\sigma^{e-2}}\cdots g^{\sigma})\widetilde{\gamma}^{-1}a = x\widetilde{\gamma}^{-1},$$

which proves (i).

Now fix $H \leqslant \langle X_{\gamma\sigma^e}, \widetilde{\sigma}\rangle$. Let E be the Shintani map of (X,σ,de), recording that $Z_\sigma \leqslant X_\sigma$ and $X_{\gamma\sigma^e} \leqslant X_{(\gamma\sigma^e)^d} = X_{\sigma^{de}}$. Write $\overline{\sigma} = \sigma|_{X_{\sigma^{de}}}$. Since $\overline{\sigma}|_{X_{\gamma\sigma^e}} = \widetilde{\sigma}$ and $|\overline{\sigma}| = de = |\widetilde{\sigma}|$, we can consider $\langle X_{\gamma\sigma^e}, \widetilde{\sigma}\rangle$ as a subgroup of $\langle X_{\sigma^{de}}, \overline{\sigma}\rangle$, where we identify $\widetilde{\sigma}$ with $\overline{\sigma}$. Therefore,

$$E(g\widetilde{\sigma}) = a^{-1}(g\widetilde{\sigma})^{de}a = x^d.$$

Therefore, by Lemma 2.7.11, the number of $X_{\sigma^{de}}$-conjugates of H containing $g\widetilde{\sigma}$ is at most $|C_{X_\sigma}(x^d)|$, which implies (ii). □

We conclude with an example that demonstrates how we use Lemma 2.7.13.

Example 2.7.14. This example continues Example 2.7.2. Recall that standard Shintani descent did not provide information about the coset $\Omega^+_{2m}(q)r\varphi$ of $\langle\Omega^+_{2m}(q), r\varphi\rangle$ when e is odd. We now use Lemma 2.7.13 to do this.

Let $e \geqslant 3$ be odd, $m \geqslant 4$ and $q = 2^e$. Write $X = \Omega_{2m}(\overline{\mathbb{F}}_2)$ and recall the standard Frobenius endomorphism φ and the involutory automorphism r. Let $Z \cong \Omega_{2m-2}(\overline{\mathbb{F}}_2)$ be the subgroup of X that centralises $\langle e_1,\ldots,f_{m-1}\rangle \perp \langle e_m, f_m\rangle$ and acts trivially on the second summand. Evidently $Z \leqslant C_X(r)$. Therefore, Lemma 2.7.13(i) implies that for all $x \in Z_{r\varphi} \cong \Omega^+_{2m-2}(2)$, there exists $g \in X_{r(r\varphi)^e} = \Omega^+_{2m}(q)$ such that $(g\varphi)^e$ is X-conjugate to xr. Moreover, Lemma 2.7.13(ii) translates information about x into information about $g\varphi$. In this way, we can select and work with elements in the coset $\Omega^+_{2m}(q)\varphi$ when e is odd.

2.8 Computational methods

Here we briefly discuss the computational methods that we employ to study the uniform spread of small almost simple classical groups. The relevant code is in Appendix A.

We implemented an algorithm in MAGMA [5] that takes as input a finite group G, an element $s \in G$ and nonnegative integers k and N. The aim of the algorithm is to determine whether $u(G) \geqslant k$ is witnessed by the conjugacy class s^G.

We first follow the probabilistic method described in Section 2.1. To determine $\mathcal{M}(G, s)$ we typically use `MaximalSubgroups`. However, for larger groups we use the function `ClassicalMaximals` of Holt and Roney-Dougal. For each conjugacy class x^G, we need to compute $\mathrm{fpr}(x, G/H)$ for each $H \in \mathcal{M}(G, s)$; we do this by calculating $|x^G \cap H|$ using `IsConjugate`. If we establish that $P(x_1, s) + \cdots + P(x_k, s) < 1$ for all k-tuples $(x_1^G, \ldots, x_k^G)$ of classes of prime order elements of G, then we have verified that $u(G) \geqslant k$ with respect to the class s^G.

Otherwise, for each k-tuple of classes $(C_1, \ldots, C_k)$, we apply a randomised method (parameterised by N) to explicitly construct an element $z \in s^G$ such that for all $c_i \in C_i$, $\langle c_1, z\rangle = \cdots = \langle c_k, z\rangle = G$. This randomised approach is based on the computations in [10, Section 4], which are described by Breuer in [9, Section 3.3]. Observe that it suffices to show that for all representatives $(x_1, \ldots, x_k)$ of the orbits of $C_1 \times \cdots \times C_k$ under the diagonal conjugation action of G, there exists $z \in s^G$ such that $\langle x_1, z\rangle = \cdots = \langle x_k, z\rangle = G$. An algorithm of [9, pp.18–19] to construct these orbit representatives is the crucial ingredient. Given these representatives, we test at most N random conjugates of s for each list of representatives, and we return any k-tuples of conjugacy classes for which no suitable conjugate of s is found. If no k-tuples fail, then the bound $u(G) \geqslant k$ holds.

These computational methods are similar to those employed to study the uniform domination number in the joint paper [20], which are detailed in [19]; any overlap with the computational methods in this joint paper is the work of the author of this thesis.

The computations were carried out in MAGMA 2.24-4 on a 2.7 GHz machine with 128 GB RAM. The largest computation took 144 s and 193 MB of memory.

3

Fixed Point Ratios

This section serves to provide the fixed point ratio bounds that we require in order to apply the probabilistic method described in Section 2.1. There is a vast literature on fixed point ratios for primitive actions of almost simple groups. One reason for this work is the important applications these bounds have to a variety of areas, such as monodromy groups and base sizes of permutation groups, via probabilistic methods (see Section 2.1).

The most general bound in this area is [49, Theorem 1] of Liebeck and Saxl, which establishes that

$$\mathrm{fpr}(x, G/H) \leqslant \frac{4}{3q} \tag{3.1}$$

for any almost simple group of Lie type G over $\mathbb{F}_q$, maximal subgroup $H \leqslant G$ and nontrivial element $x \in G$, with a known list of exceptions. This bound is essentially best possible, since $\mathrm{fpr}(x, G/H) \approx q^{-1}$ when q is odd, $G = \mathrm{PGL}_n(q)$, H is a maximal P_1 parabolic subgroup (the stabiliser of a 1-space of $\mathbb{F}_q^n$) and x lifts to the diagonal matrix $x = [-1, I_{n-1}] \in \mathrm{GL}_n(q)$.

Let G be an almost simple classical group. A maximal subgroup $H \leqslant G$ is a *subspace subgroup* if $H \cap \mathrm{soc}(G)$ acts reducibly on the natural module for $\mathrm{soc}(G)$ or if $\mathrm{soc}(G)$ is $\mathrm{Sp}_n(2^f)$ and $H \cap \mathrm{soc}(G) = \mathrm{O}_n^{\pm}(2^f)$, and H is a *nonsubspace subgroup* otherwise. In Section 3.1 we record and prove bounds on fixed point ratios for subspace subgroups.

Notice that the bound in (3.1) does not depend on the element x. A theorem of Burness [12, Theorem 1] gives a bound on $\mathrm{fpr}(x, G/H)$ depending on x when $H \leqslant G$ is nonsubspace and $x \in G$ has prime order. We present and apply this result in Section 3.2 before establishing a stronger bound for groups with socle $\mathrm{PSp}_4(q)$.

3.1 Subspace actions

We begin with a general theorem, which combines several results of Guralnick and Kantor [33, Proposition 3.1, 3.15 and 3.16].

For an almost simple classical group G, we adopt the convention that $u = 1$, unless $\mathrm{soc}(G) = \mathrm{PSU}_n(q)$, in which case $u = 2$. Therefore, $V = \mathbb{F}_{q^u}^n$ is the natural module for all of $\mathrm{GL}_n(q)$, $\mathrm{Sp}_n(q)$, $\mathrm{O}_n^\varepsilon(q)$ and $\mathrm{GU}_n(q)$. The *Witt index* of a subspace U of V is the dimension of a maximal totally singular subspace of U. (When $G = \mathrm{GL}_n(q)$ all subspaces of V are totally singular.)

Theorem 3.1.1. *Let $G \leqslant \Gamma\mathrm{L}(V)$ be an almost simple classical group with natural module $V = F^n$ where $F = \mathbb{F}_{q^u}$. Assume that $n \geqslant 6$. Let $H \leqslant G$ be a reducible maximal subgroup, stabilising a subspace $0 < U < V$ of dimension k and Witt index l. Let $1 \neq x \in G$. Let m, a, b, c be the parameters defined in Table 3.1.*

(i) *If $\mathrm{soc}(G) = \mathrm{PSL}_n(q)$, then*

$$\mathrm{fpr}(x, G/H) \leqslant 2|F|^{-\min\{k, n-k\}}.$$

(ii) *If $\mathrm{soc}(G) \neq \mathrm{PSL}_n(q)$ and U is nondegenerate, then*

$$\mathrm{fpr}(x, G/H) \leqslant 2|F|^{-m+a} + |F|^{-m+b} + |F|^{-l} + |F|^{-n+k}.$$

(iii) *If $\mathrm{soc}(G) \neq \mathrm{PSL}_n(q)$ and U is totally singular, then*

$$\mathrm{fpr}(x, G/H) \leqslant 2|F|^{-m+c} + |F|^{-\frac{m}{u}+\frac{b}{u}} + |F|^{-k}.$$

The bounds in Theorem 3.1.1 do not depend on x. In contrast, Frohardt and Magaard [29, Theorems 1–6] established upper and lower bounds for the fixed point ratio of an element x of an almost simple classical group on an appropriate set of k-spaces which depend not only on q, n and k, but also the element $x \in G \cap \mathrm{PGL}(V)$.

Table 3.1: Fixed point ratios: Values of a, b, c

$\mathrm{soc}(G)$		a	b	c
$\mathrm{PSp}_{2m}(q)$	q even	2	0	1
	q odd	1	0	1
$\Omega_{2m+1}(q)$		1	0	1
$\mathrm{P}\Omega_{2m}^\varepsilon(q)$	$\varepsilon = +$	2	1	2
	$\varepsilon = -$	2	0	1
$\mathrm{PSU}_n(q)$	$n = 2m$	2	$\frac{1}{2}$	1
	$n = 2m+1$	1	$-\frac{1}{2}$	0

More precisely, the bounds in [29] depend on the parameter $\nu(x)$, the codimension of the largest eigenspace of $\hat{x}$ on $\overline{V} = V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ for a preimage $\hat{x}$ of x in $\mathrm{GL}(V)$ (see Notation 2.5.12). For example, if $G = \mathrm{PSp}_n(q)$ and $H \leqslant G$ is the stabiliser of a nondegenerate k-space, where $k < \frac{n}{2}$, then for all elements $x \in G$ satisfying $s = \nu(x) < \frac{n}{2k}$, [29, Theorem 2] gives

$$q^{-sk} - 3q^{-(n-1)/2} < \mathrm{fpr}(x, G/H) < q^{-sk} + 200q^{-(n-1)/2}.$$

However, for our application, the constants in these bounds are not sufficient. Therefore, we present bounds which are similar to those in [29], but with sharper constants in the special cases that we are interested in. Our bounds will have no restriction on s.

Before we obtain these bounds, let us make some comments on our proofs. We will need a detailed understanding of the conjugacy of prime order elements in almost simple classical groups. Recall this topic was discussed in Sections 2.4 and 2.6.6. We will freely adopt the notation and terminology introduced therein.

The following lemma will be used frequently without reference.

Lemma 3.1.2. *Let G be a finite group with a normal subgroup G_0. Let H be a maximal subgroup of G that does not contain G_0. Write $H_0 = H \cap G_0$. Then*

(i) $|G : G_0| = |H : H_0|$ *and* $|G : H| = |G_0 : H_0|$

(ii) $\mathrm{fpr}(x, G/H) = \mathrm{fpr}(x, G_0/H_0)$ *for all* $x \in G_0$.

Proof. We begin with (i). Since H is maximal in G and does not contain G_0

$$G/G_0 = HG_0/G_0 \cong H/(H \cap G_0) = H/H_0.$$

Therefore, $|G : G_0| = |H : H_0|$ and, consequently, $|G : H| = |G_0 : H_0|$.

Let us now turn to (ii). Let $x \in G_0$. Let $g_1, \ldots, g_k$ be a (right) transversal of H_0 in G_0. We claim that $g_1, \ldots, g_k$ is a transversal of H in G. By (i), it suffices to prove that $Hg_i \neq Hg_j$ when $i \neq j$. To this end, assume that $Hg_i = Hg_j$. Then $g_j = hg_i$ for some $h \in H$. Since $g_i, g_j \in G_0$ we deduce that $h \in G_0$ and hence $h \in H_0$. Therefore, $H_0g_i = H_0g_j$ and $i = j$. Now, for each i, since $x, g_i \in G_0$ we know that $g_i x g_i^{-1} \in H$ if and only if $g_i x g_i^{-1} \in H_0$, so $Hg_ix = Hg_i$ if and only if $H_0g_ix = H_0g_i$. This proves that $\mathrm{fix}(x, G/H) = \mathrm{fix}(x, G_0/H_0)$. By (i), $|G : H| = |G_0 : H_0|$, so $\mathrm{fpr}(x, G/H) = \mathrm{fpr}(x, G_0/H_0)$, as required. □

The next result appears as Proposition 3.5 in the author's paper [38].

Proposition 3.1.3. *Let G be an almost simple group with socle $\mathrm{PSp}_{2m}(q)$ where $m \geqslant 3$. Let $x \in G$ have prime order. If $x \in \mathrm{PGSp}_{2m}(q)$, then write $s = \nu(x)$. Let H be the stabiliser in G of a nondegenerate 2-space. Then*

$$\mathrm{fpr}(x, G/H) \leqslant \begin{cases} q^{-2s} + q^{-(2s+2)} + q^{-(2m-2)} + q^{-(2m-1)} & \text{if } x \in \mathrm{PGSp}_{2m}(q) \\ 2q^{-(2m-1)} & \text{if } x \notin \mathrm{PGSp}_{2m}(q) \end{cases}$$

Proof. If x is not contained in a G-conjugate of H, then $\mathrm{fpr}(x, G/H) = 0$. Therefore, assume that $x \in H$. Write $G_0 = G \cap \mathrm{PGSp}_{2m}(q)$ and $H_0 = H \cap G_0$. Hence, H_0 is a subgroup of $\mathrm{GSp}_2(q) \times \mathrm{GSp}_{2m-2}(q)$, modulo scalars. Let r be the (prime) order of x. Let $V = \mathbb{F}_q^{2m}$ be the natural module for $\mathrm{PSp}_{2m}(q)$.

Case 1: $x \in G_0$

The information on the conjugacy classes of elements of prime order given in Section 2.4 allows the splitting of $x^{G_0} \cap H_0$ into H_0-classes to be easily determined. We then verify the claimed fixed point ratio bound by using the centraliser orders given in [17, Appendix B] Let us explain in detail how this is done when $r \notin \{2, p\}$.

Assume that $r \notin \{2, p\}$. Therefore, x is a semisimple element of odd prime order. By Lemma 2.4.3, x is G_0-conjugate to an element that lifts to a block diagonal matrix $[A_1^{a_1}, \ldots, A_t^{a_t}, I_e]$ centralising a decomposition $V = V_1^{a_1} \perp \cdots \perp V_t^{a_t} \perp W$ where, for some even k, each V_j is a nondegenerate k-space and W is the (nondegenerate) 1-eigenspace of x. Moreover, either each matrix A_j acts irreducibly on V_j or each matrix A_j centralises the decomposition $V_j = U_j \oplus U_j^*$, where U_j and U_j^* are totally singular subspaces on which A_j acts irreducibly. The submodules V_j are pairwise nonisomorphic.

Let us now determine how $x^{G_0} \cap H_0$ splits into H_0-classes. Let $h \in H_0$ be G_0-conjugate to x. Then h lifts to $(A, B) \in \mathrm{GSp}_2(q) \times \mathrm{GSp}_{2m-2}(q)$. If $A = I_2$, then $e \geqslant 2$ and h is H_0-conjugate to x_0, an element lifting to $(I_2, [A_1^{a_1}, \ldots, A_t^{a_t}, I_{e-2}])$. If $A \neq I_2$, then let $\lambda \in \overline{\mathbb{F}}_q$ be a nontrivial eigenvalue of A. Then λ is an eigenvalue of A_j for some j. Since the set of eigenvalues of A is closed under the map $\mu \mapsto \mu^q$, we deduce that $k = 2$ and $A = A_j$. Therefore, h is H_0-conjugate to x_j, an element lifting to $(A_j, [A_1^{a_1}, \ldots, A_j^{a_j - 1}, \ldots, A_t^{a_t}, I_e])$.

This information is enough to determine how $x^{G_0} \cap H_0$ splits into H_0-classes. If $k > 2$, then $e > 0$ and $x^{G_0} \cap H_0 = x_0^{H_0}$. If $k = 2$, then, writing $e = 2a_0$, we have

$$x^{G_0} \cap H_0 = \bigcup_{\substack{0 \leqslant j \leqslant t \\ a_j > 0}} x_j^{H_0}$$

We now use this information about $x^{G_0} \cap H_0$ to find an upper bound on $\mathrm{fpr}(x, G_0/H_0)$. First note that

$$\frac{|H_0|}{|G_0|} = \frac{|\mathrm{Sp}_2(q)||\mathrm{Sp}_{2m-2}(q)|}{|\mathrm{Sp}_{2m}(q)|} = \frac{q^2 - 1}{q^{2m-2}(q^{2m} - 1)}.$$

Similarly, if $e > 0$, then

$$\frac{|C_{G_0}(x)|}{|C_{H_0}(x_0)|} = \frac{|\mathrm{Sp}_e(2)|}{|\mathrm{Sp}_2(q)||\mathrm{Sp}_{e-2}(q)|} = \frac{q^{e-2}(q^e - 1)}{q^2 - 1}.$$

Now assume that $k = 2$. Let $\varepsilon = +$ if r divides $q - 1$ and let $\varepsilon = -$ otherwise (when r necessarily divides $q + 1$). Then for all $1 \leqslant j \leqslant t$ such that $a_j > 0$ we have

$$\frac{|C_{G_0}(x)|}{|C_{H_0}(x_j)|} = \frac{|\mathrm{GL}_{a_j}^{\varepsilon}(q)|}{|\mathrm{GL}_1^{\varepsilon}(q)||\mathrm{GL}_{a_j - 1}^{\varepsilon}(q)|} \leqslant \frac{q^{a_j - 1}(q^{a_j} + 1)}{q - 1}$$

Now, in light of Lemma 3.1.2,

$$\mathrm{fpr}(x, G/H) = \mathrm{fpr}(x, G_0/H_0) = \frac{|H_0|}{|G_0|} \sum_{\substack{0 \leqslant j \leqslant t \\ a_j > 0}} \frac{|C_{G_0}(x)|}{|C_{H_0}(x_j)|}.$$

Therefore, with the above bounds, we maximise our upper bound on $\mathrm{fpr}(x, G/H)$ when $a_j = 0$ for all $j \geqslant 2$. In this case, $a_0 + a_1 = m$ and $s = 2a_1 = 2m - e$. Therefore,

$$\mathrm{fpr}(x, G/H) \leqslant \frac{q^2-1}{q^{2m-2}(q^{2m}-1)} \left(\frac{q^{2m-s-2}(q^{2m-s}-1)}{q^2-1} + \frac{q^{\frac{s}{2}-1}(q^{\frac{s}{2}}+1)}{q-1} \right) \leqslant \frac{1}{q^{2s}} + \frac{1}{q^{2m-2s}}.$$

For another example, assume that $r = p = 2$. Therefore, x is a unipotent involution and we adopt the notation of Aschbacher and Seitz [3]. In light of [17, Lemma 3.4.14], it is straightforward to determine how $x^{G_0} \cap H_0$ splits into H_0-classes. For example, if $x = b_s$ for odd $s \geqslant 3$, then $x^{G_0} \cap H_0$ is the union of $x_1^{H_0} \cup x_2^{H_0} \cup x_3^{H_0}$ where x_1, x_2 and x_3 are the elements (I_2, b_s), (b_1, a_{s-1}) and (b_1, c_{s-1}) of $\mathrm{Sp}_2(q) \times \mathrm{Sp}_{2m-2}(q)$. Therefore, using the centraliser orders in [17, Appendix B],

$$\mathrm{fpr}(x, G/H) = \mathrm{fpr}(x, G_0/H_0) = \frac{|H_0|}{|G_0|} \sum_{i=1}^{3} \frac{|C_{G_0}(x_i)|}{|C_{H_0}(x_i)|} \leqslant \frac{1}{q^{2s}} + \frac{1}{q^{2m-1}} + \frac{1}{q^{2m+s-1}}.$$

Case 2: $x \notin G_0$

By Lemma 2.6.20, x is a field automorphism. In this case, $|x^G \cap H|$ is at most the number of elements of order r in $G_0 x \cap H = H_0 x$, which, by [31, Proposition 4.9.1(d)], is at most $2|x^H|$. Therefore, $|x^G \cap H| \leqslant 2|x^H|$ and

$$\mathrm{fpr}(x, G/H) = \frac{2|H||C_G(x)|}{|G||C_H(x)|} \leqslant \frac{2|\mathrm{Sp}_2(q)||\mathrm{Sp}_{2m-2}(q)|f|\mathrm{Sp}_{2m}(q^{1/r})|f}{|\mathrm{Sp}_{2m}(q)|f|\mathrm{Sp}_2(q^{1/r})||\mathrm{Sp}_{2m-2}(q^{1/r})|f} \leqslant \frac{2}{q^{2m-2}}.$$

This completes the proof. □

We now turn to orthogonal groups. In part (i) of the statement of Proposition 3.1.4, if q is even, then the nonsingular 1-space in question is degenerate and has a stabiliser of type $\mathrm{Sp}_{2m-2}(q)$ (see [43, Proposition 4.1.7]).

Proposition 3.1.4. *Let $G = \mathrm{PO}^{\varepsilon}_{2m}(q)$ where $m \geqslant 4$. Let $x \in G$ have prime order and $v(x) = s$.*

(i) *If $H \leqslant G$ is the stabiliser of a nonsingular 1-space, then*

$$\mathrm{fpr}(x, G/H) \leqslant \frac{1}{q^s} + \frac{1}{q^{2m-s}} + \frac{2}{q^m - \varepsilon}.$$

(ii) *If $H \leqslant G$ is the stabiliser of a nondegenerate 2-space, then*

$$\mathrm{fpr}(x, G/H) \leqslant \frac{1}{q^{2s}} + \frac{1}{q^{m-1}-1} + \frac{4}{q^{2m-3}} + \frac{1}{q^{2m-2s}}.$$

Proof. We focus on part (i), since part (ii) is very similar to Proposition 3.1.3. Let r be the order of x and assume that $x \in H$. Write $H = G_{\langle u \rangle}$ and write $U = \langle u \rangle^{\perp}$.

Case 1: $r \notin \{2, p\}$

As in the proof of Proposition 3.1.3, by Lemma 2.4.3, x is G-conjugate to an element that lifts to a block diagonal matrix $[M_1, \ldots, M_d, I_{2l}]$ centralising $V = V_1 \perp \cdots \perp V_d \perp W$ where each V_j is nondegenerate and W is the 1-eigenspace of x. Moreover, either each matrix M_j acts irreducibly on V_j or each matrix M_j centralises a decomposition of V_j into two totally singular subspaces on which M_j acts irreducibly.

Since $x \in H$, we deduce that x fixes u. Therefore, $2l > 0$ and on U the element x acts as $[M_1, \ldots, M_d, I_{2l-1}]$. Therefore, Lemma 2.4.3 implies that $x^G \cap H = x^H$. Moreover, from the centraliser orders in [17, Appendix B] we obtain

$$\frac{|x^G \cap H|}{|x^G|} = \frac{|H|}{|G|}\frac{|C_G(x)|}{|C_H(x)|} \leqslant \frac{(2, q-1)}{q^{m-1}(q^m - \varepsilon)}\frac{q^{l-1}(q^l+1)}{(2, q-1)} \leqslant \frac{1}{q^{2m-2l}} + \frac{1}{q^m - \varepsilon}.$$

Since $2l$ is the dimension of the 1-eigenspace of x, we know that $2m - 2l \geqslant s$. The result now follows in this case.

Case 2: $r = 2$

If $p = 2$, we proceed exactly as described in the proof of Proposition 3.1.3, so assume that $p \neq 2$. The G-classes of semisimple involutions are described in detail in [17, Section 3.5.2]. Since $x \in H$ we may deduce that x has type t_i, t_i' or γ_i for some i, in the notation of [31]. (In particular, [17, Table B.9] makes clear that involutions arising from matrices of order four do not stabilise nondegenerate 1-spaces.) Said otherwise, x lifts to an involution $-I_a \perp I_b$ centralising a decomposition $U_1 \perp U_2$ where U_1 and U_2 are nondegenerate a- and b-spaces. Therefore, either x fixes u and acts as $-I_a \perp I_{b-1}$ on U, or x negates u and acts as $-I_{a-1} \perp I_b$ on U. Therefore, $x^G \cap H = x_1^H \cup x_2^H$ where x_1 and x_2 correspond to the two possible actions of x on u. Consequently,

$$\frac{|x^G \cap H|}{|x^G|} = \frac{|H|}{|G|}\left(\frac{|C_G(x_1)|}{|C_H(x_1)|} + \frac{|C_G(x_2)|}{|C_H(x_2)|}\right).$$

Assume that $a = 2k$ and $b = 2l$; the case where a and b are odd is very similar. From the centraliser orders in [17, Appendix B] we can compute that

$$\frac{|C_G(x_1)|}{|C_H(x_1)|} \leqslant \frac{1}{2}q^{l-1}(q^l+1) \quad \text{and} \quad \frac{|C_G(x_2)|}{|C_H(x_2)|} \leqslant \frac{1}{2}q^{k-1}(q^k+1).$$

Therefore,

$$\frac{|H|}{|G|}\left(\frac{|C_G(x_1)|}{|C_H(x_1)|} + \frac{|C_G(x_2)|}{|C_H(x_2)|}\right) \leqslant \frac{q^{l-1}(q^l+1) + q^{k-1}(q^k+1)}{q^{m-1}(q^m - \varepsilon)} \leqslant \frac{1}{q^{2k}} + \frac{1}{q^{2l}} + \frac{1}{q^m - \varepsilon}.$$

Since $\{2k, 2l\} = \{s, 2m - s\}$, we have verified the result in this case.

Case 3: $r = p > 2$

By Lemma 2.4.7, x is G-conjugate to an element that lifts to a matrix with Jordan form $[J_p^{a_p}, \dots, J_2^{a_2}, J_1^{a_1}]$ where $\sum_{i=1}^{p} ia_i = 2m$. Indeed, the conjugacy class x^G is characterised by this Jordan form together with a sequence $(\delta_1, \delta_3, \dots, \delta_p)$ in $\{\square, \boxtimes\}$ that satisfies the condition $\delta_1\delta_3 \cdots \delta_p = D(Q)$, where Q is the form defining G.

Note that $V = \langle u \rangle \perp U$ since p is odd. Since $x \in H$ and the only eigenvalue of x is 1, the vector u is fixed by x. Since the 1-eigenspace of J_i is totally singular when $i > 1$, we deduce that $a_1 > 0$ and x acts on U as an element whose Jordan form is $[J_p^{a_p}, \dots, J_2^{a_2}, J_1^{a_1-1}]$. Moreover, the corresponding sequence of discriminants for the element $x|_U$ is $(\delta_1\delta, \delta_3, \dots, \delta_p)$, where $\delta = D(Q|_{\langle u \rangle})$. By Lemma 2.4.7, this completely determines the H-class of x. Therefore, $x^G \cap H = x^H$ and the result again follows from the centraliser orders in [17, Appendix B]. This completes the proof. □

A weaker version of the next result appears as Lemma 6.10 in the joint paper [20]; both versions are work of the author of this thesis.

Proposition 3.1.5. *Let G be an almost simple group with socle $\mathrm{Sp}_{2m}(q)$ where $q = 2^f$ and $m \geqslant 2$. Let $x \in G$ have prime order. If $x \in \mathrm{Sp}_{2m}(q)$, then write $s = \nu(x)$. Let $H \leqslant G$ be a maximal subgroup of type $\mathrm{O}^{\pm}_{2m}(q)$. Then*

$$\mathrm{fpr}(x, G/H) \leqslant \begin{cases} q^{-s} + (q^m - 1)^{-1} & \text{if } x \in \mathrm{Sp}_{2m}(q) \\ 2q^{-m} & \text{if } x \notin \mathrm{Sp}_{2m}(q). \end{cases}$$

Proof. Write $G_0 = \mathrm{Sp}_{2m}(q)$ and $H_0 = H \cap G_0 \cong \mathrm{O}^{\varepsilon}_{2m}(q)$. Assume that $x \in H$ and let r be the order of x.

Case 1: $x \in G_0$

First assume that r is odd. The description of the conjugacy classes of semisimple elements of odd order in G_0 and H_0 given in Lemma 2.4.3 implies that $x^{G_0} \cap H_0 = x^{H_0}$. Consequently,

$$\mathrm{fpr}(x, G/H) = \mathrm{fpr}(x, G_0/H_0) = \frac{|x^{G_0} \cap H_0|}{|x^{G_0}|} = \frac{|H_0|}{|G_0|} \frac{|C_{G_0}(x)|}{|C_{H_0}(x)|}.$$

From the centraliser orders given in Lemma 2.4.4 we deduce that

$$\mathrm{fpr}(x, G/H) = \frac{|H_0|}{|G_0|} \frac{|\mathrm{Sp}_e(q)|}{|\mathrm{O}^{\eta}_e(q)|},$$

where the 1-eigenspace of x on $\overline{\mathbb{F}}_2^{2m}$ is an e-dimensional η-type space (if $e = 0$, then we define $\mathrm{Sp}_e(q) = \mathrm{O}^{\eta}_e(q) = 1$). Since $e \leqslant 2m - s$ we deduce that

$$\mathrm{fpr}(x, G/H) \leqslant \frac{|H_0|}{|G_0|} \cdot \frac{1}{2} q^{m-s/2}(q^{m-s/2} + 1) \leqslant \frac{q^{m-s/2}(q^{m-s/2} + 1)}{q^m(q^m - 1)} \leqslant \frac{1}{q^s} + \frac{1}{q^m - 1}.$$

Now assume that $r = 2$. The conjugacy classes of unipotent involutions are described in Lemma 2.4.8. It is easy to see that the G-class and H-class of x have the same Aschbacher–Seitz label (see [17, Remark 3.5.17]), so $x^{G_0} \cap H_0 = x^{H_0}$. The conjugacy class sizes $|x^{H_0}|$ and $|x^{G_0}|$ appear in [13, Proposition 3.22] and the desired bound is easily established. For example, if s is odd and $x = b_s$, then

$$|x^{H_0}| = \frac{|\mathrm{O}^{\varepsilon}_{2m}(q)|}{2|\mathrm{Sp}_{s-1}(q)||\mathrm{Sp}_{2m-2s}(q)|q^{2m(s-1)-3s^2/2+3s/2}}$$
$$|x^{G_0}| = \frac{|\mathrm{Sp}_{2m}(q)|}{|\mathrm{Sp}_{s-1}(q)||\mathrm{Sp}_{2m-2s}(q)|q^{2ms-3s^2/2+s/2}}$$

and thus

$$\mathrm{fpr}(x, G/H) = \frac{1}{q^s}\left(1 + \frac{\varepsilon}{q^r - \varepsilon}\right) \leqslant \frac{1}{q^s}\left(1 + \frac{1}{q^m - 1}\right).$$

Case 2: $x \notin G_0$

If $m = 2$ and x is a graph-field automorphism, then G does not have a maximal subgroup of type $\mathrm{O}^{\varepsilon}_{2m}(q)$. Therefore, we may assume that x is a field automorphism of G_0. Moreover, by Lemma 2.6.20, we may assume that $x = \varphi^i$ where φ is the standard field automorphism of G_0 and $r = f/i$.

We now determine how $x^G \cap H$ splits into H-classes. First assume that r is odd. In this case, the $r - 1$ distinct G-conjugacy classes of order r field automorphisms of G_0 (represented by the nontrivial elements of $\langle\varphi\rangle$) naturally correspond to the $r - 1$ distinct H-classes of order r field automorphisms of H_0 (see Lemmas 2.6.20 and 2.6.24). Therefore, $x^G \cap H = x^H$ and from the centraliser orders in [17, Propositions 3.4.15 and 3.5.20] we obtain

$$\mathrm{fpr}(x, G/H) = \frac{|H|}{|G|}\frac{|C_G(x)|}{|C_H(x)|} = \frac{|\mathrm{O}^{\varepsilon}_{2m}(q)|f}{|\mathrm{Sp}_{2m}(q)|f}\frac{|\mathrm{Sp}_{2m}(q^{1/r})|f}{|\mathrm{O}^{\varepsilon}_{2m}(q^{1/r})|f} < \frac{1}{q^m}.$$

Now assume that $r = 2$. Lemma 2.6.24 implies that there are no involutions in $H \setminus H_0$ if $\varepsilon = -$. Therefore, we may assume that $\varepsilon = +$. In this case, Lemma 2.6.20 implies that there is a unique G-class of involutions in $G \setminus G_0$, which is represented by $\varphi^{f/2}$, but exactly two H-classes of involutions in $H \setminus H_0$ represented by $x_1 = \varphi^{f/2}$ (a field automorphism) and $x_2 = r\varphi^{f/2}$ (a graph-field automorphism). Therefore, $x^G \cap H = x_1^H \cup x_2^H$ and

$$\mathrm{fpr}(x, G/H) = \frac{|\mathrm{O}^{+}_{2m}(q)||\mathrm{Sp}_{2m}(q^{1/2})|}{|\mathrm{Sp}_{2m}(q)|}\left(\frac{1}{|\mathrm{O}^{+}_{2m}(q^{1/2})|} + \frac{1}{|\mathrm{O}^{-}_{2m}(q^{1/2})|}\right) < \frac{2}{q^m}.$$

This completes the proof. □

3.2 Nonsubspace actions

We now turn to fixed point ratios for nonsubspace actions of classical groups, which, in general, are smaller than fixed point ratios for subspace actions. Liebeck and Shalev proved the following general theorem [52].

Theorem 3.2.1. *There exists a constant $\varepsilon > 0$ such that if G is an almost simple classical group, $H \leqslant G$ is a maximal nonsubspace subgroup and $x \in G$ has prime order, then*

$$\mathrm{fpr}(x, G/H) < |x^G|^{-\varepsilon}.$$

An essentially best possible value of ε was determined by Burness in [12, Theorem 1] (see [12, Definition 2] for a precise definition of the *dimension of the natural module*).

Theorem 3.2.2. *Let G be an almost simple classical group with an n-dimensional natural module. If $H \leqslant G$ is a maximal nonsubspace subgroup and $x \in G$ has prime order, then*

$$\mathrm{fpr}(x, G/H) < |x^G|^{-\frac{1}{2}+\frac{1}{n}+\iota}$$

where ι is given in [12, Table 1].

Regarding Theorem 3.2.2, for most subgroups $H \leqslant G$ the parameter ι is simply 0, and whenever $n \geqslant 10$ we have $\iota \leqslant \frac{1}{n-2}$.

Let us now apply Theorem 3.2.2 to the classical groups that we will be interested in.

Proposition 3.2.3. *Let G be an almost simple group with socle $\mathrm{PSp}_{2m}(q)$ or $\Omega_{2m+1}(q)$, where $m \geqslant 3$ and $q = p^f$ with $f \geqslant 2$. Let $H \leqslant G$ be a maximal nonsubspace subgroup and let $x \in G$ have prime order. Let $\ell = 0$, unless either*

(a) $T = \mathrm{PSp}_{2m}(q)$ and H has type $\mathrm{Sp}_m(q) \wr S_2$ or $\mathrm{Sp}_m(q^2)$

(b) $T = \Omega_7(q)$ and H has type $G_2(q)$,

in which case $\ell = 1$. Then

(i) $\mathrm{fpr}(x, G/H) < \sqrt{5}\, q^{-(m-\frac{3}{2}-\ell)}$

(ii) $\mathrm{fpr}(x, G/H) < \sqrt{5}\, q^{-(2m-4-2\ell)}$ *if $\nu(x) \geqslant 2$ or $x \notin \mathrm{PGL}(V)$.*

Proof. Let T be the socle of G. Let n be $2m$ if $T = \mathrm{PSp}_{2m}(q)$ and $2m+1$ if $T = \Omega_{2m+1}(q)$. First assume that $x \in \mathrm{Inndiag}(T)$. From the bounds on conjugacy class sizes presented in [13, Section 3],

$$|x^G| \geqslant |x^T| \geqslant \frac{1}{4}\left(\frac{q}{q+1}\right) q^{2m-1} \geqslant \frac{1}{5}\, q^{2m-1},$$

and if $\nu(x) \geqslant 2$, then

$$|x^G| \geqslant |x^T| \geqslant \frac{1}{4}\left(\frac{q}{q+1}\right) q^{4m-4} \geqslant \frac{1}{5}\, q^{4m-4}.$$

Next assume that $x \in G \setminus \mathrm{Inndiag}(T)$. In this case,

$$|x^G| \geqslant |x^T| \geqslant \frac{|\mathrm{PSp}_{2m}(q)|}{|\mathrm{PGSp}_{2m}(q^{1/2})|} > \frac{1}{2}\, q^{m^2+m/2} \geqslant \frac{1}{5}\, q^{4m-4},$$

noting that $|\mathrm{PSp}_{2m}(q)| = |\Omega_{2m+1}(q)|$ when q is odd.

Therefore, Theorem 3.2.2 implies that

$$\mathrm{fpr}(x, G/H) < |x^G|^{-\frac{1}{2}+\frac{1}{n}+\iota} < \frac{\sqrt{5}}{q^{(2m-1)(\frac{1}{2}-\frac{1}{n}-\iota)}} \leqslant \frac{\sqrt{5}}{q^{m-\frac{3}{2}-\iota(2m-1)}},$$

and if $\nu(x) \geqslant 2$ or $x \notin \mathrm{Inndiag}(T)$,

$$\mathrm{fpr}(x, G/H) < |x^G|^{-\frac{1}{2}+\frac{1}{n}+\iota} < \frac{\sqrt{5}}{q^{(4m-4)(\frac{1}{2}-\frac{1}{n}-\iota)}} \leqslant \frac{\sqrt{5}}{q^{2m-4-\iota(4m-4)}},$$

where $\iota = 0$, unless H is listed in (a) or (b), in which case $\iota \leqslant \frac{1}{n}$. This proves the result. □

Proposition 3.2.4. *Let G be an almost simple group satisfying $\mathrm{P}\Omega^{\varepsilon}_{2m}(q) \leqslant G \leqslant \mathrm{P}\Gamma\mathrm{O}^{\varepsilon}_{2m}(q)$ where $m \geqslant 4$ and $q = p^f$ with $f \geqslant 2$. Let $H \leqslant G$ be a maximal nonsubspace subgroup and let $x \in G$ have prime order. Let $\ell = 0$, unless H has type $\mathrm{GL}^{\pm}_m(q)$, in which case $\ell = 1$. Then*

(i) $\mathrm{fpr}(x, G/H) < 2\, q^{-(m-2-\ell)}$

(ii) $\mathrm{fpr}(x, G/H) < 3\, q^{-(2m-5-2\ell)}$ *if $\nu(x) \geqslant 2$ or $x \notin \mathrm{PGL}(V)$*

Proof. Write $T = \mathrm{P}\Omega^{\varepsilon}_{2m}(q)$. First assume that $x \in \mathrm{PGO}^{\varepsilon}_{2m}(q)$. From the bounds presented in [13, Section 3],

$$|x^G| \geqslant |x^T| \geqslant \frac{1}{4} q^{2m-2},$$

and if $\nu(x) \geqslant 2$, then

$$|x^G| \geqslant |x^T| \geqslant \frac{2^{\delta_{2,p}}}{8} \left(\frac{q}{q+1}\right) q^{4m-6}.$$

Next assume that $x \in \mathrm{P}\Gamma\mathrm{O}^{\varepsilon}_{2m}(q) \setminus \mathrm{PGO}^{\varepsilon}_{2m}(q)$. In this case,

$$|x^G| \geqslant |x^T| \geqslant \frac{|\mathrm{P}\Omega^{+}_{2m}(q)|}{|\mathrm{PDO}^{-}_{2m}(q^{1/2})|} > \frac{1}{4} q^{m(m-1)} \geqslant \frac{1}{4} \left(\frac{q}{q+1}\right) q^{4m-6}.$$

Theorem 3.2.2 now implies that

$$\mathrm{fpr}(x, G/H) < |x^G|^{-\frac{1}{2}+\frac{1}{2m}+\iota} < \frac{4^{\frac{1}{2}}}{q^{(2m-2)(\frac{1}{2}-\frac{1}{2m}-\iota)}} \leqslant \frac{2}{q^{m-2-\iota(2m-2)}},$$

and if $\nu(x) \geqslant 2$ or $x \notin \mathrm{PGO}^{\varepsilon}_{2m}(q)$, then

$$\mathrm{fpr}(x, G/H) < |x^G|^{-\frac{1}{2}+\frac{1}{2m}+\iota} < \frac{\left(8/2^{\delta_{2,p}} \cdot \frac{q+1}{q}\right)^{1/2}}{q^{(4m-6)(\frac{1}{2}-\frac{1}{2m}-\iota)}} \leqslant \frac{3}{q^{2m-5-(4m-6)\iota}},$$

where $\iota = 0$ unless H has type $\mathrm{GL}^{\pm}_m(q)$ and $\iota = (2m-2)^{-1}$. This proves the result. □

The four-dimensional symplectic groups require special attention and we will provide a close to best possible fixed point ratio bound for these groups.

This appears as Proposition 3.6 in the author's paper [38].

Proposition 3.2.5. *Let $q = p^f$ where $f > 1$ and let G be an almost simple group with socle $\mathrm{PSp}_4(q)$. For a maximal nonsubspace subgroup $H \leqslant G$ and a prime order element $x \in G$*

$$\mathrm{fpr}(x, G/H) \leqslant \frac{4}{q(q-1)},$$

unless H has type $\mathrm{Sp}_2(q) \wr S_2$ or $\mathrm{Sp}_2(q^2)$ and x is an a_2 or t_2 involution, in which case

$$\mathrm{fpr}(x, G/H) \leqslant \frac{q}{q^2-1}.$$

Moreover, we have the following stronger bounds when q is even.

(i) *If H has type ${}^2B_2(q)$, then $\mathrm{fpr}(x, G/H) \leqslant q^{-2}$.*

(ii) *If H has type $\mathrm{O}_2^-(q^2)$, then $\mathrm{fpr}(x, G/H) \leqslant 8\,q^{-2}(q-1)^{-1}$.*

Proof. Let x have prime order r. We may assume that $x \in H$. By [7, Tables 8.12–8.14], the possibilities for the type of H are the following, where k is a prime divisor of f

- in all cases:

type	$\mathrm{Sp}_4(q^{1/k})$	${}^2B_2(q)$	$\mathrm{PSL}_2(q)$
condition		q even & f odd	q odd

- if G does not contain a graph-field automorphism:

type	$\mathrm{Sp}_2(q) \wr S_2$	$\mathrm{GL}_2(q)$	$\mathrm{Sp}_2(q^2)$	$\mathrm{GU}_2(q)$
condition		q odd		q odd

- if G contains a graph-field automorphism:

type	$\mathrm{O}_2^+(q) \wr S_2$	$\mathrm{O}_2^-(q) \wr S_2$	$\mathrm{O}_2^-(q^2)$

Write $T = \mathrm{PSp}_4(q)$, $G_0 = G \cap \mathrm{PGSp}_4(q)$ and $H_0 = H \cap G_0$. Assume that H does not have type $\mathrm{PSL}_2(q)$ since the calculation for this case is in [14, Proposition 2.22].

Case 1: $x \in G_0$

Suppose for now that H does not have type ${}^2B_2(q)$. We proceed as in the proof of Proposition 3.1.3. The splitting of x^{G_0} into H_0-classes is straightforward to determine, except for involutions when q is odd. For these elements the arguments are often more subtle. We present the example where q is odd, x is an involution and H has type $\mathrm{GU}_2(q)$.

Write $H_0 = B{:}\langle\iota\rangle$ where B is the image of $\mathrm{GU}_2(q)$ in $\mathrm{Sp}_4(q)$ modulo scalars, and ι induces the inverse-transpose map on B. First assume that $x \in B$. By Lemma 2.5.7(i), any element of $\mathrm{GU}_2(q)$, modulo scalars, with eigenvalue multiset $\{\lambda, \mu\}$ has an image in B with eigenvalue multiset $\{\lambda, \lambda^q, \mu, \mu^q\}$. Following [31], there are two classes of involutions in B. The t_1 class is represented by an element which lifts to $[-1, 1]$, so embeds in G_0 as $[-I_2, I_2]$, a t_1 involution of G_0. If $q \equiv 1 \pmod 4$, then the second class is represented by t_1', which lifts to $[\xi, \xi^{-q}]$, where ξ has order 4 in $\mathbb{F}_{q^2}^\times$. In this case, $\xi \in \mathbb{F}_q$ and so $[\xi, \xi^{-q}] = [\xi, \xi^{-1}]$ embeds in G_0 as $[\xi I_2, \xi^{-1} I_2] \in G_0$, a t_2 involution of G_0. If $q \equiv 3 \pmod 4$, then the second class arises from central involutions z which lift to $[\lambda, \lambda]$, where $\lambda \in \mathbb{F}_{q^2}^\times$ has order 4. Since $\lambda \notin \mathbb{F}_q$, z embeds in G_0 as a t_2' involution. Now assume that $x \in H_0 \setminus B$. Then x lifts to $A\iota$ such that $(A\iota)^2 \in \{I, -I\}$. That is, A is either symmetric or skew-symmetric. Moreover, x has a 1-eigenvector, and hence embeds as $t_1 \in G_0$, if and only if A is skew-symmetric. Therefore, we have determined how $x^{G_0} \cap H_0$ splits into H_0 classes, and the result follows as in the proof of Proposition 3.1.3. For example, if x is a t_1 involution and $G_0 = \mathrm{PSp}_4(q)$ then, since there are $q+1$ skew-symmetric matrices in $\mathrm{GU}_2(q)$,

$$\mathrm{fpr}(x, G/H) = \frac{|x^{G_0} \cap H_0|}{|x^{G_0}|} = \frac{|\mathrm{Sp}_2(q)|^2}{|\mathrm{PSp}_4(q)|}\left(\frac{|\mathrm{GU}_2(q)|}{2|\mathrm{GU}_1(q)|^2} + \frac{q+1}{2}\right) = \frac{1}{q^2}.$$

Now consider the case where H has type ${}^2B_2(q)$. By [13, Proposition 3.52], either $x = c_2$ or $x = [\lambda_1, \lambda_1^{-1}, \lambda_2, \lambda_2^{-1}]$ for $\lambda_1 \neq \lambda_2$. For the former case, we use the fact that $|x^T \cap H_0|$ is at most $(q-1)(q^2+1)$, the number of involutions in ${}^2B_2(q)$. In the latter case, the bound $|x^T \cap H_0| \leqslant |H_0|$ suffices.

The stronger bound for the subgroup of type $\mathrm{O}_2^-(q^2)$ is obtained by observing that, in this case, H_0 does not contain any involutions of type a_2 or b_1 (see [17, Proposition 5.9.2]).

Case 2: x is a field automorphism

Assume that if H has type $\mathrm{Sp}_4(q^{1/k})$ then $r \neq k$, and if $H \in \mathcal{C}_2$ or $H \in \mathcal{C}_3$ then $r \neq 2$. The calculations in these cases are similar and we will present an example below. If these conditions are not satisfied, then the situation is slightly more complicated. We will demonstrate how to handle this when $r = 2$ and $H \in \mathcal{C}_2$ before outlining the other cases.

Consider the case where H has type $\mathrm{Sp}_2(q) \wr S_2$. Let $H_0 = B{:}\langle\pi\rangle$ where $B \leqslant H_0$ is the index two subgroup of type $\mathrm{Sp}_2(q) \times \mathrm{Sp}_2(q)$. By Lemma 2.6.27, we may assume that x is a power of the standard field automorphism. Moreover, we may choose π such that π and x commute. Since $|x^G|$ is at most the number of elements of order r in Tx, $|x^G \cap H|$ is at most the number of elements of order r in $Tx \cap H = H_0 x = Bx \cup B\pi x$. If $r \neq 2$, then, since π has order two and commutes with x, no element of $B\pi x$ has order r. In this case, $|x^G \cap H|$ is at most the number of elements of order r in Bx which, by [31, Proposition 4.9.1(d)], is at most $2|x^H|$. If $r = 2$, then the previous argument gives the number of involutions in Bx, so it remains to determine the number of involutions in $B\pi x$.

Let $g\pi x \in B\pi x$ be an involution. Suppose that g lifts to $[M, N] \in \mathrm{GSp}_2(q) \times \mathrm{GSp}_2(q)$. Then for $\lambda \in \mathbb{F}_q$,

$$\lambda[I, I] = ([M, N]\pi x)^2 = [M, N][M, N]^{\pi x} = [MN^x, NM^x].$$

Hence, $\lambda \in \{1, -1\}$ and $N = \lambda M^{-x}$. Therefore, there are at most $2|\mathrm{Sp}_2(q)| = 2q(q^2 - 1)$ involutions in $B\pi x$. The bound follows.

Let us now remark on the remaining subtleties. First, if $r = 2$ and H has type $\mathrm{Sp}_2(q^2)$ or $\mathrm{GU}_2(q)$, then $\mathrm{fpr}(x, G/H) = 0$. To see this, suppose that $G = \mathrm{PSp}_4(q){:}\langle\sigma\rangle$ and that $H = \mathrm{PSp}_2(q^2){:}\langle\tau\rangle$ where σ is a field automorphism of $\mathrm{PSp}_4(q)$ of order e and τ is a field automorphism of $\mathrm{PSp}_2(q^2)$ of order $2e$; the other cases are similar. If $x \notin \mathrm{PSp}_2(q^2)$ is an involution, then $x = g\tau^e$ for some $g \in \mathrm{PSp}_2(q^2)$. However, $g\tau^e \in \mathrm{PSp}_2(q^2){:}\langle\tau^e\rangle = H \cap G_0$, so $x \in G_0$, which is a contradiction.

Now let H have type $\mathrm{Sp}_4(q^{1/k})$ with $r = k$. For $S \subseteq G$, let $i_r(S)$ be the number of elements of S of order r. Although $|x^G \cap H| = i_r(H_0x)$, we cannot argue that $i_r(H_0x) = |x^H|$ since x commutes with H_0. Therefore, we need to explicitly bound $i_r(H_0x) \leqslant 1 + i_r(H_0)$. If $r \geqslant 5$, then the bound $i_r(H_0) \leqslant |H_0| \leqslant q^2$ suffices. If $r \in \{2, 3\}$, we obtain the result by using the bounds in [45, Proposition 1.3]; in particular, $i_2(H_0) \leqslant 2(q^{3/2} + q)$ and $i_3(H_0) \leqslant 2(q^{11/9} + q^{8/9})$.

Case 3: x is a graph-field automorphism

In this case $r = p = 2$. If $H_0 = \mathrm{Sp}_4(q^{1/k})$, then the argument is the same as for field automorphisms. Next, if $H_0 = {}^2B_2(q)$, then, as above, x commutes with H_0 and we note that $i_2({}^2B_2(q)) = (q - 1)(q^2 + 1)$. Finally, if H has type $\mathrm{O}_2^\varepsilon(q) \wr S_2$ or $\mathrm{O}_2^-(q^2)$, then, since H is a split extension of H_0 by a cyclic group of order $2e = |H : H_0|$, there are at most $|H|/e = 2|H_0|$ elements of order 2 in H. The bound $|x^G \cap H| \leqslant 2|H_0|$ suffices. □

Our final result in this section is a bound relating to subfield subgroups. Before giving this result, let us record two useful technical lemmas. The first is a straightforward observation (see, for example, [17, Appendix B]).

Lemma 3.2.6. *Let G be $\mathrm{Sp}_{2m}(q)$ or $\mathrm{O}_n^\varepsilon(q)$ where $\varepsilon \in \{+, -, \circ\}$. Let $g \in G$ have prime order. Then $v(g) = 1$ if and only if one of the following hold*

(i) *$G = \mathrm{O}_{2m}^\pm(q)$ for even q or $G = \mathrm{Sp}_{2m}(q)$, and g has Jordan form $[J_2, I_{2m-2}]$*

(ii) *$G = \mathrm{O}_n^\varepsilon(q)$ for odd q and, modulo scalars, $g = -I_1 \perp I_{n-1}$.*

The next result is proved in [43, p.145].

Lemma 3.2.7. *Let $q = q_0^k$ and let $V_0 = \mathbb{F}_{q_0}^{2m}$ be equipped with a nondegenerate ε-type quadratic form Q_0. Then the quadratic form Q induced on $V = V_0 \otimes_{\mathbb{F}_{q_0}} \mathbb{F}_q$ is ε^k-type.*

Proposition 3.2.8. *Let G be an almost simple group with socle $\mathrm{PSp}_{2m}(q)$ or $\Omega_{2m+1}(q)$. Let $H \leqslant G$ be a maximal subfield subgroup. Let $x \in G \cap \mathrm{PGL}_{2m}(q)$ have prime order and satisfy $\nu(x) = 1$. Then*

$$\mathrm{fpr}(x, G/H) < \frac{2}{q^m}.$$

Proof. The possibilities for x are recorded in Lemma 3.2.6. Let us prove the result when $G = \mathrm{SO}_{2m+1}(q)$; the other cases are similar. Therefore, let $H = \mathrm{SO}_{2m+1}(q_0)$ where $q_0^k = q$ for a prime k dividing f. We may assume that $x \in H$ has type $I_1 \perp -I_{2m}$ and centralises a decomposition $\mathbb{F}_{q_0}^{2m+1} = U_0 \perp W_0$. Then x, as an element of G, centralises the decomposition $\mathbb{F}_q^{2m+1} = U \perp W$, where $U = U_0 \otimes_{\mathbb{F}_{q_0}} \mathbb{F}_q$ and $W = W_0 \otimes_{\mathbb{F}_{q_0}} \mathbb{F}_q$.

The G-class and H-class of x are characterised by the signs of the spaces W and W_0, respectively (see [17, Sections 3.5.2.1 and 3.5.2.2]). Write $\mathrm{sgn}(W) = \varepsilon$ and $\mathrm{sgn}(W_0) = \varepsilon_0$. By Lemma 3.2.7, $\varepsilon_0^k = \varepsilon$. Therefore, if k is odd, then $x^G \cap H = x^G$. However, if $k = 2$, then for $\varepsilon = -$ we have $|x^G \cap H| = 0$ and for $\varepsilon = +$ we have $x^G \cap H = x_+^H \cup x_-^H$ where x_η is an involution with an η-type -1-eigenspace.

Consequently,

$$\frac{|x^G \cap H|}{|x^G|} \leqslant \frac{|\mathrm{SO}_{2m+1}(q^{1/2})||\mathrm{SO}_{2m}^+(q)|}{|\mathrm{SO}_{2m+1}(q)|} \left(\frac{1}{|\mathrm{SO}_{2m}^+(q^{1/2})|} + \frac{1}{|\mathrm{SO}_{2m}^-(q^{1/2})|} \right) \leqslant \frac{2}{q^m + 1}$$

and the result follows. □

4

Groups of Types B_m and C_m

The work in this chapter is heavily drawn from the publication

> S. Harper, *On the uniform spread of almost simple symplectic and orthogonal groups*, J. Algebra **490** (2017), 330–371.

We now begin to prove the main results of this thesis. This chapter will focus on almost simple groups G of type B_m and C_m, or said otherwise groups G whose socle T is a symplectic or odd-dimensional orthogonal group. These groups are structurally quite similar and we aim to handle these two cases together in a reasonably uniform manner.

Before commencing with details of the proof, let us state the main results for groups of type B_m and C_m and discuss some of the general ideas that arise in the proof.

In this chapter we write

$$\mathcal{T} = \mathcal{T}_{\mathsf{BC}} = \{\mathrm{PSp}_{2m}(q) \mid m \geqslant 2 \text{ and } (m,q) \neq (2,2)\} \cup \{\Omega_{2m+1}(q) \mid q \text{ odd}, m \geqslant 3\} \quad (4.1)$$

$$\mathcal{A} = \mathcal{A}_{\mathsf{BC}} = \{\langle T, \theta \rangle \mid T \in \mathcal{T}_{\mathsf{BC}},\ \theta \in \mathrm{Aut}(T)\}. \quad (4.2)$$

Remark. In the definition of $\mathcal{T}$, we exclude $\mathrm{Sp}_4(2) \cong S_6$, since this group is not simple. For the avoidance of doubt, let us discuss the spread and uniform spread of $\mathrm{Sp}_4(2)' \cong A_6$ and its three cyclic extensions: S_6, $\mathrm{PGL}_2(9)$ and M_{10}. It is well known that $u(A_6) = 2$ and $u(S_6) = 0$ but $s(S_6) = 2$. Moreover, by computing in MAGMA (see Section 2.8) we can show that $u(\mathrm{PGL}_2(9)) = 5$ and $u(\mathrm{M}_{10}) \geqslant 8$.

The two main results of this chapter are the following.

Theorem 4A. *If $G \in \mathcal{A}$, then $u(G) \geqslant 2$.*

Theorem 4B. *Let (G_i) be a sequence of groups in $\mathcal{A}$ with $|G_i| \to \infty$. Then $u(G_i) \to \infty$ if and only if (G_i) does not have an infinite subsequence of groups over a field of fixed size whose socles are either symplectic groups in even characteristic or odd-dimensional orthogonal groups.*

Moreover, in this chapter we will actually prove stronger results than the two headline theorems above. If we exclude some cases, we can tighten the bound in Theorem 4A.

Theorem 4C. *Let $G \in \mathcal{A}$. Assume that q is odd and $m \geqslant 3$. If $\mathrm{soc}(G) = \Omega_{2m+1}(q)$ then $u(G) \geqslant 3$, and if $\mathrm{soc}(G) = \mathrm{PSp}_{2m}(q)$ then $u(G) \geqslant 4$.*

We can find explicit bounds for the groups in Theorem 4B with bounded uniform spread.

Theorem 4D. *Let $G \in \mathcal{A}$. If q is even, $\mathrm{soc}(G) = \mathrm{PSp}_{2m}(q)$ and θ is not a graph-field automorphism, then $s(G) \leqslant q$. If $\mathrm{soc}(G) = \Omega_{2m+1}(q)$, then $s(G) < \frac{q^2+q}{2}$.*

Remark. Let q be even. Write $G = \langle T, \theta \rangle$ where $T = \mathrm{Sp}_{2m}(q)$ and $\theta \in \mathrm{Aut}(T)$.

(i) In [37, Proposition 2.5], Guralnick and Shalev prove that $s(T) \leqslant q$. Theorem 4D extends this result by establishing that $s(G) \leqslant q$ if θ is a field automorphism.

(ii) If $m = 2$, $q = 4$ and θ is an involutory field automorphism, then a MAGMA computation verifies that $u(G) = 4$, so the bound for symplectic groups in Theorem 4D is sharp. Moreover, by Proposition 4.3.21(iii), if $m \geqslant 16$ and $\theta \in \mathrm{Aut}(T) \setminus T$, then $q - 1 \leqslant u(G) \leqslant s(G) \leqslant q$, so the upper bound for symplectic groups in Theorem 4D is close to best possible in large rank.

(iii) The upper bound in Theorem 4D does *not* apply when $m = p = 2$ and θ is a graph-field automorphism. Indeed, in this case, if $q = 4$ then $u(G) \geqslant 10$, and, strikingly, if $q = 8$ and θ has order two then $u(G) \geqslant 76$. This behaviour is captured by Proposition 4.4.8(iii), which establishes that if θ is an involutory graph-field automorphism then $u(G) \geqslant q^2/18$. In particular, this gives an infinite family of groups G where $|u(G) - u(\mathrm{soc}(G))|$ is unbounded.

Let us now discuss the proofs. Let $G = \langle T, \theta \rangle \in \mathcal{A}$ with $T \in \mathcal{T}$. To prove that $u(G) \geqslant k$, we adopt the probabilistic approach introduced by Guralnick and Kantor in [33] (see Section 2.1). Recall that this approach has three stages. First we must fix an element $s \in G$. In order for s^G to witness $u(G) \geqslant k$, the element s cannot be contained in a proper normal subgroup of G, so we may assume that $s \in T\theta$. Consequently we need to understand the conjugacy classes in the coset $T\theta$. We then study the set $\mathcal{M}(G, s)$ of maximal subgroups of G that contain s, before showing that every prime order element $x \in G$ satisfies

$$P(x, s) \leqslant \sum_{H \in \mathcal{M}(G,s)} \mathrm{fpr}(x, G/H) < \frac{1}{k}.$$

We can now sketch our proof.

Generically, the almost simple groups G we consider will be extensions of the socle T by diagonal automorphisms (elements of $\mathrm{Inndiag}(T) \setminus T$), field automorphisms and products thereof. The precise cases to be considered will be determined in Section 4.1 (see Proposition 4.1.5 in particular).

If θ is diagonal, then $G = \langle T, \theta \rangle \leqslant \mathrm{PGL}(V)$ and we can employ methods similar to those used by Breuer, Guralnick and Kantor in [10]. In particular, we can think of the elements in $T\theta$ as matrices (modulo scalars). This is our focus in Section 4.2.

However, when θ is not a diagonal automorphism, then we adopt a different approach and view $G = \langle T, \theta \rangle$ from the perspective of algebraic groups, which we introduced in Section 2.6. This viewpoint allows us to employ the technique of Shintani descent described in Section 2.7. Central to this method is a bijection F with useful group theoretic properties that, given a connected algebraic group X, a Steinberg endomorphism σ of X and an integer $e > 1$, provides a correspondence between the conjugacy classes of elements in the coset $X_{\sigma^e}\sigma$ and in the subgroup X_σ. The main idea, therefore, is to write $\mathrm{Inndiag}(T) = X_\sigma$ and $\theta \in \mathrm{Inndiag}(T)\sigma$ for a suitable connected algebraic group X and Steinberg endomorphism σ (see Example 2.7.2). We may then select an element $s \in T\theta$ as the preimage under F of a judiciously chosen element $x \in X_\sigma$ (see Proposition 4.3.5).

Once we have thus selected $s \in G$, the idea is to exploit features of the element $x = F(s)$ and properties of the map F (see Section 2.7.3) in order to determine a superset of $\mathcal{M}(G, s)$ (see Theorem 4.3.7). Here Aschbacher's subgroup structure theorem (Theorem 2.5.1) provides our framework. This is the stage that will require the most work. Once this is complete, we can bound the probability $P(x, s)$ using the fixed point ratio estimates from Chapter 3.

Let us highlight now some particularly interesting or subtle features of the proof.

Element orders

A common technique for identifying an element of a classical group that is contained in few maximal overgroups, is to choose an element with a large and restrictive order. For instance, if $s \in \mathrm{GL}_n(q)$ has order divisible by a primitive prime divisor of $q^k - 1$ for $k > \frac{n}{2}$, then the subgroups $H \leqslant \mathrm{GL}_n(q)$ that contain s are classified by the main theorem of [35] (see Theorem 2.5.5 for a convenient statement of a related result).

However, this technique will, in general, *not* be useful in our proofs. To see why, consider the example where $G = \langle \mathrm{PSp}_{2m}(p^f), \varphi \rangle$ and φ is the standard order f field automorphism. Then, via Shintani descent, we choose an element $t\varphi \in G$ such that $(t\varphi)^f$ is conjugate to an element of $\mathrm{PSp}_{2m}(p)$. Therefore, $t\varphi$, and even more so $(t\varphi)^f$, which is the element we typically have better information about, has a small order compared with the order of G. Consequently, we will need to use other properties of the element $t\varphi$ in order to constrain its maximal overgroups.

Shintani splitting

Assume that q is odd. As described above, Shintani descent will provide a bijection F between the conjugacy classes in the coset $\mathrm{Inndiag}(T)\theta$ and conjugacy classes in a particular subgroup $\mathrm{Inndiag}(T_0)$. Since we want to select an element $s \in T\theta$, we need to know which elements in $\mathrm{Inndiag}(T_0)$ have preimages under F in $T\theta$. By exploiting properties of Shintani descent, we will see that F restricts to a bijection between classes in $T\theta$ and T_0 (see Lemmas 4.3.2 and 4.3.3). For symplectic groups, there is a concrete means of seeing this which naturally generalises work of Burness and Guest for linear groups [18, Lemma 4.2] (see Remark 4.3.4); however, orthogonal groups are not amenable to this approach, so we develop a new approach for establishing this restriction, which applies uniformly to all classical groups (see Lemma 2.7.4 and Example 2.7.5).

Reducible subgroups

Subspace subgroups have comparatively large fixed point ratios. Therefore, we will pay particular attention to determining the maximal subspace overgroups of s. For linear and symplectic groups, subspace stabilisers arise from closed connected subgroups of the ambient algebraic group, so Lemma 2.7.9 is the key tool (see also Example 2.7.10). However, the stabiliser of a nondegenerate subspace in an orthogonal group is disconnected, so we need to modify our approach. The idea is to use the inclusion $\mathrm{SO}_{2m+1}(\overline{\mathbb{F}}_p) \leqslant \mathrm{SL}_{2m+1}(\overline{\mathbb{F}}_p)$ and lift the Shintani map for $\mathrm{SO}_{2m+1}(\overline{\mathbb{F}}_p)$ to one for $\mathrm{SL}_{2m+1}(\overline{\mathbb{F}}_p)$, where the corresponding reducible subgroups are connected (see Proposition 4.3.9).

Orthogonal subgroups

If $T = \mathrm{Sp}_{2m}(2^f)$, then in addition to reducible subgroups, the subgroups of type $\mathrm{O}^{\pm}_{2m}(2^f)$ are subspace subgroups of G. Determining which subgroups of this type contain s will require particular attention and is a novel feature of our work (see Proposition 4.3.13).

Graph-field automorphisms

The group $\mathrm{Sp}_4(q)$ is an exceptional case since when q is even it has a graph-field automorphism. Since this automorphism naturally arises from a Steinberg endomorphism of the associated algebraic group, we can still apply Shintani descent in the general setup. However, the study of $\mathcal{M}(G, s)$ will require arguments of a different style and we will use the bespoke fixed point ratio bound obtained in Proposition 3.2.3 (see Section 4.4).

The above discussion motivates the following partition of the proof of our main theorems

I $\theta \in \mathrm{Inndiag}(T)$

II $m \geqslant 3$, $\theta \in \mathrm{Aut}(T) \setminus \mathrm{Inndiag}(T)$

III $m = 2$, $\theta \in \mathrm{Aut}(T) \setminus \mathrm{Inndiag}(T)$

In Section 4.1, we will determine the precise cases to be considered to prove Theorems 4A–4D, and these theorems, in each of Cases I–III, will be proved in Sections 4.2–4.4.

4.1 Automorphisms

Let $T \in \mathcal{T}$. This section's principal aim is to determine the automorphisms $\theta \in \mathrm{Aut}(T)$ we need to consider in order to prove Theorems 4A and 4B, and the main result to this end is Proposition 4.1.5.

4.1.1 Preliminaries

We begin with some preliminary observations, which we will also use in Section 5.1. For $g \in \mathrm{Aut}(T)$, write $\ddot{g}$ for the set Tg. Therefore, $\mathrm{Out}(T) = \{\ddot{g} \mid g \in \mathrm{Aut}(T)\}$. The following is straightforward.

Lemma 4.1.1. *Let T be a simple group and let $g, h \in \mathrm{Aut}(T)$. If the elements $\ddot{g}$ and $\ddot{h}$ are $\mathrm{Out}(T)$-conjugate, then the subgroups $\langle T, g\rangle$ and $\langle T, h\rangle$ are $\mathrm{Aut}(T)$-conjugate.*

The following elementary observation is useful.

Lemma 4.1.2. *Let $S = \langle a\rangle{:}\langle b\rangle$ be a semidirect product of finite cyclic groups. For all $i > 0$ there exists $j, k \in \mathbb{N}$ such that $\langle ab^i\rangle = \langle a^j b^k\rangle$ and k divides $|b|$.*

Proof. Let $i > 0$. We will repeatedly use the fact that, since $\langle a\rangle \trianglelefteqslant S$, for all $l \in \mathbb{N}$

$$(ab^i)^l \in \langle a\rangle b^{il}. \tag{4.3}$$

Write $|b| = n$, and let k divide n and satisfy $\langle b^i\rangle = \langle b^k\rangle$. Now let r be the least positive integer such that $b^{ir} = b^k$. By (4.3), $|ab^i| = s|b^i|$. Let d be the product of the distinct prime divisors of s which do not divide r. Then, by (4.3), $(ab^i)^{r+d|b^i|} = a^j b^k$ for some $j \in \mathbb{N}$. Therefore, $\langle a^j b^k\rangle \leqslant \langle ab^i\rangle$.

Recall that $|ab^i| = s|b^i|$. Note that $(r + d|b^i|, |b^i|) = (r, |b^i|) = 1$ as $\langle b^{ir}\rangle = \langle b^i\rangle$. Let t be a prime divisor of s. If t does not divide r, then t does not divide $r + d|b^i|$ since t divides d. Now assume that t divides r. If t divides $r + d|b^i|$, then t divides $d|b^i|$, so t divides $|b^i|$ since t does not divide d. However, this implies that t divides $(r, |b^i|) = 1$, which is a contradiction. Therefore, t does not divide $r + d|b^i|$. Consequently, $(r + d|b^i|, s) = 1$. We now conclude that $(r + d|b^i|, s|b^i|) = 1$, so $\langle a^j b^k\rangle = \langle ab^i\rangle$, which proves the claim. □

4.1.2 Symplectic groups

Let $q = p^f$ and let $n = 2m$. Let T be $\mathrm{PSp}_{2m}(q)$. We recorded $\mathrm{Aut}(T)$ in Lemmas 2.6.18(i) and 2.6.25. In this section, we give further information about $\mathrm{Out}(T)$.

For this section, we fix the standard Frobenius endomorphism $\varphi = \varphi_{\mathcal{B}}\colon (a_{ij}) \mapsto (a_{ij}^p)$ (see Definition 2.6.9) defined with respect to the basis $\mathcal{B} = (e_1, f_1, \ldots, e_m, f_m)$ (see (2.4)). Write $\mathbb{F}_q^\times = \langle\alpha\rangle$. If q is odd, then let $\beta \in \mathbb{F}_q^\times$ with $|\beta| = (q-1)_2$ and note $\alpha, \beta \notin (\mathbb{F}_q^\times)^2$.

We now define an element, which we will also make use of in Chapter 5.

Definition 4.1.3. Let q be odd. With respect to the basis $\mathcal{B}$ for $\mathbb{F}_q^{2m}$, define $\hat{\delta}^+ \in \mathrm{GL}_{2m}(q)$ as the element $\beta I_m \oplus I_m$, centralising the decomposition $\langle e_1, \ldots, e_m \rangle \oplus \langle f_1, \ldots, f_m \rangle$ and let $\delta^+ \in \mathrm{PGL}_{2m}(q)$ be the image of $\hat{\delta}^+$.

Remark 4.1.4. We comment on Definition 4.1.3.

(i) Note that $\hat{\delta}^+$ is a similarity with $\tau(\hat{\delta}^+) = \beta$ and $\det(\hat{\delta}^+) = \beta^m$ (see Lemma 2.3.21).

(ii) In Chapter 4, we will refer to δ^+ simply as δ.

(iii) In [43, Section 2], the symbol δ refers to an element of $\mathrm{GL}_{2m}(q)$, but we prefer to use this symbol for an element of $\mathrm{PGL}_{2m}(q)$. Our definition of δ also has a less cosmetic difference: both versions centralise the decomposition $\langle e_1, \ldots, e_m \rangle \oplus \langle f_1, \ldots, f_m \rangle$, but we work with $\beta I_m \oplus I_m$ rather than $\alpha I_m \oplus I_m$. However, both versions give the same element $\ddot{\delta}$. To see this, write $k = ((q-1)_{2'} - 1)/2$ and note that

$$(\alpha I_m \oplus I_m) \cdot (\alpha^k I_m \oplus \alpha^{-k} I_m) \cdot \alpha^k I_{2m} = \beta I_m \oplus I_m$$

where $(\alpha^k I_m \oplus \alpha^{-k} I_m) \in \mathrm{Sp}_{2m}(q)$ and $\alpha^k I_{2m}$ is a scalar. Therefore, our notation for elements of $\mathrm{Out}(T)$ is consistent with [43].

By [43, Proposition 2.4.4], if $(m, p) \neq (2, 2)$, then

$$\mathrm{Out}(T) = \begin{cases} \langle \ddot{\varphi} \rangle \cong C_f & \text{if } q \text{ is even} \\ \langle \ddot{\delta} \rangle \times \langle \ddot{\varphi} \rangle \cong C_2 \times C_f & \text{if } q \text{ is odd.} \end{cases} \tag{4.4}$$

Now suppose that $m = p = 2$. Then $T = \mathrm{Sp}_4(q)$ has a *graph-field* automorphism ρ such that $\rho^2 = \varphi$ (see [23, Proposition 12.3.3]) and

$$\mathrm{Out}(T) = \langle \ddot{\rho} \rangle \cong C_{2f}. \tag{4.5}$$

If i is an odd divisor of f, then $\rho^i \in \mathrm{Aut}(T) \setminus \Gamma\mathrm{Sp}_4(q)$ and $C_T(\rho^i) = {}^2B_2(p^i)$, which is the *Suzuki group* (often also denoted by $Sz(p^i)$).

It follows from (2.17) that, for all m and q, the innerdiagonal group of T is

$$\mathrm{Inndiag}(T) = \begin{cases} T & \text{if } q \text{ is even} \\ \langle T, \delta \rangle & \text{if } q \text{ is odd.} \end{cases} \tag{4.6}$$

4.1.3 Orthogonal groups

Let $q = p^f$ be odd and let $n = 2m + 1$. Let T be $\Omega_{2m+1}(q)$. We gave $\mathrm{Aut}(T)$ in Lemma 2.6.18(ii), and we now further describe $\mathrm{Out}(T)$.

Write $\varphi = \varphi_{\mathcal{B}}$ where $\mathcal{B}$ is the basis $(e_1, f_1, \ldots, e_m, f_m, x)$ from (2.7). Fix $r_\square, r_\boxtimes \in \mathrm{SO}_{2m+1}(q)$ as reflections in vectors of square and nonsquare norms (see Section 2.2.4).

Table 4.1: The relevant automorphisms in types B_m and C_m

	I	II/III	
	1	φ^i	(1)
θ	δ	$\delta\varphi^i$	(2)
	$r_\square r_\boxtimes$	$r_\square r_\boxtimes \varphi^i$	(3)

[i is a proper divisor of f]

By [43, Proposition 2.6.3],

$$\mathrm{Out}(T) = \langle \ddot{r}_\square \ddot{r}_\boxtimes \rangle \times \langle \ddot{\varphi} \rangle \cong C_2 \times C_f. \tag{4.7}$$

As a consequence of (2.18) we have

$$\mathrm{Inndiag}(T) = \langle T, r_\square r_\boxtimes \rangle. \tag{4.8}$$

4.1.4 Cases to consider

We now present a useful reduction of Theorems 4A and 4B.

Proposition 4.1.5. *Let $T \in \mathcal{T}$. To prove that $u(G) \geqslant k$ for all $G \in \mathcal{A}$ with socle T, it suffices to show $u(\langle T, \theta \rangle) \geqslant k$ for all of the following*

(i) *θ in Row (1) of Table 4.1*

(ii) *θ in Row (2) of Table 4.1, if q is odd and $T = \mathrm{PSp}_{2m}(q)$*

(iii) *θ in Row (3) of Table 4.1, if q is odd and $T = \Omega_{2m+1}(q)$*

(iv) *$\theta = \rho^i$ for an odd proper divisor i of f, if q is even and $T = \mathrm{Sp}_4(q)$.*

Proof. Let $G = \langle T, g \rangle$ for an automorphism $g \in \mathrm{Aut}(T)$. For now assume that T is not $\mathrm{Sp}_4(2^f)$. By inspecting the structure of $\mathrm{Out}(T)$ given in (4.4) and (4.7), it is manifest that we may write $g = th\varphi^i$ where $t \in T$ and h is 1 or δ (when $T = \mathrm{PSp}_{2m}(q)$) or $r_\square r_\boxtimes$ (when $T = \Omega_{2m+1}(q)$). Since $\langle T, th\varphi^i \rangle = \langle T, h\varphi^i \rangle$, we may assume, in fact, that $g = h\varphi^i$.

If $i > 0$, then, since $\langle \ddot{h}, \ddot{\varphi} \rangle = \langle \ddot{h} \rangle \times \langle \ddot{\varphi} \rangle$, by Lemma 4.1.2, there exist $j, k \in \mathbb{N}$ with k dividing f such that $\langle \ddot{h}\ddot{\varphi}^i \rangle = \langle \ddot{h}^j \ddot{\varphi}^k \rangle$ and, consequently, $\langle T, h\varphi^i \rangle = \langle T, h^j \varphi^k \rangle$. Therefore, we may assume that $i = 0$ or i divides f. This implies that $\langle T, g \rangle = \langle T, \theta \rangle$ for an automorphism θ in Table 4.1.

It remains to assume that $T = \mathrm{Sp}_4(2^f)$. In this case $g = t\rho^i$ for $t \in T$ and $0 \leqslant i \leqslant 2f$. As before, we may assume that $t = 1$ and either $i = 0$ or i divides $2f$. If $i = 2l$, then $g = \rho^{2l} = \varphi^l$, and if i is odd, then $g = \rho^i$. Therefore, g is an automorphism featuring in the statement. This completes the proof. □

4.1.5 Element variants

For each automorphism θ in Table 4.1, to apply the probabilistic method described in Section 2.1, we need to select an element $t\theta \in T\theta$. Recall that in Definitions 2.3.26 and 2.3.28, we defined standard *types* of elements denoted $(2d)^{\pm}_q$ for some $d \geqslant 1$. Moreover, in Definitions 2.3.32 and 2.3.34, for odd q we also defined variants indicated by superscripts Δ and Σ. These variants have a very similar action on the natural module but crucially are contained in a different coset of the simple group. By working with the latter, we will be able to select an element that lies in the precise coset $T\theta$.

To this end, for each automorphism θ appearing in Table 4.1 we define three symbols, which we will use in Chapter 5 also. The first two are

$$a = a(\theta) = \begin{cases} & \text{if } \theta \text{ is in Row (1) or (3)} \\ \Delta & \text{if } \theta \text{ is in Row (2)} \end{cases} \tag{4.9}$$

$$b = b(\theta) = \begin{cases} & \text{if } \theta \text{ is in Row (1)} \\ \Delta & \text{if } \theta \text{ is in Row (2)} \\ \Sigma & \text{if } \theta \text{ is in Row (3)} \end{cases} \tag{4.10}$$

where we mean the empty symbol in both of the first cases.

In Case II we will have an ambient field size q_0, and the dependence on whether q_0 is Mersenne in Lemma 2.3.30 will have to be propagated throughout this thesis. We have decided to handle this issue by defining a variant c on b which depends on both the automorphism θ and whether q_0 is Mersenne. It is convenient to define c slightly differently for symplectic groups, so we allow a dependence on T also. The definition is

$$c = c(\theta, q_0, T) = \begin{cases} \Delta & \text{if } \theta \text{ is in Row (2)} \\ \Sigma & \text{if } \theta \text{ is in Row (3) and } q_0 \text{ is not Mersenne} \\ \Sigma & \text{if } \theta \text{ is in Row (1), } q_0 \text{ is Mersenne and } T \neq \mathrm{PSp}_{2m}(q) \\ & \text{otherwise} \end{cases} \tag{4.11}$$

Remark 4.1.6. Let us comment on the symbols we have defined.

(i) Notice that $a = b = c$ is empty when q is even. If $T = \mathrm{PSp}_{2m}(q)$, then $a = b = c$. Moreover, in this case, $a = b = c = \Delta$ if and only if $\theta = \delta\varphi^i$.

(ii) As advised in Section 2.3, when one sees an expression of the form ${}^*(2m)^{\pm}$ one should focus on the general description of how $(2m)^{\pm}$ acts on the natural $2m$-dimensional space and keep in the back of one's mind that the $*$ modifies the element in order to place it in the appropriate coset.

4.2 Case I

In this section we study the uniform spread of almost simple groups $T \leqslant G \leqslant \mathrm{Inndiag}(T)$ for each $T \in \mathcal{T}$. In [10], Breuer, Guralnick and Kantor proved that $s(T) \geqslant 2$. As they point out [10, p.447], their proofs, in fact, prove that $s(G) \geqslant 2$. The following result is motivated by this comment (see [18, Theorem 3.1] for a similar argument).

Proposition 4.2.1. *Let $G = \langle T, \theta \rangle \in \mathcal{A}$, where $T \in \mathcal{T}$ and $\theta \in \mathrm{Inndiag}(T)$.*

(i) *In all cases, $u(G) \geqslant 2$*

(ii) *If $T = \Omega_{2m+1}(q)$, then $u(G) \geqslant 3$.*

(iii) *If $T = \mathrm{PSp}_{2m}(q)$ for $m \geqslant 3$ and odd q, then $u(G) \geqslant 4$.*

(iv) *In all cases, $u(G) \to \infty$ as $q \to \infty$.*

Proof. If $G = T$, then the result holds by [10], except the claim that $u(\mathrm{PSp}_{2m}(q)) \geqslant 4$ when q is odd and $m \geqslant 3$, which we return to later. Therefore, assume that q is odd and $G = \mathrm{Inndiag}(T)$. By computation in MAGMA (see Section 2.8) $u(G) \geqslant k$ when

$$(G, k) \in \{(\mathrm{PGSp}_4(3),\ 2),\ (\mathrm{PSp}_6(3),\ 4),\ (\mathrm{PGSp}_6(3),\ 4),\ (\mathrm{SO}_7(3),\ 3)\}.$$

First assume that $T = \Omega_{2m+1}(q)$ with $q > 3$. Write $V = \mathbb{F}_q^{2m+1}$. Let $g = g_1 \perp g_2 \in G$, centralising the decomposition $V = V_1 \perp V_1^{\perp}$, where g_1 acts trivially on the 1-space V_1 and g_2 has order $q^m + 1$ and acts irreducibly on $V_1^{\perp}$. By [22, Theorem 4], $q^m + 1$ does not divide the order of a maximal torus of T, so $g \in G \setminus T$. The order of g is divisible by a primitive prime divisor r of $q^{2m} - 1$ with $r > 4m + 1$ (see Lemma 2.3.15). Therefore, by Theorem 2.5.5, we deduce that $\mathcal{M}(G, g)$ consists entirely of reducible subgroups, noting that no subfield subgroups of G contain an element of order $q^m + 1$. By Lemma 2.3.3, the only proper nonzero subspaces of V stabilised by g are V_1 and $V_1^{\perp}$. Therefore, $\mathcal{M}(G, g) = \{H\}$ where H has type $\mathrm{O}_{2m}^{-}(q)$. Consequently, by Theorem 3.1.1, for all $x \in G$ of prime order,

$$P(x, g) \leqslant \mathrm{fpr}(x, G/H) < \frac{1}{q} + \frac{3}{q^{m-1}} + \frac{1}{q^m} < \frac{1}{3}.$$

Now Lemma 2.1.1 implies that $u(G) \geqslant 3$ as claimed. Moreover, as $q \to \infty$ we have $P(x, g) \to 0$ and thus $u(G) \to \infty$. (In [10], the authors use the element $s = g^2$ to prove that $u(T) \geqslant 3$ in exactly the same manner.)

Now assume that $T = \mathrm{PSp}_{2m}(q)$. Write $\widehat{T}$ and $\widehat{G}$ for $\mathrm{Sp}_{2m}(q)$ and $\mathrm{GSp}_{2m}(q)$. For an element $x \in \widehat{G}$ write $\overline{x}$ for its image in G. In the proofs of [10, Propositions 5.10–5.20] the authors identify a semisimple element $s = s_1 \perp \cdots \perp s_k \in \widehat{T}$, centralising the decomposition $V = V_1 \perp \cdots \perp V_k$, where each s_i lifts to an element of order $q^{m_i} + 1$ that acts irreducibly on the $2m_i$-space V_i. For this element s, it is shown that $P(x, \overline{s}) < \frac{1}{2}$ for all prime order elements $x \in T$. By Lemma 2.3.20, there exists an element $g \in \widehat{G}$ such

that $\tau(g) = \alpha$, so $g \in \widehat{G} \setminus \widehat{T}$, and $g^{q-1} = s$. By exactly the same argument as in [10], we can determine $\mathcal{M}(\widehat{G}, g)$, whose members have the same types as those in $\mathcal{M}(\widehat{T}, s)$. The bounds in Theorem 3.1.1 and Proposition 3.2.3 imply that $P(x, g) < \frac{1}{4}$ for all prime order $x \in G$. (In this manner we also see that $P(x, s) < \frac{1}{4}$ for all prime order $x \in T$, which proves the stronger claim for simple groups in the statement.)

For example, if $m \geqslant 5$ is odd, then $k = 2$, $\dim V_1 = 2$ and $\dim V_2 = 2m - 2$. Therefore, the order of g is divisible by a primitive prime divisor of $q^{2m-2} - 1$, which by Lemma 2.3.15 we can assume is strictly greater than $4m - 3$. By Theorem 2.5.5, we deduce that $\mathcal{M}(\widehat{G}, g) = \{\widehat{H}\}$ where $\widehat{H}$ has type $\mathrm{Sp}_2(q) \times \mathrm{Sp}_{2m-2}(q)$ and Theorem 3.1.1 implies that $P(x, s) < \frac{1}{4}$.

It remains to assume that $T = \Omega_{2m+1}(3)$ with $m \geqslant 4$. For now assume that m is odd and let $g = g_1 \perp g_2$ centralise $V = V_1 \perp V_1^{\perp}$ where $g_1 = [J_3]$ on the 3-space V_1 and g_2 has order $q^{m-1} + 1$ and acts irreducibly on $V_1^{\perp}$. Note that $g \in G \setminus T$. By the argument in [10, Proposition 5.19], we deduce that $\mathcal{M}(G, g) = \{H, K\}$, where H has type P_1 and K has type $\mathrm{O}_3(q) \times \mathrm{O}^-_{2m-2}(q)$, and that $P(x, g) < \frac{1}{3}$ for all prime order $x \in G$.

Finally assume that $T = \Omega_{2m+1}(3)$ for even m. Let $g = g_1 \perp g_2 \in G$ centralise the decomposition $V = V_1 \perp V_1^{\perp}$, where g_1 acts trivially on the 1-space V_1 and g_2 has order $q^m + 1$ and acts irreducibly on $V_1^{\perp}$. We saw earlier that $g \in G \setminus T$ and $\mathcal{M}(G, g) = \{H\}$ where H has type $\mathrm{O}^-_{2m}(q)$. In [10, Proposition 5.7] it is shown that $P(x, s) \leqslant \frac{1}{3}$, for all $x \in T$, with equality if and only if x is a reflection. In fact, this argument also proves that $P(x, g) \leqslant \frac{1}{3}$, for all $x \in G$, with equality if and only if x is a reflection. By the proof of [10, Proposition 5.7], for all reflections $x_1, x_2, x_3 \in G$, there exists a G-conjugate h of g for which $\langle x_1, h\rangle = \langle x_2, h\rangle = \langle x_3, h\rangle = G$. Therefore, $u(G) \geqslant 3$. □

With a view towards Theorem 4B we prove the following asymptotic result.

Proposition 4.2.2. *Let (G_i) be a sequence in $\mathcal{A}$ where $\mathrm{PSp}_{2m_i}(q_i) \leqslant G_i \leqslant \mathrm{PGSp}_{2m_i}(q_i)$ and each q_i is odd. Then $u(G_i) \to \infty$ if $m_i \to \infty$.*

Proof. By [37, Theorem 1.1], the result is true if each $G_i = \mathrm{PSp}_{2m_i}(q_i)$. Therefore, it suffices to prove the claim when each $G_i = \mathrm{PGSp}_{2m_i}(q_i)$. Fix $G = G_i = \mathrm{PGSp}_{2m}(q)$. Assume that $m \geqslant 40$ and fix $m/2 < d < 3m/4$ such that $(d, m - d) = 1$ and $m - d$ is odd. Let $y \in G$ have type ${}^{\Delta}(2d)^- \perp {}^{\Delta}(2m - 2d)^-$. Since $d > m/2$, a power z of y has type $(2d)^- \perp I_{2m-2d}$ and the order of z is a primitive prime divisor r of $q^{2d} - 1$, where $2d > m$. By Lemma 2.3.15, since $2d > 20$, we may assume that $r > 4d + 1$.

By applying Theorem 2.5.5, we conclude that $\mathcal{M}(G, y)$ contains only reducible subgroups, and Lemma 2.3.3 implies that $\mathcal{M}(G, y) = \{H\}$, where H has type $\mathrm{Sp}_{2d}(q) \times \mathrm{Sp}_{2m-2d}(q)$. Finally, we apply Lemma 2.1.1. Theorem 3.1.1 implies that for all prime order $x \in G$,

$$P(x, y) \leqslant \frac{3}{q^{m-1}} + \frac{2}{q^{m/2}} \to 0$$

as $m \to \infty$. Therefore, $u(G) \to \infty$ as $m \to \infty$. □

4.3 Case II

In this section, we prove Theorems 4A–4D in Case II. To this end, let $T \in \mathcal{T}$ and write $G = \langle T, \theta \rangle$ where $\theta \in \mathrm{Aut}(T) \setminus \mathrm{Inndiag}(T)$. From Section 4.3.2 onwards, we will assume further that $m \geqslant 3$; however, it is convenient to allow $T = \mathrm{PSp}_4(q)$ initially, so that we may use some of the preliminary results from this section in Section 4.4.

4.3.1 Element selection

Shintani descent (see Section 2.7) will play an indispensable role in identifying appropriate elements $t\theta \in T\theta$ for each automorphism θ (see Example 2.7.2). With this in mind let us fix the following notation for Section 4.3.

Notation 4.3.1. Write $q = p^f$ where $f \geqslant 2$ and fix a proper divisor i of f.

Let $V = \mathbb{F}_q^n$ be the natural module for T (so n is $2m$ or $2m+1$).

Fix the simple algebraic group

$$X = \begin{cases} \mathrm{PSp}_{2m}(\overline{\mathbb{F}}_p) & \text{if } T = \mathrm{PSp}_{2m}(q) \\ \mathrm{SO}_{2m+1}(\overline{\mathbb{F}}_p) & \text{if } T = \Omega_{2m+1}(q). \end{cases}$$

Fix the standard Frobenius endomorphism φ of X, defined with respect to the standard basis $\mathcal{B}$, as $(a_{ij}) \mapsto (a_{ij}^p)$, modulo scalars.

Write $\sigma = \varphi^i$ and $q_0 = p^i$. Therefore, $q = q_0^e$ for $e = f/i$.

Fix the Shintani map F of (X, σ, e), so $\widetilde{\sigma} = \sigma|_{X_{\sigma^e}}$ and

$$F\colon \{(g\widetilde{\sigma})^{X_{\sigma^e}} \mid g \in X_{\sigma^e}\} \to \{x^{X_\sigma} \mid x \in X_\sigma\}.$$

Observe that $X_{\sigma^e} = \mathrm{Inndiag}(T)$ and $X_\sigma = \mathrm{Inndiag}(T_0)$ where

$$T_0 = \begin{cases} \mathrm{PSp}_{2m}(q_0) & \text{if } T = \mathrm{PSp}_{2m}(q) \\ \Omega_{2m+1}(q_0) & \text{if } T = \Omega_{2m+1}(q). \end{cases}$$

The main idea is to select the element $t\theta \in \mathrm{Inndiag}(T)\sigma$ as the preimage under F of a carefully chosen element $y \in \mathrm{Inndiag}(T_0)$. If q is even, then $\mathrm{Inndiag}(T) = T$ and this is a transparent process. When q is odd, $T < \mathrm{Inndiag}(T)$ has index two and the following two results facilitate this selection procedure.

Lemma 4.3.2. *Let q be odd and $T = \mathrm{PSp}_{2m}(q)$. The Shintani map F restricts to bijections*

(i) $F_1\colon \{(g\widetilde{\sigma})^{\mathrm{PGSp}_{2m}(q)} \mid g \in T\} \to \{x^{\mathrm{PGSp}_{2m}(q_0)} \mid x \in T_0\}$

(ii) $F_2\colon \{(g\delta\widetilde{\sigma})^{\mathrm{PGSp}_{2m}(q)} \mid g \in T\} \to \{x^{\mathrm{PGSp}_{2m}(q_0)} \mid x \in \mathrm{PGSp}_{2m}(q_0) \setminus T_0\}$.

Proof. This is Lemma 2.7.4 applied to the natural isogeny $\pi\colon \mathrm{Sp}_{2m}(\overline{\mathbb{F}}_p) \to \mathrm{PSp}_{2m}(\overline{\mathbb{F}}_p)$, noting that $\langle \mathrm{PSp}_{2m}(q), \widetilde{\sigma}\rangle$ and $\mathrm{PSp}_{2m}(q_0)$ are index two subgroups of $\langle \mathrm{PGSp}_{2m}(q), \widetilde{\sigma}\rangle$ and $\mathrm{PGSp}_{2m}(q_0)$, respectively. (We proved this in Example 2.7.5.) □

Lemma 4.3.3. *Let q be odd and $T = \Omega_{2m+1}(q)$. The Shintani map F restricts to bijections*

(i) $F_1\colon \{(g\widetilde{\sigma})^{\mathrm{SO}_{2m+1}(q)} \mid g \in T\} \to \{x^{\mathrm{SO}_{2m+1}(q_0)} \mid x \in T_0\}$

(ii) $F_2\colon \{(gr_{\square}r_{\boxtimes}\widetilde{\sigma})^{\mathrm{SO}_{2m+1}(q)} \mid g \in T\} \to \{x^{\mathrm{SO}_{2m+1}(q_0)} \mid x \in \mathrm{SO}_{2m+1}(q_0) \setminus T_0\}$.

Proof. This is Lemma 2.7.4 with the natural isogeny $\pi\colon \mathrm{Spin}_{2m+1}(\overline{\mathbb{F}}_p) \to \mathrm{SO}_{2m+1}(\overline{\mathbb{F}}_p)$, noting that $\langle \Omega_{2m+1}(q), \widetilde{\sigma}\rangle$ and $\Omega_{2m+1}(q_0)$ are index two subgroups of $\langle \mathrm{SO}_{2m+1}(q), \widetilde{\sigma}\rangle$ and $\mathrm{SO}_{2m+1}(q_0)$, respectively. □

Remark 4.3.4. There is a more concrete means of seeing Lemma 4.3.2, which does not apply to Lemma 4.3.3. As before, we note that $\langle \mathrm{PSp}_{2m}(q), \widetilde{\sigma}\rangle \trianglelefteqslant \langle \mathrm{PGSp}_{2m}(q), \widetilde{\sigma}\rangle$ and $\mathrm{PSp}_{2m}(q_0) \trianglelefteqslant \mathrm{PGSp}_{2m}(q_0)$. Now let $g \in \mathrm{PGSp}_n(q)$ and let $F(g\widetilde{\sigma}) = x$, where we have $x = a^{-1}(g\widetilde{\sigma})^e a$ for $a \in \mathrm{PSp}_n(\overline{\mathbb{F}}_p)$ such that $g = aa^{-\sigma^{-1}}$. Let $Z = \langle -I_n\rangle$ and write $a = \hat{a}Z$, $\hat{g} = \hat{a}\hat{a}^{-\sigma^{-1}}$ and $\hat{y} = \hat{a}^{-1}(\hat{g}\widetilde{\sigma})^e\hat{a}$. Then

$$\tau(\hat{y}) = \tau(\hat{a}^{-1}(\hat{g}\widetilde{\sigma})^e\hat{a}) = \tau((\hat{g}\widetilde{\sigma})^e) = \tau(\hat{g})\tau(\hat{g}^{\sigma^{e-1}})\cdots\tau(\hat{g}^{\sigma}) = \tau(\hat{g})^{1+\sigma+\cdots+\sigma^{e-1}}.$$

In particular, $\tau(\hat{g})$ is a square in $\mathbb{F}_q^\times$ if and only if $\tau(\hat{y})$ is a square in $\mathbb{F}_{q_0}^\times$. Consequently, Lemma 2.2.6 implies that $g \in \mathrm{PSp}_n(q)$ if and only if $F(g\widetilde{\sigma}) \in \mathrm{PSp}_n(q_0)$.

We are now in a position to define the elements we will use to prove Theorems 4A and 4C. In light of the probabilistic method outlined in Section 2.1, we need to select $t\theta \in G$ in a way which allows us to control both the maximal subgroups of G which contain it and the fixed point ratios associated with these subgroups.

Therefore, we will choose $t\theta$ such that it has the following two features, which place significant restrictions on its maximal overgroups. First, $t\theta$ should not be contained in many reducible subgroups, since subspace subgroups have comparatively large fixed point ratios. Second, a power of $t\theta$ should have a 1-eigenspace of large dimension in its action on the natural module for G, noting that eigenvalue patterns place tight restrictions on possible maximal overgroups (see Section 2.5.2). These two conditions inform our choice of the element $y \in X_\sigma$, which via Shintani descent yields an element $t\theta \in G$.

Proposition 4.3.5. *Let $T \in \mathcal{T}$ with $m \geqslant 3$ and let θ be an automorphism in Table 4.1 (in Case II). For the element $y \in \mathrm{Inndiag}(T_0)$ in Table 4.2 there exists $t \in T$ such that $(t\theta)^e$ is X-conjugate to y.*

Remark 4.3.6. Let us comment on the definition of y in Table 4.2. The parameters a and c are defined in (4.9) and (4.11). The final bracketed summand should be excluded when $T = \mathrm{PSp}_{2m}(q)$ and included when $T = \Omega_{2m+1}(q)$. The dependence on m implies that elements of this type actually exist (see Lemmas 2.3.27 and 2.3.29); for example, $(6)_2^-$ never appears in the definition of an element y.

Table 4.2: Case II: The element y for the automorphism θ

m	y
odd	${}^a(2)^- \perp {}^c(2m-2)^- (\perp I_1)$
even	${}^a(2)^- \perp {}^c(2m-2)^+ (\perp I_1)$

[we describe y by specifying the type of a lift of y, which is defined over $\mathbb{F}_{q_0}$]

Proof of Proposition 4.3.5. From Definitions 2.3.26, 2.3.28 and 2.3.32, we see that y truly is an element of $\mathrm{Inndiag}(T_0)$. Therefore, by Theorem 2.7.1, there exists $g \in \mathrm{Inndiag}(T)$ such that $(g\widetilde{\sigma})^e$ is X-conjugate to y. If q is even, then $T = \mathrm{Inndiag}(T)$ and $\theta = \varphi^i = \widetilde{\sigma}$, so $g\widetilde{\sigma} \in T\theta$, as required.

Next assume that q is odd and $T = \mathrm{PSp}_{2m}(q)$. If $\theta = \varphi^i$, then $a = c$ is empty and $y \in \mathrm{PSp}_{2m}(q_0)$, so Lemma 4.3.2 implies that $g\widetilde{\sigma} \in T\widetilde{\sigma} = T\theta$, as required. If $\theta = \delta\varphi^i$, then $a = c = \Delta$, which implies that $\tau(y) = \beta \notin (\mathbb{F}_q^\times)^2$ and $y \notin \mathrm{PSp}_{2m}(q_0)$, so Lemma 4.3.2 gives $g\widetilde{\sigma} \in T\delta\widetilde{\sigma} = T\theta$.

Now assume that $T = \Omega_{2m+1}(q)$. For now assume that q_0 is not Mersenne. Therefore, by Lemma 2.3.30, an element of type $(2)^-_{q_0}$ is contained in $\Omega_2^-(q_0)$. If $\theta = \varphi^i$, then noting the precise definition of $c = c(\theta, q_0, T)$ in (4.11), we note that $a = c$ is empty, so $y \in \Omega_{2m+1}(q_0)$ and, by Lemma 4.3.3, $g\widetilde{\sigma} \in T\theta$. If $\theta = r_\square r_\boxtimes \varphi^i$, then a is empty but $c = \Sigma$, so $y \in \Omega_{2m+1}(q_0) r_\square r_\boxtimes$ and, by Lemma 4.3.3, $g\widetilde{\sigma} \in T\theta$.

Finally assume that $T = \Omega_{2m+1}(q)$ and q_0 is Mersenne. In this case an element of type $(2)^-_{q_0}$ is contained in $\mathrm{SO}_2^-(q_0) \setminus \Omega_2^-(q_0)$. However, $c = \Sigma$ if and only if $\theta = \varphi^i$ in this case. Consequently, by the argument in the previous paragraph $g\widetilde{\sigma} \in T\theta$ in this case too, and we have completed the proof. □

4.3.2 Maximal subgroups

Continue to let $T \in \mathcal{T}$ with $m \geqslant 3$ and let θ be an automorphism from Table 4.1. Fix $y \in \mathrm{Inndiag}(T_0)$ from Table 4.2 and $t\theta \in G = \langle T, \theta \rangle$ from Proposition 4.3.5. We will now study the set $\mathcal{M}(G, t\theta)$ of maximal overgroups of $t\theta$ in G.

Theorem 4.3.7. *The maximal subgroups of G that contain $t\theta$ are listed in Table 4.3, where $m(H)$ is an upper bound on the multiplicity of the subgroups of type H in $\mathcal{M}(G, t\theta)$.*

In Table 4.3 (and also Tables 4.4, 5.2, 5.5, 5.7 and 5.8) the *conditions* column provides *necessary* conditions for a subgroup of the relevant type to be contained in $\mathcal{M}(G, t\theta)$.

Let us outline the proof of Theorem 4.3.7. If $T \leqslant H$, then we deduce that $\theta \in H$, since $t\theta \in H$, but then we would have $H = G$, which is not the case. Therefore, $T \not\leqslant H$, so Theorem 2.5.1 implies that H is contained in one of the geometric families $\mathcal{C}_1, \ldots, \mathcal{C}_8$ or is an almost simple irreducible group in $\mathcal{S}$.

Table 4.3: Case II: Description of $\mathcal{M}(G, t\theta)$

T		type of H	$m(H)$	conditions
$\mathrm{PSp}_{2m}(q)$	$\mathcal{C}_1$	$\mathrm{Sp}_2(q) \times \mathrm{Sp}_{2m-2}(q)$	1	
		P_{m-1}	2	m even
	$\mathcal{C}_2$	$\mathrm{Sp}_2(q) \wr S_m$	1	$(m-1) \mid e$
		$\mathrm{GL}_m(q)$	$2^{(m-1,e)}$	q odd, $e_2 \geqslant (2m-2)_2$ if m odd
		$\mathrm{Sp}_m(q) \wr S_2$	$\frac{1}{2}\binom{m}{\frac{m}{2}}$	m even, $(m-1) \mid e$
	$\mathcal{C}_5$	$\mathrm{Sp}_{2m}(q^{1/k})$	e^2	$k = e$ is prime
			$\lvert C_{X_\sigma}(y)\rvert$	k is prime, $k \mid f$, $k \neq e$
	$\mathcal{C}_8$	$\mathrm{O}^{\varepsilon}_{2m}(q)$	1	q even
$\Omega_{2m+1}(q)$	$\mathcal{C}_1$	$\mathrm{O}^{\varepsilon_1}_{2m}(q)$	1	for a *unique* sign $\varepsilon_1 \in \{+,-\}$
		$\mathrm{O}^{\varepsilon_2}_2(q) \times \mathrm{O}_{2m-1}(q)$	1	for a *unique* sign $\varepsilon_2 \in \{+,-\}$
		$\mathrm{O}_3(q) \times \mathrm{O}^{\varepsilon_3}_{2m-2}(q)$	1	for a *unique* sign $\varepsilon_3 \in \{+,-\}$
		P_{m-1}	2	m even
	$\mathcal{C}_5$	$\mathrm{O}_{2m+1}(q^{1/k})$	e^3	$k = e$ is prime
			$\lvert C_{X_\sigma}(y)\rvert$	k is prime, $k \mid f$, $k \neq e$

Our general idea is to consider each of these families in turn and determine which possible types of subgroup could contain the element $t\theta$, by exploiting the restrictive properties that we have chosen $t\theta$ to have. For types of subgroups which could contain the element $t\theta$ we will find an upper bound on the number of subgroups of this type that contain $t\theta$. We will not concern ourselves with determining *exactly* which subgroups contain $t\theta$; sometimes it will be sufficient, for example, to use an overestimate on the number of subgroups of a given type which contain $t\theta$.

In the following four sections, we will prove Theorem 4.3.7 for reducible subgroups ($\mathcal{C}_1$), imprimitive subgroups ($\mathcal{C}_2$), classical subgroups ($\mathcal{C}_8$) and the remaining primitive subgroups ($\mathcal{C}_3$–$\mathcal{C}_7$ and $\mathcal{S}$). However, we begin by presenting a result on the multiplicities of subgroups in $\mathcal{M}(G, t\theta)$.

Write

$$\widetilde{G} = \langle X_{\sigma^e}, \widetilde{\sigma} \rangle \tag{4.12}$$

noting that $\mathrm{Inndiag}(T) \leqslant \widetilde{G} \leqslant \mathrm{Aut}(T)$ and $G \leqslant \widetilde{G}$.

Proposition 4.3.8. *Let $T \leqslant A \leqslant \mathrm{Aut}(T)$ and let H be a maximal geometric subgroup of A. Then there is a unique $\widetilde{G}$-conjugacy class of subgroups of A of type H.*

Proof. Note that q is not prime since $f \geqslant 2$. If $n \leqslant 12$, then the result follows from the tables in [7, Chapter 8]. Now assume that $n \geqslant 13$. We will apply the Main Theorem of [43] as described in Section 2.5.1 (see Example 2.5.3 in particular).

Let H be a maximal geometric subgroup of G. Let $\mathcal{H} = \{H_1, \dots, H_c\}$ be a set of representatives of the c distinct T-classes of subgroups of T of the same type as H, and let $H_{G,i}$ be the G-associate of H_i. Recall the homomorphism $\pi\colon \mathrm{Out}(T) \to S_c$ associated to the action of $\mathrm{Out}(T)$ on $\mathcal{H}$.

By [43, Tables 3.5C and 3.5D], $c = 1$ and the G-classes of subgroups are precisely the $\mathrm{Aut}(T)$-classes, unless q is odd and H is a subfield subgroup over $\mathbb{F}_{q^{1/2}}$. In this case, $c = 2$, so the $\mathrm{Aut}(T)$-class splits into two T-classes. By [43, Table 3.5G], $\ddot{\delta}$ and $\ddot{r}_{\square}\ddot{r}_{\boxtimes}$ are not contained in the kernel of π when T is $\mathrm{PSp}_{2m}(q)$ and $\Omega_{2m+1}(q)$, respectively. Therefore, the subfield subgroups over $\mathbb{F}_{q^{1/2}}$ are $\widetilde{G}$-conjugate, as required. □

Reducible subgroups

We now prove Theorem 4.3.7 in several parts, beginning with reducible subgroups.

Proposition 4.3.9. *Theorem 4.3.7 is true for reducible subgroups.*

Proof. We will apply Lemma 2.7.9 (see Example 2.7.10).

Case 1: stabilisers of totally singular subspaces

Let H be a maximal parabolic subgroup of G. Then $H \leqslant \widetilde{H} = \langle Y_{\sigma^e}, \widetilde{\sigma}\rangle$ for a $\widetilde{\sigma}$-stable parabolic subgroup $Y \leqslant X$. In particular, Y is a closed connected subgroup of X. Moreover, $\widetilde{H}$ and Y_σ are maximal (and hence self-normalising) subgroups of $\widetilde{G}$ and X_σ, respectively. Therefore, Lemma 2.7.9 implies that the number of X_{σ^e}-conjugates of H which contain $t\theta$ equals the number of X_σ-conjugates of $H \cap X_\sigma$ which contain $F(t\theta) = y$.

We use Lemma 2.3.3. If m is odd, then y does not stabilise any totally singular subspace of $\mathbb{F}_{q_0}^n$, so y is not contained in any parabolic subgroup of X_σ and consequently $t\theta$ is not contained in any parabolic subgroups of X_{σ^e}. However, if m is even, then y stabilises exactly two totally singular subspaces, of dimension $m-1$, so $t\theta$ is contained in exactly two parabolic subgroups of G, each of type P_{m-1}. This is what we claim in Theorem 4.3.7.

Case 2: stabilisers of nondegenerate subspaces

Now let H be the stabiliser in G of a nondegenerate k-space. If $T = \Omega_{2m+1}(q)$, then H arises from a disconnected subgroup of X, so we must alter our approach (when $T = \mathrm{PSp}_{2m}(q)$ these are connected subgroups, so we could have handled this case as above, but for uniformity we handle both $\mathrm{PSp}_{2m}(q)$ and $\Omega_{2m+1}(q)$ together).

Let $L = \mathrm{SL}_n(\overline{\mathbb{F}}_p)/\langle -I_n\rangle$ and extend the domain of σ to L. Let E be the Shintani map of (L, σ, e). Observe that $t\theta \in G \leqslant \langle L_{\sigma^e}, \theta\rangle$ and $F(t\theta) \in X_\sigma \leqslant L_\sigma$. Accordingly, Lemma 2.7.3 implies that $F(t\theta) = E(t\theta)$. Let $M \leqslant L$ be a P_k parabolic subgroup. Applying Lemma 2.7.9 to the Shintani map E for L and the subgroup $M \leqslant L$, we see that the number of k-spaces of $V = \mathbb{F}_q^n$ fixed by $t\theta$ equals the number of k-spaces of $V_0 = \mathbb{F}_{q_0}^n$ fixed by $E(t\theta) = F(t\theta) = y$.

First assume that $T = \Omega_{2m+1}(q)$. For now assume further that m is odd. Then, by Lemma 2.3.3, y stabilises exactly six proper nonzero subspaces of V_0, of dimensions 1, 2, 3, $2m-2$, $2m-1$ and $2m$. Therefore, $t\theta$ stabilises exactly six subspaces of V of the same dimensions. In Case 1, we demonstrated that $t\theta$ is not contained in a parabolic subgroup of G. Therefore, each of these six subspaces of V must be nondegenerate, for otherwise $t\theta$ would stabilise its (totally singular) radical and therefore be contained in a parabolic subgroup. Consequently, $t\theta$ is contained in exactly three $\mathcal{C}_1$ subgroups of G, of types $\mathrm{O}^{\varepsilon_1}_{2m}(q)$, $\mathrm{O}^{\varepsilon_2}_2(q) \times \mathrm{O}_{2m-1}(q)$ and $\mathrm{O}_3(q) \times \mathrm{O}^{\varepsilon_3}_{2m-2}(q)$ for particular signs $\varepsilon_1, \varepsilon_2$ and ε_3. (It is exactly for the reason that we pass to the linear group L that we cannot determine the signs.)

Continue to assume that $T = \Omega_{2m+1}(q)$ and now let m be even. By arguing as above, we see that $t\theta$ stabilises exactly 14 proper nonzero subspaces of V, of dimensions

$$\begin{gathered} 1, \quad 2, \quad 3, \quad 2m-2, \quad 2m-1, \quad 2m \\ m-1 \ (2), \quad m \ (2), \quad m+1 \ (2), \quad m+2 \ (2), \end{gathered}$$

where the (2) in the second row denotes the fact that there are two subspaces of each of these dimensions. From Case 1, we know that $t\theta$ stabilises exactly two totally singular subspaces, each of dimension $m-1$. Since $t\theta$ stabilises a (necessarily not totally singular) 1-, 2- and 3-space, we deduce that the stabilised m-, $(m+1)$- and $(m+2)$-spaces must be the direct sum of the 1-, 2- and 3-spaces with the two $(m-1)$-spaces. These subspaces are neither totally singular (there are only two such subspaces stabilised by $t\theta$) nor nondegenerate (they have an $(m-1)$-dimensional totally singular subspace). The subspaces that we have not yet accounted for are the ones of dimension 1, 2, 3, $2m-2$, $2m-1$, $2m$. These give the same three subgroups we identified when m is odd. This completes the proof for $T = \Omega_{2m+1}(q)$.

If $T = \mathrm{PSp}_{2m}(q)$, then we argue in the same manner but there are fewer subspaces to consider. If m is odd, then $t\theta$ stabilises a (necessarily nondegenerate) 2-space and $(2m-2)$-space, so the only maximal reducible subgroup of G containing $t\theta$ has type $\mathrm{Sp}_2(q) \times \mathrm{Sp}_{2m-2}(q)$. If m is even, $t\theta$, in addition, stabilises two $(m-1)$- and $(m+1)$-spaces. These must be the two totally singular subspaces from Case 1 together with their direct sums with the nondegenerate 2-space, so these subspaces do not give rise to any further maximal overgroups of $t\theta$. This completes the proof. □

Imprimitive subgroups

We now turn to irreducible imprimitive subgroups. Recall our terminology associated with decompositions introduced in Section 2.3.1. Our proof is inspired by an argument in the proof of [18, Lemma 4.5].

Proposition 4.3.10. *Theorem 4.3.7 is true for irreducible imprimitive subgroups.*

Proof. Let $H \leqslant G$ be a maximal imprimitive subgroup of G containing $t\theta$. Let $\mathcal{D}$ be the direct sum decomposition

$$\mathbb{F}_q^n = V = V_1 \oplus \cdots \oplus V_k \tag{4.13}$$

of which H is the stabiliser in G. Note that $k \geqslant 2$ divides n and $\dim V_i = \frac{n}{k}$ for all $i \in \{1, \ldots, k\}$. Since H is maximal we know that either each V_i is nondegenerate or $T = \mathrm{PSp}_{2m}(q)$, $k = 2$ and V_1 and V_2 are maximal totally singular subspaces. If $T = \mathrm{PSp}_{2m}(q)$, then this evidently implies that $\dim V_i \geqslant 2$. If $T = \Omega_{2m+1}$, then since q is not prime, the maximality of H implies that $\dim V_i \geqslant 2$ also (see [43, Table 3.5D]).

By construction, a suitable power x of $t\theta$ has type $(2m-2)^{\varepsilon}_{q_0} \perp I_{2+n-2m}$, where $\varepsilon = (-)^m$. Therefore, the order of x is a primitive prime divisor r of $q_0^\ell - 1$ where $\ell = (2m-2)/(m,2)$ and the nontrivial eigenvalues of x are distinct. Therefore, Lemma 2.5.6 guarantees that x centralises the decomposition $\mathcal{D}$.

Let $\{u_1, \ldots, u_n\}$ be a basis for V and let $\overline{V} = \langle u_1, \ldots, u_n \rangle_{\overline{\mathbb{F}}_p}$. Extend the semilinear action of G on V to an action on $\overline{V}$ by defining, for each $g \in G \cap \mathrm{GL}(V)$ and $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{F}}_p$,

$$(\alpha_1 u_1 + \cdots + \alpha_n u_n)g\widetilde{\sigma} = \alpha_1^{q_0}(u_1 g) + \cdots + \alpha_n^{q_0}(u_n g).$$

Then the decomposition in (4.13) gives rise to the corresponding decomposition $\overline{\mathcal{D}}$

$$\overline{V} = \overline{V}_1 \oplus \cdots \oplus \overline{V}_k. \tag{4.14}$$

We now claim that $y = F(t\theta)$ centralises $\mathcal{D}$. Suppose that x acts nontrivially on V_i and $1 \neq \mu \in \overline{\mathbb{F}}_p$ is an eigenvalue of x with μ-eigenvector $v \in \overline{V}_i$. Since x and y commute,

$$(vy)x = (vx)y = (\mu v)y = \mu(vy).$$

That is, vy is a μ-eigenvector of x. However, all nontrivial eigenvalues of x have multiplicity one, so $vy \in \overline{V}_i$. Since y stabilises the decomposition in (4.14), y stabilises $\overline{V}_i$. However, V is y-stable, so y stabilises $\overline{V}_i \cap V = V_i$. Since the 1-eigenspace of x is at most 3-dimensional and $\dim V_i \geqslant 2$, x acts nontrivially on at least $k-1$ summands. Therefore, y stabilises at least $k-1$ summands and, hence, all k summands.

Now we will find subspaces which are stabilised by $t\theta$. The element y has an eigenvalue λ of multiplicity one that is contained in $\mathbb{F}_{q_0^2}$ and in no proper subfield. Let $\overline{V}_i$ contain the λ-eigenspace of y and $\overline{V}_j$ contain the λ^{q_0}-eigenspace of y. Since y and $t\theta$ commute, if $v \in \overline{V}_i$ is a λ-eigenvector for y, then

$$(vt\theta)y = (vy)(t\theta) = (\lambda v)(t\theta) = \lambda^{q_0}(vt\theta),$$

so $vt\theta$ is a λ^{q_0}-eigenvector for y. However, λ^{q_0} has multiplicity one so $vt\theta \in \overline{V}_j$. Similarly, if $w \in \overline{V}_j$ is a λ^{q_0}-eigenvector, then $w\theta$ is a λ-eigenvector, so $wt\theta \in \overline{V}_i$. Thus, since y centralises $\overline{\mathcal{D}}$, $t\theta$ stabilises $\overline{V}_i + \overline{V}_j$, and, since V is $t\theta$-stable, $t\theta$ stabilises $V_i + V_j$.

For now assume that $T = \mathrm{PSp}_{2m}(q)$. If $i \neq j$, then $t\theta$ stabilises $V_i \oplus V_j$, so, by Proposition 4.3.9, $2\dim V_i = 4m/k \in \{2, 2m-2, 2m\}$. However, $m \geqslant 3$ and $2m/k$ divides $2m$, so

$k = 2$. Similarly, if $i = j$ then $t\theta$ stabilises V_i, so $\dim V_i = 2m/k \in \{2, m-1, m+1, 2m-2\}$. Since $2m/k$ divides $2m$, $\dim V_i = 2$. By a similar line of reasoning, if $T = \Omega_{2m+1}(q)$, then $\dim V_i = 3$. This implies that $y = M_1 \perp \cdots \perp M_k$ where $M_i \in \mathrm{SO}_3(q)$. Now M_i has eigenvalues $\lambda_i, \mu_i, 1$, which contradicts 1 being an eigenvalue of y with multiplicity 1.

To summarise, we have established that if $T = \Omega_{2m+1}(q)$, then no imprimitive irreducible subgroups arise, and if $T = \mathrm{PSp}_{2m}(q)$, then either $k = 2$ or $k = m$. Therefore, for the remainder of the proof we may assume that $T = \mathrm{PSp}_{2m}(q)$ and we will focus on establishing necessary conditions for these subgroups to arise and bounds on their multiplicities when they do.

Let H and B be the stabiliser and centraliser in G of the decomposition $\mathcal{D}$. Fix z as a power of y of type $(2m-2)^{\varepsilon}_{q_0} \perp (2)^{-}_{q_0}$ where $\varepsilon = (-)^m$. Note that $z \in B$.

Case 1: $k = m$

We may write $z = M_1 \perp \cdots \perp M_m$ where $M_i \in \mathrm{Sp}_2(q)$. By Lemma 2.3.36 this implies that $m-1$ divides e. Since the eigenvalues of y are distinct, by Corollary 2.3.5, $|C_G(y)| = |C_B(y)| = |C_H(y)|$. Moreover, $y^G \cap H$ splits into $m!$ B-classes (corresponding to the possible permutations of $M_1, \ldots, M_m$), which are fused in H, so $y^G \cap H = y^H$. Therefore, by Lemma 2.1.3, the number of G-conjugates of H that contain y is

$$\frac{|y^G \cap H|}{|y^G|}\frac{|G|}{|H|} = \frac{|y^H|}{|y^G|}\frac{|G|}{|H|} = \frac{|C_G(y)|}{|C_H(y)|} = 1.$$

Consequently, $t\theta$ is contained in at most one G-conjugate of H.

Case 2: $k = 2$ and V_1 and V_2 are nondegenerate

Here m is even. Write $z = M \perp N$ where $M, N \in \mathrm{Sp}_m(q)$. The set of eigenvalues of z is

$$\{\lambda_1, \lambda_1^{q_0}, \lambda_2, \lambda_2^{-1}, \ldots, \lambda_2^{q_0^{m-2}}, \lambda_2^{-q_0^{m-2}}\}.$$

By Lemma 2.2.7, the eigenvalues of M are closed under taking inverses. Since $\lambda_1^{q_0} = \lambda_1^{-1}$, we may assume that λ_1 and $\lambda_1^{q_0}$ are eigenvalues of M.

Let $d = (m-1, e)$ and $b = (m-1)/d$. By Lemma 2.3.36, the eigenvalue set of z is $\Lambda \cup \Lambda_1 \cup \cdots \cup \Lambda_d$, where $\Lambda = \{\lambda_1, \lambda_1^{q_0}\}$ and $\Lambda_i = \{\lambda_2^{q_0^i}, \lambda_2^{-q_0^i}, \ldots, (\lambda_2^{q_0^i})^{q^{b-1}}, (\lambda_2^{q_0^i})^{-q^{b-1}}\}$, for each i. Since the eigenvalue sets of M and N are closed under the map $\alpha \mapsto \alpha^q$, the eigenvalue set of M is $\Lambda \cup \Lambda_{a_1} \cup \cdots \cup \Lambda_{a_l}$ and the eigenvalue set of N is $\Lambda_{a_{l+1}} \cup \cdots \cup \Lambda_{a_d}$ where $l \geqslant 1$ and $\{a_1, \ldots, a_d\} = \{1, \ldots, d\}$. Therefore, b divides m and $m-2$. Thus, b divides 2, so $\Lambda_i = \{\lambda_2^{q_0^i}, \lambda_2^{-q_0^i}\}$, for each i. In particular, $d = m-1$, which proves that $m-1$ divides e when these subgroups arise.

By arguing as in Case 1, we can show that $|C_G(z)| = |C_H(z)|$ and that $z^G \cap H$ splits into $\binom{m}{\frac{m}{2}}$ B-classes (corresponding to the possible choices for $m/2$ of $\Lambda, \Lambda_1, \ldots, \Lambda_{m-1}$ for M) which fuse to $\frac{1}{2}\binom{m}{\frac{m}{2}}$ H-classes. Therefore, z, and thus $t\theta$, lies in at most $\frac{1}{2}\binom{m}{\frac{m}{2}}$ G-conjugates of H.

Case 3: $k = 2$ and V_1 and V_2 are totally singular

Assume that m is odd. Then a power z of y has type $(2m-2)^-_{q_0} \perp (2)^-_{q_0}$, and, since $z \in B$, $z = M \oplus M^{-\mathsf{T}}$ for $M \in \mathrm{GL}_m(q)$. Now the set of eigenvalues of z is

$$\{\lambda_1, \lambda_1^{q_0}, \lambda_2, \lambda_2^{q_0}, \ldots, \lambda_2^{q_0^{2m-2}}\}.$$

Since $\lambda_1^{q_0} = \lambda_1^{-1}$, assume that λ_1 is an eigenvalue of M and $\lambda_1^{q_0}$ is an eigenvalue of $M^{-\mathsf{T}}$.

Let $d = (2m-2, e)$ and $b = (2m-2)/d$. The eigenvalue set of z is $\Lambda \cup \Lambda_1 \cup \cdots \cup \Lambda_d$, where $\Lambda = \{\lambda_1, \lambda_1^{q_0}\}$ and where $\Lambda_1, \ldots, \Lambda_d$ are the orbits of the eigenvalue set of an element of type $(2m-2)^-$ under the map $\alpha \mapsto \alpha^q$. Since the eigenvalue set of M is closed under the map $\alpha \mapsto \alpha^q$, the eigenvalue set of M is $\{\lambda_1\} \cup \Lambda_{a_1} \cup \cdots \cup \Lambda_{a_l}$ where $l = \frac{d}{2}$ and where $a_1, \ldots, a_l \in \{1, \ldots, d\}$ are distinct. If b is even, then $\Lambda_i^{-1} = \Lambda_i$, for each i. However, this contradicts the distinctness of the eigenvalues of z. Therefore, b is odd. In particular, $e_2 \geqslant (2m-2)_2$.

As in Case 1, we can show that $|C_G(z)| = |C_H(z)|$. Additionally, if $N \in \mathrm{GL}_n(q)$ has eigenvalue set $\{\lambda_1^\varepsilon\} \cup \Lambda_1^{\varepsilon_1} \cup \cdots \cup \Lambda_l^{\varepsilon_l}$, then a G-conjugate of y is B-conjugate to $[N, N^{-\mathsf{T}}]$ for exactly one choice of $(\varepsilon, \varepsilon_1, \ldots, \varepsilon_l) \in \{+,-\}^{l+1}$. Therefore, z^G splits into 2^{l+1} B-classes, which fuse to 2^l H-classes. Consequently, z, and thus $t\theta$, lies in at most $2^l = 2^{(2m-2,e)/2} \leqslant 2^{(m-1,e)}$ G-conjugates of H.

When m is even, the analysis is very similar but we work with an element of type $(2)^-_{q_0} \perp (2m-2)^+_{q_0}$ instead; we omit the details.

We have now completed the proof. □

Orthogonal subgroups of symplectic groups

Before turning to primitive subgroups in general, let us first carefully consider the classical $\mathcal{C}_8$ subgroups. In our context, these are the subgroups of type $\mathrm{O}^\pm_{2m}(2^f)$ in almost simple groups with socle $\mathrm{Sp}_{2m}(2^f)$. These subgroups merit special attention because, on one hand, they are subspace subgroups and therefore have comparatively large fixed point ratios (see Section 3.1), but on the other hand, they are not stabilisers of subspaces of the natural module $\mathbb{F}_{2^f}^{2m}$ and therefore are not amenable to Shintani descent in a transparent way. The idea is to apply Shintani descent by exploiting the fact that there is a bijective isogeny $\mathrm{SO}_{2m+1}(\overline{\mathbb{F}}_2) \to \mathrm{Sp}_{2m}(\overline{\mathbb{F}}_2)$ (see Remark 2.6.2). This section is somewhat more technical than its environs.

For this section fix $p = 2$, so $T = \mathrm{Sp}_{2m}(q)$ and $\theta = \widetilde{\sigma} = \varphi^i$ (where $i = f/e$). We will allow $m = 2$ here, so that we can exploit the main result, Proposition 4.3.13, in Case III also.

We begin by introducing an auxiliary map E. Recall that X is the algebraic group $\mathrm{Sp}_{2m}(\overline{\mathbb{F}}_2)$. Define $Y = \mathrm{SO}_{2m+1}(\overline{\mathbb{F}}_2)$ and let $\pi^{-1}\colon Y \to X$ be the isogeny that is given explicitly in Lemma 2.6.2. Define $\tau\colon Y \to Y$ as $\tau = \pi \circ \sigma \circ \pi^{-1}$.

Lemma 4.3.11. *With the notation above, τ is a Steinberg endomorphism of Y.*

Proof. Let $h \in Y$. Then, by Lemma 2.6.2, we may write

$$h = \pi(g) = \begin{pmatrix} a_{11} & \cdots & a_{1(2m)} & (\sum_{i=1}^{m} a_{1(2i-1)}a_{1(2i)})^{\frac{1}{2}} \\ \vdots & \ddots & \vdots & \vdots \\ a_{(2m)1} & \cdots & a_{(2m)(2m)} & (\sum_{i=1}^{m} a_{(2m)(2i-1)}a_{(2m)(2i)})^{\frac{1}{2}} \\ 0 & \cdots & 0 & 1 \end{pmatrix} = (b_{ij})$$

where $g = (a_{ij}) \in X$. Since $g^\sigma = (a_{ij}^{q_0})$,

$$h^\tau = \pi(g^\sigma) = \begin{pmatrix} a_{11}^{q_0} & \cdots & a_{1(2m)}^{q_0} & (\sum_{i=1}^{m} a_{1(2i-1)}^{q_0}a_{1(2i)}^{q_0})^{\frac{1}{2}} \\ \vdots & \ddots & \vdots & \vdots \\ a_{(2m)1}^{q_0} & \cdots & a_{(2m)(2m)}^{q_0} & (\sum_{i=1}^{m} a_{(2m)(2i-1)}^{q_0}a_{(2m)(2i)}^{q_0})^{\frac{1}{2}} \\ 0 & \cdots & 0 & 1 \end{pmatrix} = (b_{ij}^{q_0}).$$

Therefore, $\tau\colon Y \to Y$ is nothing other than the map $(b_{ij}) \mapsto (b_{ij}^{q_0})$, which is evidently a Steinberg endomorphism. □

Recall the Shintani map

$$F\colon \{(g\widetilde{\sigma})^{X_{\sigma^e}} \mid g \in X_{\sigma^e}\} \to \{x^{X_\sigma} \mid x \in X_\sigma\}.$$

It is straightforward to verify that $\pi\colon X \to Y$ extends to an isomorphism (of abstract groups) $\pi\colon X{:}\langle\sigma\rangle \to Y{:}\langle\tau\rangle$ by defining $\pi(\sigma) = \tau$. Therefore, we may define a map

$$E\colon \{(h\widetilde{\tau})^{Y_{\tau^e}} \mid h \in Y_{\tau^e}\} \to \{y^{Y_\tau} \mid y \in Y_\tau\}.$$

as $E = \pi \circ F \circ \pi^{-1}$, where $\widetilde{\tau} = \tau|_{Y_{\tau^e}}$.

Lemma 4.3.12. *With the notation above, E is the Shintani map of (Y, τ, e).*

Proof. Let $h \in Y_{\tau^e}$ and let $g \in X_{\sigma^e}$ such that $\pi(g) = h$. By Corollary 2.6.6 (a consequence of the Lang–Steinberg Theorem), we may fix $a \in X$ such that $aa^{-\sigma^{-1}} = g$. Then

$$E(h\widetilde{\tau}) = \pi(F(\pi^{-1}(h\widetilde{\tau}))) = \pi(F(g\widetilde{\sigma})) = \pi(a^{-1}(g\widetilde{\sigma})^e a) = \pi(a)^{-1}(h\widetilde{\tau})^e\pi(a),$$

where

$$\pi(a)\pi(a)^{-\tau^{-1}} = \pi(a)\pi(a)^{-\pi(\sigma)^{-1}} = \pi(aa^{-\sigma^{-1}}) = \pi(g) = h.$$

This proves the claim. □

We now use the map E to determine the multiplicities of orthogonal subgroups of G (when $T = \mathrm{Sp}_{2m}(2^f)$). The author thanks Robert Guralnick for helpful comments on the proof of the following proposition.

Proposition 4.3.13. *Let q be even, $m \geqslant 2$, $T = \mathrm{Sp}_{2m}(q)$, $\widetilde{\sigma} = \varphi^i$ and $G = \langle T, \widetilde{\sigma} \rangle$. For $g \in T$, the total number of maximal subgroups of G of type $\mathrm{O}^+_{2m}(q)$ or $\mathrm{O}^-_{2m}(q)$ that contain $g\widetilde{\sigma}$ equals the total number of subgroups of $\mathrm{Sp}_{2m}(q_0)$ of type $\mathrm{O}^+_{2m}(q_0)$ or $\mathrm{O}^-_{2m}(q_0)$ which contain $F(g\widetilde{\sigma})$.*

Proof. The maximal subgroups of G of type $\mathrm{O}^{\pm}_{2m}(q)$ which contain $g\widetilde{\sigma}$ correspond to the maximal subgroups of $\mathrm{O}_{2m+1}(q)$ of type $\mathrm{O}^{\pm}_{2m}(q)$ which are normalised by $\pi(g\widetilde{\sigma})$, and these are exactly the stabilisers of nondegenerate hyperplanes of $W = \mathbb{F}_q^{2m+1}$.

If a hyperplane U is nondegenerate, then U does not contain the radical $W \cap W^\perp = \langle x \rangle$. We claim that the converse also holds. To see this, assume $x \notin U$ and suppose that $v \in U \cap U^\perp$ is nonzero. Since $x \notin U$, we know that $v \notin \mathrm{rad}(W)$. Hence, there exists $w \in W$ such that $(v, w) \neq 0$. Therefore, $w \notin U$ and, hence, $W = \langle U, w \rangle$. In particular, $x = u + \lambda w$ for some $u \in U$ and $\lambda \neq 0$. Then $(v, x) = (v, u) + \lambda(v, w) = 0 + \lambda(v, w) \neq 0$ since $\lambda \neq 0$ and $(v, w) \neq 0$. However, $(v, x) = 0$ since $x \in W \cap W^\perp$, which is a contradiction. Therefore, $U \cap U^\perp = 0$, so U is nondegenerate. To summarise, the maximal subgroups of $\mathrm{O}_{2m+1}(q)$ of type $\mathrm{O}^{\pm}_{2m}(q)$ are exactly the stabilisers of hyperplanes not containing x.

Therefore, the maximal subgroups of G of type $\mathrm{O}^{\pm}_{2m}(q)$ which contain $g\widetilde{\sigma}$ correspond to the stabilisers in $\mathrm{O}_{2m+1}(q)$ of hyperplanes not containing x that are normalised by $\pi(g\widetilde{\sigma})$. By Lemma 2.7.3, we may lift to $\mathrm{SL}_{2m+1}(q)$ and apply Lemma 2.7.9 (see the proof of Proposition 4.3.9), which demonstrates that the stabilisers in $\mathrm{SL}_{2m+1}(q)$ of hyperplanes not containing x that are normalised by $\pi(g\widetilde{\sigma})$ correspond to the stabilisers in $\mathrm{SL}_{2m+1}(q_0)$ of hyperplanes not containing the radical of $\mathbb{F}_{q_0}^{2m+1}$ that contain $E(\pi^{-1}(g\widetilde{\sigma}))$. By the argument of the previous paragraph, the intersections of these subgroups with $\mathrm{O}_{2m+1}(q_0)$ are exactly the maximal subgroups of $\mathrm{O}_{2m+1}(q_0)$ of type $\mathrm{O}^{\pm}_{2m}(q_0)$ which contain $E(\pi^{-1}(g\widetilde{\sigma}))$. These subgroups correspond to the maximal subgroups of $\mathrm{Sp}_{2m}(q_0)$ of type $\mathrm{O}^{\pm}_{2m}(q_0)$ that contain $\pi^{-1}(E(\pi(g\widetilde{\sigma}))) = F(g\widetilde{\sigma})$. □

Remark 4.3.14. Let us clarify what we mean in the statement of Proposition 4.3.13. We are only claiming that the *total number* of $\mathcal{C}_8$ subgroups of $\mathrm{Sp}_{2m}(q)$ containing $g\widetilde{\sigma}$ is equals the total number of $\mathcal{C}_8$ subgroups of $\mathrm{Sp}_{2m}(q_0)$ containing $F(g\widetilde{\sigma})$. We are *not* claiming that the subgroups of G of type $\mathrm{O}^-_{2m}(q)$ that contain $g\widetilde{\sigma}$ correspond to the subgroups of $\mathrm{Sp}_{2m}(q_0)$ of type $\mathrm{O}^-_{2m}(q_0)$ that contain $F(g\widetilde{\sigma})$ (and the analogous claim for plus-type orthogonal groups).

Indeed, this stronger claim is, in general, false. For example, let $e = 2$ and consider $g = 1$. Then $F(\widetilde{\sigma}) = a^{-1}\widetilde{\sigma}^2 a = 1$ is contained in every subgroup of $\mathrm{Sp}_{2m}(q_0)$ and in particular in all subgroups of type $\mathrm{O}^-_{2m}(q_0)$ (of which there are $\frac{1}{2}q^m(q^m+1)$). However, we saw in Lemma 2.6.24 that there are no involutions in the coset $\mathrm{O}^-_{2m}(q)\widetilde{\sigma}$, so $\widetilde{\sigma}$ is not contained in any subgroup of $\mathrm{Sp}_{2m}(q)$ of type $\mathrm{O}^-_{2m}(q)$.

Recall the following well-known result [27, Theorem 2].

Theorem 4.3.15. *Let q be even and $m \geqslant 2$. Then every element of $\mathrm{Sp}_{2m}(q)$ is contained in at least one subgroup of type $\mathrm{O}^+_{2m}(q)$ or $\mathrm{O}^-_{2m}(q)$.*

Using Proposition 4.3.13, we can establish a generalisation of Theorem 4.3.15.

Corollary 4.3.16. *Let $q = 2^f$ and $m \geqslant 2$. Let $G = \langle \mathrm{Sp}_{2m}(q), \varphi^j \rangle$ for a proper divisor j of f. Every element of G is contained in at least one maximal subgroup of type $\mathrm{O}^+_{2m}(q)$ or $\mathrm{O}^-_{2m}(q)$.*

Proof. Let $x \in G$. If $x \in \mathrm{Sp}_{2m}(q)$, then, by Theorem 4.3.15, x is contained in at least one subgroup H of type $\mathrm{O}^\pm_{2m}(q)$ and, thus, $x \in N_G(H)$, a maximal subgroup of G of type $\mathrm{O}^\pm_{2m}(q)$. Now assume that $x \in G \setminus \mathrm{Sp}_{2m}(q)$. By Lemma 4.1.2, we may write $\langle x \rangle = \langle y \rangle$ where $y = g\varphi^i$ and i is a proper divisor of f. Writing $\widetilde{\sigma} = \varphi^i$, by Proposition 4.3.13, the number of subgroups of G of type $\mathrm{O}^\pm_{2m}(q)$ containing $g\widetilde{\sigma}$ equals the number of subgroups of $\mathrm{Sp}_{2m}(q_0)$ of type $\mathrm{O}^\pm_{2m}(q_0)$ containing $F(g\widetilde{\sigma})$, which, by Theorem 4.3.15, is at least one. □

The following is the application of Proposition 4.3.13 that feeds into our immediate concern of studying $\mathcal{M}(G, t\theta)$. We return to assuming that $m \geqslant 3$. Recall that $F(t\theta) = y$ has type $(2)^-_{q_0} \perp (2m-2)^\varepsilon_{q_0}$ where $\varepsilon = (-)^m$.

Corollary 4.3.17. *Let q be even, $m \geqslant 3$, $T = \mathrm{Sp}_{2m}(q)$ and $G = \langle T, \theta \rangle$. Then $t\theta$ is contained in exactly one $\mathcal{C}_8$ subgroup of G (either of type $\mathrm{O}^+_{2m}(q)$ or of type $\mathrm{O}^-_{2m}(q)$).*

Proof. By Proposition 4.3.13, it suffices to show that y is contained in exactly one subgroup of $T_0 = \mathrm{Sp}_{2m}(q_0)$ of type $\mathrm{O}^+_{2m}(q_0)$ or $\mathrm{O}^-_{2m}(q_0)$.

First let H_0 be a subgroup of type $\mathrm{O}^\eta_{2m}(q_0)$ containing y. We can write $y = y_1 \perp y_2$, centralising a decomposition $\mathbb{F}_{q_0}^{2m} = V_0 = V_1 \perp V_2$. Now y_1 acts irreducibly on V_1 and has order $r_1 \in \mathrm{ppd}(q_0, 2)$. Therefore, equipping V_0 with the nondegenerate quadratic form defining H_0, we see that V_1 is minus-type, since $\mathrm{O}^+_2(q_0)$ does not contain an element of order r_1 (for $|\mathrm{O}^+_2(q_0)| = 2(q_0 - 1)$). Similarly, if m is odd, then we deduce that V_2 is minus-type, and if m is even, then we deduce that V_2 is plus-type. Therefore, V_0 is plus-type if m is odd and minus-type if m is even. That is, $\eta = (-)^{m+1}$.

Continue to assume that $H_0 \cong \mathrm{O}^\eta_{2m}(q_0)$ contains y; we now know that $\eta = (-)^{m+1}$. If A is either $\mathrm{Sp}_{2m}(q_0)$ or $\mathrm{O}^\eta_{2m}(q_0)$, then two semisimple elements of odd order in A are A-conjugate if and only if they are similar, by Theorem 2.3.10. Therefore, $y^{T_0} \cap H_0 = y^{H_0}$. Moreover, by Corollary 2.3.5 and Lemma 2.4.4, we deduce that

$$|C_{T_0}(y)| = (q_0 + 1)(q_0^{m-1} - \varepsilon) = |C_{H_0}(y)|,$$

so Lemma 2.1.3 implies that y is contained in exactly one T_0-conjugate of H_0. Said otherwise, $y = F(t\theta)$ is contained in a unique subgroup of $\mathrm{Sp}_{2m}(q_0)$ of type $\mathrm{O}^\eta_{2m}(q_0)$. Proposition 4.3.13 now implies that $t\theta$ is contained in a unique $\mathcal{C}_8$ subgroup of $\mathrm{Sp}_{2m}(q)$, as claimed. □

Primitive subgroups

We now turn to general primitive subgroups. We begin with a lemma about powers of the element $y = F(t\theta)$.

Lemma 4.3.18. *A suitable power of y has type $A \perp I_{n-2}$ where*

$$A = \begin{cases} (2)^-_{q_0} & \text{if } q_0 \text{ is not Mersenne, or } T = \mathrm{PSp}_{2m}(q) \text{ and } m \text{ is even} \\ -I_2 & \text{otherwise.} \end{cases}$$

Proof. Write $\varepsilon = (-)^m$. All element types we discuss are over $\mathbb{F}_{q_0}$ and we omit the subscripts q_0 for clarity.

Case 1: q_0 is not Mersenne

First assume that $\theta = \varphi^i$. Then $y = y_1 \perp y_2 (\perp I_1)$, where y_1 has type $(2)^-$ and order $r_1 \in \mathrm{ppd}(q_0, 2)$, and y_2 has type $(2m-2)^\varepsilon$ and order $r_2 \in \mathrm{ppd}(q_0, \ell)$, where we write $\ell = (2m-2)/(m-1, 2)$. In particular, $\ell > 2$, so r_1 and r_2 are coprime. Consequently, y^{r_2} has type $(2)^- \perp I_{n-2}$ as required.

Next assume that $T = \mathrm{PSp}_{2m}(q)$ and $\theta = \delta\varphi^i$, so y has type ${}^\Delta(2)^- \perp {}^\Delta(2m-2)^\varepsilon$. Noting that $(2)^-$ has odd order, by Definition 2.3.32, $y^{(q_0^{m-1}+1)_2 (q_0-1)_2}$ has type $(2)^- \perp (2m-2)^\varepsilon$, which reduces to the previous case.

Now assume that $T = \Omega_{2m+1}(q)$ and $\theta = r_\square r_\boxtimes \varphi^i$, so y has type $(2)^- \perp {}^\Sigma(2m-2)^\varepsilon \perp I_1$. Therefore, by Definition 2.3.34, y^k has type $(2)^- \perp (2m-2)^\varepsilon \perp I_1$ for some k that is a power of two. This reduces to the first case.

Case 2: q_0 is Mersenne

In this case, an element of type $(2)^- = (2)^-_{q_0}$ has order $q_0 + 1$, which is a power of two, so we must be more careful when raising elements to even powers. However, note that elements of type $(2)^-$ and $(2m-2)^\varepsilon$ still have coprime order.

The following observation will be useful. Since q_0 is Mersenne, $q_0 \equiv -1 \pmod 4$, and hence $q_0^{m-1} \equiv (-1)^{m-1} \pmod 4$. This gives $q_0^{m-1} \not\equiv \varepsilon \pmod 4$ and $(q_0^{m-1} - \varepsilon)_2 = 2$.

If $T = \mathrm{PSp}_{2m}(q)$ and $\theta = \varphi^i$, then y has type $(2)^- \perp (2m-2)^\varepsilon$ and a power of y has type $(2)^- \perp I_{2m-2}$.

If $T = \Omega_{2m+1}(q)$ and $\theta = r_\square r_\boxtimes \varphi^i$, then y has type $(2)^- \perp (2m-2)^\varepsilon \perp I_1$, a power of which has type $(2)^- \perp I_{2m-1}$.

Now assume that $T = \mathrm{PSp}_{2m}(q)$ and $\theta = \delta\varphi^i$. Then y has type ${}^\Delta(2)^- \perp {}^\Delta(2m-2)^\varepsilon$. First assume that m is even. Then $\varepsilon = +$ and $y^{(q_0-1)_2}$ has type $(2)^- \perp (2m-2)^\varepsilon$, a suitable power of which has type $(2)^- \perp I_{2m-2}$. Next assume that m is odd. In this case, $\varepsilon = -$ and $y^{(q_0^{m-1}+1)_2 (q_0-1)_2}$ has type $w \perp I_{2m-2}$, where w has order $\frac{1}{2}(q_0+1) \geqslant 2$, since $(q_0^{m-1}+1)_2 = 2$. This implies that a suitable power of this element has type $-I_2 \perp I_{n-2}$.

Finally assume that $T = \Omega_{2m+1}(q)$ and $\theta = \varphi^i$. Then y has type $(2)^- \perp {}^{\Sigma}(2m-2)^\varepsilon \perp I_1$. Definition 2.3.34 informs us that y^2 has type $w \perp (2m-2)^\varepsilon \perp I_1$, where w has order $\frac{1}{2}(q_0+1) \geqslant 2$, so a power of y^2 has type $-I_2 \perp I_{n-2}$. This completes the proof. □

One special case requires techniques of a different flavour, so we handle it separately.

Proposition 4.3.19. *Let $G = \langle T, \theta \rangle$ where $T = \mathrm{Sp}_6(q)$ with $p = 2$ or $T = \Omega_7(q)$ with p odd. Then $t\theta$ is not contained in an almost simple subgroup of G with socle $G_2(q)$.*

Proof. Assume that $T = \Omega_7(q)$ since a very similar argument can be applied to $\mathrm{Sp}_6(q)$. For a contradiction, suppose that $t\theta$ is contained in a subgroup H of G with socle $G_2(q)$. A power of $t\theta$ is $\mathrm{SO}_7(\overline{\mathbb{F}}_p)$-conjugate to $y = F(t\theta)$, and by Lemma 4.3.18, $z = -I_2 \perp I_5$ is a power of y.

The subgroup $H \leqslant G$ arises from the embedding $G_2(\overline{\mathbb{F}}_p) \leqslant \mathrm{SO}_7(\overline{\mathbb{F}}_p)$ afforded by an irreducible representation of $G_2(\overline{\mathbb{F}}_p)$ on $\overline{V} = \overline{\mathbb{F}}_p^7$. It is well known that $\mathrm{SL}_3(\overline{\mathbb{F}}_p)$ is a maximal rank subgroup of $G_2(\overline{\mathbb{F}}_p)$ and the restriction of $\overline{V}$ to $\mathrm{SL}_3(\overline{\mathbb{F}}_p)$ decomposes as $\overline{V} = U \oplus U^* \oplus 0$ where U and 0 are the natural and trivial modules for $\mathrm{SL}_3(\overline{\mathbb{F}}_p)$.

Now $z \in G_2(\mathbb{F}_q) \leqslant G_2(\overline{\mathbb{F}}_p)$ is a semisimple element. Therefore, z is contained in a maximal torus of $G_2(\overline{\mathbb{F}}_p)$ and all maximal tori of $G_2(\overline{\mathbb{F}}_p)$ are conjugate. Since $\mathrm{SL}_3(\overline{\mathbb{F}}_p)$ is a maximal rank subgroup of $G_2(\overline{\mathbb{F}}_p)$ we deduce that z is conjugate to an element of $\mathrm{SL}_3(\overline{\mathbb{F}}_p)$. From the action of $\mathrm{SL}_3(\overline{\mathbb{F}}_p)$ on $\overline{V}$, we see that we may write

$$z = [\alpha_1, \alpha_2, \alpha_3, \alpha_1^{-1}, \alpha_2^{-1}, \alpha_3^{-1}, 1].$$

Without loss of generality, we may assume that $\alpha_1 = -1$ and $\alpha_2 = \alpha_3 = 1$. This implies that $\alpha_1\alpha_2\alpha_3 = -1$, which is a contradiction to $[\alpha_1, \alpha_2, \alpha_3] \in \mathrm{SL}_3(\overline{\mathbb{F}}_p)$. Therefore, z, and hence y, and hence $t\theta$, is not contained in a subgroup of G of type $G_2(q)$. □

We now complete the proof of Theorem 4.3.7.

Proposition 4.3.20. *Theorem 4.3.7 is true for primitive subgroups.*

Proof. Write $\varepsilon = (-)^m$. By construction, a suitable power of $t\theta$ is X-conjugate to y. By Lemma 4.3.18, we may fix a power $z = z_1 \perp I_{n-2}$ of y where

$$z_1 = \begin{cases} (2)^- & \text{if } q_0 \text{ is not Mersenne} \\ -I_2 & \text{otherwise} \end{cases}$$

and a power $w = w_1 \perp I_{n-2}$ of y where

$$w_1 = \begin{cases} (2)^- & \text{if } q_0 \text{ is not Mersenne} \\ [\lambda, \lambda^{-1}] & \text{if } q_0 \text{ is Mersenne and } T = \mathrm{PSp}_{2m}(q) \\ -I_2 & \text{otherwise} \end{cases}$$

for an element $\lambda \in \mathbb{F}_{q_0}^\times$ of order 4. Note that z has prime order.

Let $H \in \mathcal{M}(G, t\theta)$ be primitive. By Theorem 2.5.1, H is contained in one of the geometric families $\mathcal{C}_3, \ldots, \mathcal{C}_8$ or is an almost simple irreducible group in the $\mathcal{S}$ family. We consider each family in turn.

Consider $\mathcal{C}_3$ subgroups. Suppose that H is a field extension subgroup of prime degree k. Let $H_0 = H \cap \mathrm{PGL}(V)$ and write $H_0 = B.k$.

First suppose that H has type $\mathrm{Sp}_{n/k}(q^k)$ or $\mathrm{O}_{n/k}(q^k)$, where k is odd in the latter case. Lemma 2.5.7(ii) implies that $z \in B$. Moreover, since $\nu(z) = 2$, Lemma 2.5.7(i) implies that $k = 2$, which in turn implies that $T = \mathrm{PSp}_{2m}(q)$. If q_0 is not Mersenne, then we obtain a contradiction to Corollary 2.5.9(i). If q_0 is Mersenne, then Lemma 2.5.7(i) implies that z arises from an element in $\mathrm{Sp}_m(q^2)$ with exactly one nontrivial eigenvalue, which is impossible. Therefore, H is not contained in a subgroup of type $\mathrm{Sp}_{n/k}(q^k)$ or $\mathrm{O}_{n/k}(q^k)$.

Now suppose that $T = \mathrm{PSp}_{2m}(q)$ and H has type $\mathrm{GU}_m(q)$. As we argued in the proof of Lemma 4.3.18, we can fix g as a power of y of type $(2m-2)^\varepsilon \perp I_2$. Since g has odd prime order, $g \in B$. Now we apply Corollary 2.5.9. If m is even, then $\varepsilon = +$ and we contradict (ii)(a), and if m is odd, then $\varepsilon = -$ and we contradict (ii)(b) if e is odd. If m is odd and e is even, then z contradicts (ii)(c). Therefore, $H \notin \mathcal{C}_3$.

Now let us turn to $\mathcal{C}_4$ subgroups. Suppose that H is the centraliser of a decomposition $V = V_1 \otimes V_2$ where $\dim V_1 \geqslant \dim V_2 > 1$. Since $w \in H$, we may write $w = w_1 \otimes w_2$. Since $\nu(w) = 2$, Lemma 2.5.13 implies that $\nu(w_1) = 1$, $\nu(w_2) = 0$ and $\dim V_2 = 2$. If $T = \Omega_{2m+1}(q)$, then this is immediately a contradiction since $\dim V = 2m+1$ is odd. If $T = \mathrm{PSp}_{2m}(q)$, then $\nu(w_2) = 0$ and Lemma 2.5.10 implies that every eigenvalue of w appears with even multiplicity, but this is a contradiction, since the nontrivial eigenvalues of w are distinct. Therefore, $H \notin \mathcal{C}_4$

If $H \in \mathcal{C}_5$, then H has type $\mathrm{Sp}_{2m}(q_1)$ or $\mathrm{O}_{2m+1}(q_1)$ (depending on T), where $q = q_1^k$ for a prime k. By Proposition 4.3.8, there is a unique $\widetilde{G}$-class of subgroups of a given type and Lemma 2.7.11 implies that the number of $\widetilde{G}$-conjugates of H that contain $t\theta$ is at most $|C_{X_\sigma}(y)|$. Moreover, if $k = e$, then Lemma 2.7.12 implies that $t\theta$ is contained in at most e^2 subgroups of type $\mathrm{Sp}_{2m}(q_0)$ or at most e^3 subgroups of type $\mathrm{O}_{2m+1}(q_0)$.

The $\mathcal{C}_6$ family is empty since q is not prime.

We now treat $\mathcal{C}_7$ subgroups. Suppose that H is the stabiliser of a decomposition

$$V = U_1 \otimes U_2 \otimes \cdots \otimes U_k$$

with $k < n$. Let $H_0 = H \cap \mathrm{PGL}(V)$ and write $H_0 = B.S_k$. Since w does not centralise a tensor product decomposition (see the discussion of $\mathcal{C}_4$ subgroups), $w \notin B$. Therefore, w cyclically permutes the k factors.

If q_0 is not Mersenne, then w has prime order and the two nontrivial eigenvalues of w are distinct, which is inconsistent with the eigenvalue pattern required by Lemma 2.5.11(ii). Similarly, we obtain a contradiction when q_0 is Mersenne and $T = \Omega_{2m+1}(q)$.

Now assume that q_0 is Mersenne and $T = \mathrm{PSp}_{2m}(q)$. Since w acts transitively on the k tensor factors, k is even and without loss of generality $w^2 = z$ centralises the decomposition $V = V_1 \otimes V_2$ where $V_1 = \otimes_{i\,\mathrm{odd}} U_i$ and $V_2 = \otimes_{i\,\mathrm{even}} U_i$. In particular, $\dim V_1 = \dim V_2$. However, $\nu(z) = 2$, so Lemma 2.5.13 implies that $\dim V_1 = \dim V_2 = 2$, which is impossible since $\dim V = 2m \geqslant 6$. Therefore, $H \notin \mathcal{C}_7$.

If $H \in \mathcal{C}_8$, then $T = \mathrm{Sp}_{2m}(q)$, q is even and H has type $\mathrm{O}^{\varepsilon}_{2m}(q)$ for $\varepsilon \in \{+, -\}$. Moreover, by Corollary 4.3.17, $t\theta$ is contained in a unique $\mathcal{C}_8$ subgroup.

It remains to consider the $\mathcal{S}$ family. Since $\nu(z) = 2$, $n \geqslant 6$ and q is not prime, H is an exception in Theorem 2.5.14(iii). By Table 2.3, the possibilities are

(i) $T = \mathrm{Sp}_6(q)$ ($p = 2$) or $T = \Omega_7(q)$: $H = G_2(q)$

(ii) $T = \mathrm{PSp}_6(p^2)$ (p odd): $H = \mathrm{J}_2$

We excluded the possibility of case (i) in Proposition 4.3.19.

Now consider case (ii). If $q_0 \neq 3$, then $|w|$ is at least $2 \cdot 9 = 18$ (see Lemma 2.3.15), and if $q_0 = 3$, the $|w| = 4 \cdot 5 = 20$. Therefore, w is not contained in a subgroup of type J_2 since the maximum order of an element of J_2 is 15 (see [24]).

We have now considered each possible type of maximal subgroup of G and have, therefore, completed the proof. □

We have now proved Theorem 4.3.7.

4.3.3 Probabilistic method

Continue to let $T \in \mathcal{T}$ with $m \geqslant 3$ and let θ be an automorphism from Table 4.1. Fix $y \in \mathrm{Inndiag}(T_0)$ from Table 4.2 and $t\theta \in G = \langle T, \theta \rangle$ from Proposition 4.3.5. Recall that $\mathcal{M}(G, t\theta)$ is the set of maximal subgroups of G that contain $t\theta$, which is described in Theorem 4.3.7.

In this section, we prove Theorems 4A and 4C in Case II. We will also collect together results that will feed into the proof of Theorem 4B, which is further discussed in Section 4.3.4. For an integer k, define $\pi_k = (k, 2) - 1$.

Proposition 4.3.21. *Let $G = \langle \mathrm{PSp}_{2m}(q), \theta \rangle \in \mathcal{A}$ where $m \geqslant 3$ and $\theta \notin \mathrm{PGSp}_{2m}(q)$. Then*

(i) $u(G) \geqslant 2$

(ii) $u(G) \geqslant 4$ *if q is odd*

(iii) $u(G) \geqslant q - 1$ *if $m \geqslant 16$*

(iv) $u(G) \to \infty$ *as $q \to \infty$.*

Proof. We apply the probabilistic method encapsulated by Lemma 2.1.1. Let $x \in G$ have prime order. We will obtain an upper bound on

$$P(x, t\theta) \leqslant \sum_{H \in \mathcal{M}(G,t\theta)} \mathrm{fpr}(x, G/H).$$

By Lemma 2.1.1 we need to show that $P(x, t\theta) < \frac{1}{2}$ when q is even and $P(x, t\theta) < \frac{1}{4}$ when q is odd. In addition, we will establish that $P(x, t\theta) \to 0$ as $q \to \infty$.

Theorem 4.3.7 gives a superset of $\mathcal{M}(G, t\theta)$ and the bounds on the fixed point ratios $\mathrm{fpr}(x, G/H)$ are given in Chapter 3. In particular, by Theorem 3.1.1 and Proposition 3.1.3, the $\mathcal{C}_1$ subgroups contribute

$$\left(\frac{1}{q^2} + \frac{1}{q^4} + \frac{2}{q^{2m-2}}\right) + \pi_m \left(\frac{6}{q^{m-1}} + \frac{2}{q^m}\right)$$

to the upper bound on $P(x, t\theta)$, and by Proposition 3.1.5, the $\mathcal{C}_8$ subgroups contribute

$$\pi_q \left(\frac{1}{q} + \frac{1}{q^m - 1}\right).$$

Now let $H \in \mathcal{M}(G, t\theta)$ be a nonsubspace subgroup. Then Proposition 3.2.3 implies that

$$\mathrm{fpr}(x, G/H) < \sqrt{5}\, q^{-(m-3/2-\ell)}.$$

where $\ell = 0$, unless H has type $\mathrm{Sp}_m(q) \wr S_2$, in which case $\ell = 1$. From the description of the possibilities for H in Table 4.3, we see that $t\theta$ is contained in at most

$$1 + M_{\mathsf{nd}} + M_{\mathsf{ti}} + M_{\mathsf{s}}$$

nonsubspace subgroups, where M_{nd}, M_{ti} and M_{s} are the numbers of subgroups in $\mathcal{M}(G, t\theta)$ of type $\mathrm{Sp}_m(q) \wr S_2$, $\mathrm{GL}_m(q)$ and subfield subgroups, respectively.

Write

$$M = 1 + M_{\mathsf{nd}} \cdot q + M_{\mathsf{ti}} + M_{\mathsf{s}}$$

where the factor of q associated with M_{nd} is to account for the fact that $\ell = 1$ in this case. Then we have deduced that

$$P(x, t\theta) < \left(\frac{1}{q^2} + \frac{1}{q^4} + \frac{2}{q^{2m-2}}\right) + \pi_m \left(\frac{6}{q^{m-1}} + \frac{2}{q^m}\right) + \pi_q \left(\frac{1}{q} + \frac{1}{q^m - 1}\right) + \frac{M\sqrt{5}}{q^{m-3/2-\ell}}.$$

Writing $\varepsilon = (-)^m$, Theorem 4.3.7 gives

$$M_{\mathsf{nd}} \leqslant \frac{1}{2}\binom{m}{\frac{m}{2}} \quad M_{\mathsf{ti}} \leqslant 2^{(m-1,e)} \quad M_{\mathsf{s}} \leqslant \log\log q \cdot (q_0 + 1)(q_0^{m-1} - \varepsilon).$$

noting that, by Corollary 2.3.4 and Lemma 2.4.4,

$$|C_{\mathrm{PGSp}_{2m}(q_0)}(y)| = (q_0 + 1)(q_0^{m-1} - \varepsilon).$$

From here we see that if $m \geqslant 16$, then $P(x, t\theta) < \frac{1}{q-1}$, so $u(G) \geqslant q-1$, as claimed in part (iii). Therefore, we may now focus on parts (i), (ii) and (iv).

First assume that $e \geqslant 4$. Then the above bounds demonstrate that $P(x, t\theta) \to 0$ as $q \to \infty$. If $e \geqslant 5$, then these bounds also give $P(x, t\theta) < \frac{1}{2}$ when q is even and $P(x, t\theta) < \frac{1}{4}$ when q is odd. If H is a subfield subgroup, Propositions 3.2.3 and 3.2.8 allow us to improve the fixed point ratio to

$$\mathrm{fpr}(x, G/H) < \begin{cases} \sqrt{5}\, q^{-2} & \text{if } m = 3 \\ 2\, q^{-m} & \text{if } m \geqslant 4 \end{cases}$$

This gives $P(x, t\theta) < \frac{1}{2}$ if q is even and $P(x, t\theta) < \frac{1}{4}$ if q is odd, when $e = 4$.

From now on we can assume that $e \in \{2, 3\}$. Since e is prime, by Theorem 4.3.7, we have $M_{\mathsf{s}} \leqslant e^2$. With this, we can now see that $P(x, t\theta) \to 0$ as $q \to \infty$. Moreover, we obtain $P(x, t\theta) < \frac{1}{2}$ when q is even and $P(x, t\theta) < \frac{1}{4}$ when q is odd, unless $(m, q) \in \{(4, 4), (3, 8)\}$ or $(e, m) = (2, 3)$. In the former cases, we can discount the $\mathcal{C}_2$ subgroups since $m - 1$ does not divide e and we obtain the result.

Finally assume that $e = 2$ and $m = 3$. Here, Theorem 4.3.7 indicates that $M_{\mathsf{ti}} = 0$ since m is odd. With this we obtain the desired bounds on $P(x, t\theta)$ unless $q = 4$. In this case, $G = \langle \mathrm{Sp}_6(4), \varphi \rangle = \mathrm{Aut}(\mathrm{Sp}_6(4))$ and we prove that $u(G) \geqslant 2$ in MAGMA (see Section 2.8). □

Proposition 4.3.22. *Let $G = \langle T, \theta \rangle \in \mathcal{A}$ where $T = \Omega_{2m+1}(q)$ and $\theta \notin \mathrm{Inndiag}(T)$. Then*

(i) $u(G) \geqslant 3$

(ii) $u(G) \to \infty$ *as* $q \to \infty$.

Proof. We adopt the same approach as in the proof of Proposition 4.3.21 but we do not need to divide into as many cases. Let $x \in G$ have prime order. Theorem 4.3.7 gives a superset of $\mathcal{M}(G, t\theta)$ and Theorem 3.1.1 together with Propositions 3.2.4 and 3.2.8 provide bounds on the corresponding fixed point ratios. This gives

$$P(x, t\theta) < \frac{1}{q} + \frac{1}{q^2} + \frac{1}{q^3} + \frac{1}{q^{m-2}} + \frac{14}{q^{m-1}} + \frac{5}{q^m} + M\frac{\sqrt{5}}{q^{m-1}},$$

where M is the number of subfield subgroups of G containing $t\theta$. Now

$$M \leqslant \log\log q \cdot q_0(q_0 + 1)(q_0^{m-1} + 1).$$

If $e \geqslant 4$, then this shows that $P(x, t\theta) < \frac{1}{3}$ and $P(x, t\theta) \to 0$ and $q \to \infty$. If $e \in \{2, 3\}$, then $M \leqslant e^3$ and we obtain our desired bound unless $(m, q) = (3, 9)$. In this exceptional case, we obtain our desired result by determining the fixed point ratios using MAGMA. □

4.3.4 Asymptotic results

We now prove some asymptotic results towards a proof of Theorem 4B, which will be completed in Section 4.4.4.

Proposition 4.3.23. *Let (G_i) be a sequence in $\mathcal{A}$ and such that $\mathrm{soc}(G_i) = \mathrm{PSp}_{2m_i}(q_i)$. Assume that q_i is odd and $G_i \not\leqslant \mathrm{PGSp}_{2m_i}(q_i)$ for all i. Then $u(G_i) \to \infty$ if $m_i \to \infty$.*

Proof. Fix $G_i = G = \langle T, \theta \rangle$ with $T = \mathrm{PSp}_{2m}(q)$. Since we may assume that $m \geqslant 3$, we will use the notation from earlier in this section. In particular, by Proposition 4.1.5, we may assume that θ appears in Table 4.1.

As before, we will apply the probabilistic method given by Lemma 2.1.1. Assume that m is large enough so that we may fix d satisfying $1 \leqslant \sqrt{2m}/8 < d < \sqrt{2m}/4$. Let $y \in \mathrm{PGSp}_{2m}(q_0)$ have type ${}^a(2d)^- \perp {}^a(2m-2d)^-$. Then as in the proof of Proposition 4.3.5, there exists $t \in T$ such that $t\theta$ is X-conjugate to y.

As in the proof of Proposition 4.3.9, by applying Lemma 2.7.9, the unique $\mathcal{C}_1$ subgroup of G containing $t\theta$ has type $\mathrm{Sp}_{2d}(q) \times \mathrm{Sp}_{2m-2d}(q)$. There are at most $2m$ types of subgroup in each of $\mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4, \mathcal{C}_7$ and at most $\log\log q$ in $\mathcal{C}_5$. In each of these cases, by Lemma 2.7.11 and Proposition 4.3.8, there are at most $(q_0^d+1)(q_0^{m-d}+1) \leqslant 2q^{m/2}$ subgroups of each type in $\mathcal{M}(G, t\theta)$. Note that the classes $\mathcal{C}_6$ and $\mathcal{C}_8$ are empty. Since $1 < d < m-d$ a power of y has type $(2d)^- \perp I_{2m-2d}$. By Theorem 2.5.14, since $\nu(z) = 2d < \sqrt{2m}/2$, we deduce that $\mathcal{M}(G, t\theta)$ contains no subgroups from $\mathcal{S}$.

The fixed point ratio bounds in Theorem 3.1.1 and Proposition 3.2.3 imply that for all prime order elements $x \in G$,

$$P(x, t\theta) \leqslant \frac{3}{q^{m-2}} + \frac{1}{q^{\sqrt{2m}/4}} + \frac{1}{q^{m-\sqrt{2m}/4}} + (8m + \log\log q) \cdot 2q^{m/2} \cdot \frac{1}{q^{m-3}} \to 0$$

as $m \to \infty$. Therefore, $u(G) \to \infty$ as $m \to \infty$. □

With a view to Theorem 4D, we now turn to upper bounds on spread, where we allow $T = \mathrm{PSp}_4(q)$. In [37, Proposition 2.5], Guralnick and Shalev prove the following.

Theorem 4.3.24. *Let $T \in \mathcal{T}$.*

(i) *If q is even and $T = \mathrm{PSp}_{2m}(q)$, then $s(T) \leqslant q$.*

(ii) *If $T = \Omega_{2m+1}(q)$, then $s(T) < \frac{q^2+q}{2}$.*

We now establish a generalisation of Theorem 4.3.24.

Proposition 4.3.25. *Let $G \in \mathcal{A}$ and write $T = \mathrm{soc}(G)$.*

(i) *If q is even, $T = \mathrm{PSp}_{2m}(q)$ and $\theta \in \mathrm{P\Gamma Sp}_{2m}(q)$, then $s(G) \leqslant q$.*

(ii) *If $T = \Omega_{2m+1}(q)$, then $s(G) < \frac{q^2+q}{2}$.*

Proof. First consider (i). In the proof of Theorem 4.3.24(i), a set $\mathcal{X}$ of $q+1$ transvections in T is constructed with the property that for all subgroups H_0 of T with type $\mathrm{O}^+_{2m}(q)$ or $\mathrm{O}^-_{2m}(q)$ there exists $x \in \mathcal{X}$ such that $x \in H_0$. Let $g \in G$. By Corollary 4.3.17, G has at least

one subgroup H of type $\mathrm{O}^+_{2m}(q)$ or $\mathrm{O}^-_{2m}(q)$ such that $g \in H$. Therefore, there exists $x \in \mathcal{X}$ such that $x \in H$. As a result, $\langle x, g\rangle \neq G$ and $s(G) \leqslant q$.

Now consider (ii). Let $V = \mathbb{F}_q^{2m+1}$ and consider the semilinear action of G on V. Write $\ell = (q^2+q)/2$. In the proof of Theorem 4.3.24(ii), a set $\mathcal{Y}$ of ℓ reflections in T is constructed such that for all vectors $v \in V$ there exists $y \in \mathcal{Y}$ such that $vy = v$. Let $g \in G$. We will show that g stabilises a 1-space. If $g \in \mathrm{SO}_{2m+1}(q)$, then the set of eigenvalues of g is closed under taking inverses. Therefore, g must have an eigenvalue in $\{1, -1\}$, which implies that g stabilises a 1-space. If $g \in G \setminus \mathrm{SO}_{2m+1}(q)$, then without loss of generality, we may write $g = h\widetilde{\sigma}$ where $h \in \mathrm{SO}_{2m+1}(q)$ and $\widetilde{\sigma} = \varphi^i_{\mathcal{B}}$, where $q = p^f$ and i divides f. Let $X = \mathrm{SO}_{2m+1}(\overline{\mathbb{F}}_p)$, let $e = f/i$ and let F be the Shintani map of (X, σ, e). Then $F(h\widetilde{\sigma}) \in X_\sigma \cong \mathrm{SO}_{2m+1}(p^i)$, so $F(h\widetilde{\sigma})$ stabilises a 1-space of $\mathbb{F}_{p^i}^{2m+1}$ by the argument above. Therefore, Lemma 2.7.9 implies that $h\widetilde{\sigma}$ stabilises a 1-space of V. Consequently, in both cases there exists $y \in \mathcal{Y}$ such that $\langle g, y\rangle \neq G$. Hence, $s(G) < \ell$. □

We will see in Proposition 4.4.8(iii), that the condition $\theta \in \mathrm{P\Gamma Sp}_{2m}(q)$ appearing in Proposition 4.3.25(i) is necessary.

4.4 Case III

In this section, we will complete the proofs of Theorems 4A–4D by considering Case III. Write $G = \langle T, \theta \rangle$ where $T = \mathrm{PSp}_4(q)$ and $\theta \in \mathrm{Aut}(T) \setminus T$. It will be convenient to make the case distinction

(a) $G \leqslant \mathrm{P\Gamma Sp}_4(q)$

(b) $G \not\leqslant \mathrm{P\Gamma Sp}_4(q)$.

4.4.1 Element selection

As in Case II, Shintani descent plays an indispensable role in identifying an element $t\theta$. Let us fix our notation for Section 4.4.

Notation 4.4.1. Write $q = p^f$ where $f \geqslant 2$.

Let $V = \mathbb{F}_q^4$ be the natural module for $T = \mathrm{PSp}_4(q)$.

Fix the simple algebraic group $X = \mathrm{PSp}_4(\overline{\mathbb{F}}_p)$.

Fix the standard Frobenius endomorphism φ of X, defined with respect to the standard basis $\mathcal{B} = \langle e_1, f_1, e_2, f_2 \rangle$, as $(a_{ij}) \mapsto (a_{ij}^p)$, modulo scalars.

If q is even, let ρ be the graph-field endomorphism of X such that $\rho^2 = \varphi$ (see (4.5)).

By Proposition 4.1.5, in Case (a) we may assume $\theta = \varphi^i$ or q is odd and $\theta = \delta\varphi^i$, where in both cases i is a proper divisor of f. In Case (b), we may assume that $q > 2$ is even and $\theta = \rho^i$ where i is an odd (not necessarily proper) divisor of f.

Notation 4.4.1. (continued) Write $q = q_0^e$ and $e = f/i$.

Fix the pair

$$(\sigma,\, d) = \begin{cases} (\varphi^i,\, 1) & \text{in Case (a)} \\ (\rho^i,\, 2) & \text{in Case (b).} \end{cases}$$

Let F be the Shintani map of (X, σ, de), so $\widetilde{\sigma} = \sigma|_{X_{\sigma^{de}}}$ and

$$F\colon \{(g\widetilde{\sigma})^{X_{\sigma^{de}}} \mid g \in X_{\sigma^{de}}\} \to \{x^{X_\sigma} \mid x \in X_\sigma\}.$$

Observe that $X_{\sigma^e} = \mathrm{Inndiag}(T)$ and $X_\sigma = \mathrm{Inndiag}(T_0)$ where

$$T_0 = \begin{cases} \mathrm{PSp}_4(q_0) & \text{in Case (a)} \\ {}^2B_2(q_0) & \text{in Case (b)} \end{cases}$$

(Note that $X_\sigma = T_0$ in Case (b).)

We now define our elements. We begin with a comment on Suzuki groups.

Remark 4.4.2. Consider Case (b). The order of ${}^2B_2(q_0)$ is $q_0^2(q_0-1)(q_0^2+1)$. Since any primitive prime divisor r of q_0^4-1 divides q_0^2+1, we deduce that ${}^2B_2(q_0)$ contains an element of order r, which is necessarily an element of type $(4)^-_{q_0}$, thought of as an element of $\mathrm{Sp}_4(q_0)$.

Let us now use Shintani descent to fix an element $t\theta$. (Note that the definition of a in (4.9) implies that a is the empty symbol unless $\theta = \delta\varphi^i$ in which case $a = \Delta$.)

Proposition 4.4.3. *Let $T = \mathrm{PSp}_4(q)$ and let $\theta \in \{\varphi^i, \delta\varphi^i, \rho^i\}$ where i divides f. Let $y \in \mathrm{Inndiag}(T_0)$ have type ${}^a(4)^-_{q_0}$. Then there exists $t \in T$ such that $(t\theta)^{de}$ is X-conjugate to y.*

Proof. This follows from Theorem 2.7.1 in conjunction with Lemma 4.3.2 (see the proof of Proposition 4.3.5). □

4.4.2 Maximal subgroups

Continue to let $T = \mathrm{PSp}_4(q)$ and let $\theta \in \{\varphi^i, \delta\varphi^i, \rho^i\}$ where i is a proper divisor of f. Fix $y \in \mathrm{Inndiag}(T_0)$ and $t\theta \in G = \langle T, \theta\rangle$ from Proposition 4.4.3. We now describe $\mathcal{M}(G, t\theta)$.

Theorem 4.4.4. *The maximal subgroups of G that contain $t\theta$ are listed in Table 4.4, where $m(H)$ is an upper bound on the multiplicity of subgroups of type H in $\mathcal{M}(G, t\theta)$.*

Before we prove Theorem 4.4.4, let us deal with two special cases that occur in Case (b).

Proposition 4.4.5. *Let $q = 2^f$ and let i be a proper odd divisor of f such that $e = f/i$ is prime. Let $G = \langle T, \theta\rangle$ where $T = \mathrm{Sp}_4(q)$ and $\theta = \rho^i$. Then $t\theta$ is contained in at most e subgroups of G of type $\mathrm{Sp}_4(2^i)$.*

Proof. Recall that $X = \mathrm{Sp}_4(\overline{\mathbb{F}}_2)$ and $q = q_0^e$. In addition,

$$F\colon \{(g\rho^i)^{\mathrm{Sp}_4(q)} \mid g \in \mathrm{Sp}_4(q)\} \to \{x^{{}^2B_2(q_0)} \mid x \in {}^2B_2(q_0)\}$$

is the Shintani map of $(X, \rho^i, 2e)$. Define

$$E\colon \{(g\varphi^i)^{\mathrm{Sp}_4(q)} \mid g \in \mathrm{Sp}_4(q)\} \to \{x^{\mathrm{Sp}_4(q_0)} \mid x \in \mathrm{Sp}_4(q_0)\}$$

as the Shintani map of (X, φ^i, e). Now $y \in {}^2B_2(q_0)$ and $F(t\rho^i) = y$. By Lemma 2.7.6, $E((t\rho^i)^2) = y$. Let $H = \langle \mathrm{Sp}_4(q_0), \rho^i\rangle$, and write $G_1 = \langle \mathrm{Sp}_4(q), \varphi^i\rangle$ and $H_1 = \langle \mathrm{Sp}_4(q_0), \varphi^i\rangle$. By Lemma 2.7.12 (applied to E), $t\rho^i$ is contained in at most e G_1-conjugates of H_1. Since H_1 and G_1 are index two subgroups of H and G, the subgroups of type $\mathrm{Sp}_4(q_0)$ in G_1 and G are in bijection, with each G-conjugate of H in G having exactly one G_1-conjugate of H_1 as an index two subgroup. Consequently, $t\rho^i$ is contained in at most e G-conjugates of H, as required. □

Before we handle the next case, let us present the following technical lemma.

Table 4.4: Case III: Description of $\mathcal{M}(G, t\theta)$

case		type of H	$m(H)$	conditions
(a)	$\mathcal{C}_2$	$\mathrm{Sp}_2(q) \wr S_2$	1	e even
		$\mathrm{GL}_2(q)$	N	q odd
	$\mathcal{C}_3$	$\mathrm{Sp}_2(q^2)$	1	e odd
		$\mathrm{GU}_2(q)$	N	q odd
	$\mathcal{C}_5$	$\mathrm{Sp}_4(q^{1/k})$	e	$k = e$
			N	$k \neq e$
	$\mathcal{C}_8$	$\mathrm{O}_4^\varepsilon(q)$	1	q even
	$\mathcal{S}$	${}^2B_2(q)$	N	q even, f odd
		$\mathrm{PSL}_2(q)$	N	q odd
(b)	$\mathcal{C}_5$	$\mathrm{Sp}_4(q^{1/k})$	e	$k = e$
			N	$k \neq e$
	$\mathcal{S}$	${}^2B_2(q)$	1	$e = 1$
			N	$e \neq 1$
	$\mathcal{N}$	$\mathrm{O}_2^+(q) \wr S_2$	N	$e \neq 1$
		$\mathrm{O}_2^-(q) \wr S_2$	N	$e \neq 1$
		$\mathrm{O}_2^-(q^2)$	N	

[$N = |C_{X_\sigma}(y)|$ and k is prime]

Lemma 4.4.6. *Let $q = 2^f$ where f is odd. Let $T = \mathrm{Sp}_4(q)$ and $S = {}^2B_2(q)$. Let r be a primitive prime divisor of $q^4 - 1$. Then every element of T of order r is T-conjugate to an element of S.*

Proof. This is a consequence of Sylow's Theorem. Let $x \in T$ have order r. Let R be a Sylow r-subgroup of S. Let r^k be the largest r-power dividing $|T| = q^4(q^2-1)(q^4-1)$. Since r is a primitive prime divisor of $q^4 - 1$ we know that r divides $q^2 + 1$ and consequently r^k divides $q^2 + 1$. Therefore, r^k divides $|S| = q^2(q-1)(q^2+1)$. Consequently, R is also a Sylow r-subgroup of T. Now x is contained in a Sylow r-subgroup Q of T. Since all Sylow r-subgroups of T are T-conjugate, there exists $g \in T$ such that $Q^g = R$ and, therefore, $x^g \in R \leqslant S$, as claimed. □

Proposition 4.4.7. *Let $q = 2^f$ where f is odd. Let $G = \langle T, \theta \rangle$ where $T = \mathrm{Sp}_4(q)$ and $\theta = \rho^f$. Then $t\theta$ is contained in exactly one subgroup of G of type ${}^2B_2(q)$.*

Proof. There is a unique G-class of subgroups of type ${}^2B_2(q)$ in G (see [7, Table 8.14]). Let $T_0 = C_T(\theta) \cong {}^2B_2(q)$ and $H = C_G(\theta) = C_T(\theta) \times \langle \theta \rangle$. We need to show that $t\theta$ is contained in exactly one G-conjugate of H. Thus, if we assume that $t\theta \in H$, by Lemma 2.1.3, it suffices to show that $|C_G(t\theta)| = |C_H(t\theta)|$ and $(t\theta)^G \cap H = (t\theta)^H$.

Let us first show that $|C_G(t\theta)| = |C_H(t\theta)|$. The Shintani map

$$F\colon \{(g\theta)^T \mid t \in T\} \to \{x^{T_0} \mid x \in T_0\}$$

is defined as $F(g\theta) = a^{-1}(g\theta)^2 a$ where $a^{-\theta^{-1}}a = g$. By Theorem 2.7.1,

$$|C_G(t\theta)| = 2|C_T(t\theta)| = 2|C_{T_0}(F(t\theta))|.$$

By construction, the order of $F(t\theta) \in T_0$ is a primitive prime divisor r of $q^4 - 1$. Since r divides $q + \varepsilon\sqrt{2q} + 1$ for some $\varepsilon \in \{+, -\}$, by [61, Proposition 16],

$$|C_{T_0}(x)| = q + \varepsilon\sqrt{2q} + 1,$$

for every element $x \in T_0$ of order r. Since $t\theta$ has order $2r$, t has order r and

$$2|C_{T_0}(F(t\theta))| = 2(q + \varepsilon\sqrt{2q} + 1) = 2|C_{T_0}(t\theta)| = |C_H(t\theta)|.$$

We will now prove that $(t\theta)^G \cap H = (t\theta)^H$. Let $s\theta \in H$ be G-conjugate to $t\theta$. We will first show that s and t are T-conjugate. By Remark 2.7.7(i), $s\theta$ and $t\theta$ are T-conjugate. Therefore, $s^2 = (s\theta)^2$ and $t^2 = (t\theta)^2$ are T-conjugate. Record that $s, t \in C_T(\theta) \leqslant T$ have order r. Since r is odd, the square map on T permutes the T-classes of order r. Therefore, since s^2 and t^2 are T-conjugate, s and t are T-conjugate.

We will now verify that $s\theta$ and $t\theta$ are $C_T(\theta)$-conjugate. Observe that it suffices to show that s and t are $C_T(\theta)$-conjugate. Since s and t are T-conjugate it suffices to show that no two $C_T(\theta)$-classes of elements of order r are fused into one T-class. By Lemma 4.4.6, every element of T of order r is T-conjugate to an element of $C_T(\theta)$. Hence, it suffices to verify that there are the same number of classes of elements of order r in $C_T(\theta) \cong {}^2B_2(q)$ and $T \cong \mathrm{Sp}_4(q)$.

First consider ${}^2B_2(q)$. Let $\mathcal{K}$ be the set of centralisers of elements of order r in ${}^2B_2(q)$. By [61, Proposition 16], for all $K \in \mathcal{K}$, $|K| = q + \varepsilon\sqrt{2q} + 1$ and $C_{{}^2B_2(q)}(K) = K$. In particular, two members of $\mathcal{K}$ are either equal or intersect trivially. Moreover, by [61, Theorem 9], all members of $\mathcal{K}$ are ${}^2B_2(q)$-conjugate. Since $|N_{{}^2B_2(q)}(K)| = 4|K|$, for all $x \in K$, $|x^{{}^2B_2(q)} \cap K| = 4$. Therefore, there are $(r-1)/4$ conjugacy classes of elements of order r in ${}^2B_2(q)$. Now consider $\mathrm{Sp}_4(q)$. The conjugacy classes of elements of order r in $\mathrm{Sp}_4(q)$ are represented by the elements $[\lambda, \lambda^q, \lambda^{q^2}, \lambda^{q^3}]$ where $\lambda \in \mathbb{F}_{q^4}$ is a nontrivial rth root of unity. Hence, there are $(r-1)/4$ conjugacy classes of elements of order r. This establishes that $(t\theta)^G \cap H = (t\theta)^H$ and, thus, proves the result. □

Proof of Theorem 4.4.4. Let $H \in \mathcal{M}(G, t\theta)$. Evidently $T \not\leqslant H$, so, by Theorem 2.5.1, H is contained in one of the families $\mathcal{C}_1, \ldots, \mathcal{C}_8$ of geometric subgroups, $\mathcal{S}$ of almost simple subgroups or $\mathcal{N}$ of novelty subgroups. A complete list of the possible types of subgroups is given in [7, Tables 8.12–8.14]. In particular, note that there is a unique $\langle X_{\sigma^e}, \widetilde{\sigma}\rangle$-conjugacy class of subgroups of each type. Write $V = \mathbb{F}_q^4$ and $V_0 = \mathbb{F}_{q_0}^4$.

We begin with reducible subgroups. As in the proof of Proposition 4.3.9, if H has type P_1 or P_2 in Case (a) or type $P_1 \cap P_2$ in type Case (b), then $H \leqslant \langle Y_{\sigma^{de}}, \widetilde{\sigma} \rangle$, where Y is a closed connected subgroup of X of type P_1, P_2 or $P_1 \cap P_2$, respectively. Therefore, by Lemma 2.7.9, the number of X_{σ^e}-conjugates of H which contain $t\theta$ is equal to the number of X_σ-conjugates of $H \cap X_\sigma$ which contain y. However, y acts irreducibly on V_0, so $t\theta$ is not contained in a parabolic subgroup.

We next let q be even and turn to orthogonal subgroups in Case (a). By Proposition 4.3.13, the total number of $\mathcal{C}_8$ subgroups of G that contain $t\theta$ equals the total number of $\mathcal{C}_8$ subgroups of T_0 that contain y. Now the order of y is a primitive prime divisor of $q_0^4 - 1$, so y is not contained in any subgroups of type $\mathrm{O}_4^+(q_0)$. Moreover, $y^{\mathrm{Sp}_4(q_0)} \cap \mathrm{O}_4^-(q_0) = y^{\mathrm{O}_4^-(q_0)}$ and $|C_{\mathrm{Sp}_4(q_0)}(y)| = q_0^2 + 1 = |C_{\mathrm{O}_4^-(q_0)}(y)|$, so Lemma 2.1.3 implies that y is contained in a unique subgroup of type $\mathrm{O}_4^-(q_0)$. Therefore, we conclude that $t\theta$ is contained in a unique $\mathcal{C}_8$ subgroup of G.

The remaining types of subgroups of G all appear in Table 4.4. Let us now justify the conditions and multiplicities that are stronger than those given by Lemma 2.7.11.

Assume that H has type $\mathrm{Sp}_2(q) \wr S_2$ in Case (a). We will show that e is even and $t\theta$ is contained in a unique G-conjugate of H. The argument is similar to, but briefer than, the proof of Proposition 4.3.10. Suppose that H is the stabiliser of a decomposition $V = V_1 \oplus V_2$ where V_1 and V_2 are nondegenerate 2-spaces and let B be the index two centraliser of the decomposition. A power g of y has type $(4)^-_{q_0}$. Since g stabilises the decomposition and has odd order, g centralises the decomposition. Therefore, each of the eigenvalues of g is contained in $\mathbb{F}_{q^2}$. In particular, since $q = q_0^e$ and the eigenvalues of g are not contained in a proper subfield of $\mathbb{F}_{q_0^4}$, it must be that e is even. Therefore, Lemma 2.3.36 implies that y has type $(2)^\varepsilon_q \perp (2)^\varepsilon_q$ for some $\varepsilon \in \{+, -\}$. Now Corollary 2.3.4 and Lemma 2.4.4 give

$$|C_G(g)| = |\mathrm{GL}_1^\varepsilon(q)||\mathrm{GL}_1^\varepsilon(q)| = |C_B(g)| = |C_H(g)|.$$

Moreover, as in Case 1 of the proof of Proposition 4.3.10, $g^G \cap H = g^H$. Therefore, Lemma 2.1.3 implies that g, and thus $t\theta$, lies in at most one G-conjugate of H.

Next assume that H has type $\mathrm{Sp}_2(q^2)$ in Case (a). Write $H_0 = H \cap \mathrm{PGSp}_4(q)$ and $H_0 = B.2$. Since y has odd order, $y \in B$. Suppose that e is even. Then Lemma 2.3.36 implies that y has type $(4)^-_{q_0} = (2)^\eta_q \perp (2)^\eta_q$, where $\eta = (-)^{e/2}$. Therefore, Corollary 2.5.8 implies that $y \notin B$, which is a contradiction. Therefore, e is odd. In this case Lemma 2.3.36 implies that y has type $(4)^-_q$. Therefore, $y = [\lambda, \lambda^q, \lambda^{q^2}, \lambda^{q^3}]$ where $y \in \mathbb{F}_{q^4}$. Now y arises from an element $x \in B$ with eigenvalues $[\lambda, \lambda^{q^2}]$ or $[\lambda^q, \lambda^{q^3}]$. Now $[\lambda, \lambda^{q^2}]$ and $[\lambda^q, \lambda^{q^3}]$ are H_0-conjugate (although not B-conjugate), so $y^L \cap H_0 = y^{H_0}$, where $L = G \cap \mathrm{PGSp}_4(q)$. Moreover, $|C_L(x)| = q^2 + 1 = |C_{H_0}(y)|$, by Lemma 2.4.4. Hence, by Lemma 2.1.3, y, and hence $t\theta$, is contained in at most one G-conjugate of H.

Now assume that e is prime and H has type $\mathrm{Sp}_4(q_0)$. We claim that $t\theta$ is contained in at most e conjugates of H. In Case (a) this is a consequence of Lemma 2.7.12, and in Case (b) this is Proposition 4.4.5.

Finally assume that q is even, $\theta = \rho^i$ and $e = 1$. In this case, the uniqueness of the subgroup of type ${}^2B_2(q)$ follows from Proposition 4.4.7 and there are no subgroups of type $\mathrm{O}_2^\varepsilon(q) \wr S_2$ in $\mathcal{M}(G, t\theta)$ since the order of y is a primitive prime divisor of of $q^4 - 1$, which does not divide the order of these groups. This completes the proof. □

4.4.3 Probabilistic method

The following is the final part of the proof of Theorem 4A.

Proposition 4.4.8. *Let $G = \langle \mathrm{PSp}_4(q), \theta \rangle$ where $\theta \in \mathrm{Aut}(\mathrm{PSp}_4(q)) \setminus \mathrm{PSp}_4(q)$. Then*

(i) $u(G) \geqslant 2$

(ii) $u(G) \to \infty$ *as* $q \to \infty$

(iii) $u(G) \geqslant q^2/18$ *if θ is an involutory graph-field automorphism.*

Proof. For $q \in \{4, 8, 9, 16, 25, 27\}$ the result can be verified computationally in MAGMA (see Section 2.8 for a description of our computational methods). Therefore, we may assume that $q \geqslant 32$. Let $x \in G$ have prime order.

First assume that θ is a field automorphism. Theorem 4.4.4 gives a superset of $\mathcal{M}(G, t\theta)$ and together with the fixed point ratios in Theorem 3.1.1 and Proposition 3.2.5 we obtain

$$P(x, t\theta) \leqslant \frac{4(q_0^2+1)(3+2+\log\log q)}{q(q-1)} + \frac{q}{q^2-1} + \frac{1}{q} + \frac{1}{q^2-1} \tag{4.15}$$

$$\leqslant \frac{4(q+1)(3+2+\log\log q)}{q(q-1)} + \frac{q}{q^2-1} + \frac{1}{q} + \frac{1}{q^2-1}. \tag{4.16}$$

The asymptotic statement in (ii) now follows from (4.16). If $q \geqslant 64$, then $P(x, t\theta) < \frac{1}{2}$ by (4.15). If $q = 32$, then $q_0 = 2$ and $P(x, t\theta) < \frac{1}{2}$, by (4.15). Therefore, $u(G) \geqslant 2$.

Now assume that θ is a graph-field automorphism. Therefore, $q = 2^f$ and

$$P(x, t\theta) \leqslant \frac{4 \cdot 5(q_0 + \sqrt{2q_0} + 1)}{q(q-1)} \leqslant \frac{20(q + \sqrt{2q} + 1)}{q(q-1)}$$

which gives (ii). If θ does not have order two, then $P(x, t\theta) < \frac{1}{2}$ and (i) follows. (If $q = 32$, then we use the observation that $q_0 = 2$ since θ does not have order 2.) If θ is an involutory graph-field automorphism, then, $e = 1$, so Theorem 4.4.4 gives refined subgroup multiplicities and Proposition 3.2.5 has refined fixed point ratios, which together give

$$P(x, t\theta) \leqslant \frac{8(q + \sqrt{2q} + 1)}{q^2(q-1)} + \frac{1}{q^2} \leqslant \frac{16}{q^2} + \frac{1}{q^2} < \frac{18}{q^2}.$$

Therefore, $u(G) \geqslant q^2/18$. This proves (i) and (iii), thus completing the proof. □

4.4.4 Proofs of Main Results

Let us demonstrate that we have now proved Theorems 4A–4D.

Proof of Theorems 4A and 4C. Proposition 4.1.5 details the groups $G = \langle T, \theta \rangle$ that must be considered in order to prove Theorem 4A. If $\mathrm{soc}(G) = \mathrm{PSp}_{2m}(q)$ and $p = 2$ or $m = 2$, then $u(G) \geqslant 2$ is shown in Propositions 4.2.1, 4.3.21 and 4.4.8. If $\mathrm{soc}(G) = \mathrm{PSp}_{2m}(q)$ and $m > 2$ and $p > 2$, then $u(G) \geqslant 4$ is shown in Propositions 4.2.1 and 4.3.21. If $\mathrm{soc}(G) = \Omega_{2m+1}(q)$, then $u(G) \geqslant 3$ is shown in Proposition 4.3.22. □

Proof of Theorems 4B and 4D. Let (G_i) be a sequence of groups in $\mathcal{A}$ with $|G_i| \to \infty$. First assume that (G_i) has no subsequence of odd-dimensional orthogonal groups or even characteristic symplectic groups, over a field of fixed size. Then (G_i) is the union of two sequences: groups for which the field size q tends to infinity and symplectic groups in odd characteristic whose dimension n tends to infinity. In both cases the uniform spread is unbounded, by Proposition 4.3.23 in the latter case and by Propositions 4.2.1, 4.3.21, 4.3.22 and 4.4.8 in the former cases.

Now assume that (G_i) has a subsequence (G_{i_j}) of odd-dimensional orthogonal groups or even characteristic symplectic groups, over a field of fixed size q. Then Proposition 4.3.25 implies that $u(G_{i_j}) \leqslant s(G_{i_j}) < (q^2 + q)/2$, so $u(G_i)$ does not tend to infinity. □

In particular, we have proved Theorems A and B for almost simple groups whose socles are symplectic or odd-dimensional orthogonal groups. In the next, and final, chapter we turn our attention to almost simple even-dimensional orthogonal groups.

As noted at the beginning of this chapter, much of this work appears in the author's published single-author paper [38]. To abide by the University's antiplagiarism procedures, we indicate which individual results in this chapter correspond to ones in that paper. In each case, the first reference is to this thesis and the second is to the roughly equivalent result in [38]. Here we go: 4.2.1 is 4.2; 4.3.2 is 2.4; 4.3.3 is 2.5; 4.3.7 is 4.6; 4.3.8 is 4.7; 4.3.9 is 4.9; 4.3.10 is 4.11; 4.3.13 is 2.10; 4.3.15 is 2.11; 4.3.17 is 4.14; 4.3.20 is 4.15; 4.3.21 is 4.20; 4.3.22 is 4.21; 4.3.23 is 4.23; 4.3.25 is 4.25; 4.4.4 is 4.18; 4.4.7 is 4.16; 4.4.8 is 4.22. Phew.

5

Groups of Type D_m

The work in this chapter is original and unpublished.

Let us now turn to the groups of type D_m, or said otherwise groups G whose socle T is an even-dimensional orthogonal group. In this chapter, we write $q = p^f$ and

$$\mathcal{T} = \mathcal{T}_{\mathsf{D}} = \{\mathrm{P}\Omega^{\varepsilon}_{2m}(q) \mid m \geqslant 4 \text{ and } \varepsilon \in \{+,-\} \text{ where } (m,\varepsilon) \neq (4,+)\} \tag{5.1}$$

$$\mathcal{A} = \mathcal{A}_{\mathsf{D}} = \{\langle T, \theta\rangle \mid T \in \mathcal{T},\ \theta \in \mathrm{Aut}(T)\}. \tag{5.2}$$

The main results of this chapter are the following.

Theorem 5A. *If $G \in \mathcal{A}$, then $u(G) \geqslant 2$.*

Theorem 5B. *Let (G_i) be a sequence of groups in $\mathcal{A}$ with $|G_i| \to \infty$. Then $u(G_i) \to \infty$ unless (G_i) has an infinite subsequence of groups such that $\mathrm{soc}(G_i) = \mathrm{P}\Omega^{\varepsilon_i}_{2m_i}(q)$ for some fixed q and $G_i \cap \mathrm{PGO}^{\varepsilon_i}_{2m_i}(q) \not\leqslant \mathrm{PDO}^{\varepsilon_i}_{2m_i}(q)$.*

The author suspects that, in Theorem 5B, the sufficient condition on the sequence (G_i) for $u(G_i) \to \infty$ is necessary and we refer to Remark 5.3.25 for further comments.

We now discuss how we prove these results. Our general approach to showing that $G = \langle T, \theta\rangle \in \mathcal{A}$ satisfies $u(G) \geqslant k$ is the same as in Chapter 4. In particular, we adopt the probabilistic method from Section 2.1, which involves selecting an element $s \in T\theta$, studying the set $\mathcal{M}(G,s)$ of the maximal overgroups of s and bounding a probability via fixed point ratios. However, let us highlight the various new obstacles that we need to surmount in this case.

Determination of cases

First, the structure of the automorphism group of T is particularly complicated, so determining exactly which cases it suffices to consider requires a detailed analysis, which is the focus on Section 5.1. Here Proposition 5.1.12 is the main result. We will need to consider diagonal, graph and field automorphisms, together with products thereof.

Graph automorphisms

If θ is a diagonal or graph automorphism, then $G \leqslant \mathrm{PGL}(V)$ and we can work in terms of matrices. When θ is diagonal, then, as in Chapter 4, the argument mirrors the work in [10]. However, when θ is a graph automorphism (for example, a reflection), then we must necessarily select an element $s \in T\theta$ that fixes a 1-space of $\mathbb{F}_q^{2m}$, which makes bounding $P(x,s)$ more difficult (recall from Chapter 3 that the fixed point ratio of an element of prime order on 1-spaces can be as large as roughly q^{-1}). Consequently, we give a constructive proof that some specific pairs of elements generate G in addition to a probabilistic argument which deals with the general case (see Proposition 5.2.12). This constructive argument is of a different flavour to much of the rest of this thesis.

Obstructions to Shintani descent

When $\theta \notin \mathrm{PGO}_{2m}^{\pm}(q)$, then we apply Shintani descent. However, unlike in Chapter 4, complications arise here. Recall that the premise of Shintani descent is that we can write $\theta \in \mathrm{Inndiag}(T)\tilde{\sigma}$ and $\mathrm{Inndiag}(T) = X_\omega$ for an algebraic group X and Steinberg endomorphisms σ and ω, where $\tilde{\sigma} = \sigma|_{\mathrm{Inndiag}(T)}$. In Chapter 4 we could always arrange this setup such that $\omega = \sigma^e$ for some $e > 1$. However, in this chapter, this will not always be the case.

For instance, assume that $q = 2^e$, $T = \Omega_{2m}^{+}(q)$ and $\theta = r\tilde{\sigma}$, where σ is the field automorphism $(a_{ij}) \mapsto (a_{ij}^2)$ and r is a reflection (see Definition 2.6.15). Then σ is a Steinberg endomorphism of $X = \Omega_{2m}(\overline{\mathbb{F}}_p)$ and we have $T = X_{\sigma^e}$. If e is even, then $\tilde{\sigma}^e = (r\tilde{\sigma})^e$ and we can apply Shintani descent as in Chapter 4. However, if e is odd, then we cannot write $\tilde{\sigma}^e$ as a power of $r\tilde{\sigma}$ and we need a different approach (see Example 2.7.2). In the latter case, we need to be more flexible with our application of Shintani descent and we will use Lemma 2.7.13 (see Example 2.7.14).

Minus-type orthogonal groups

There are two natural definitions the minus-type orthogonal group $\mathrm{O}_{2m}^{-}(q)$. On one hand, it is the isometry group of a minus-type quadratic form on the vector space $\mathbb{F}_q^{2m}$ and consequently is naturally a subgroup of $\mathrm{GL}_{2m}(q)$. This perspective affords a concrete means of studying the group via its action on $\mathbb{F}_q^{2m}$. On the other hand, this group is the fixed points under a Steinberg endomorphism of the algebraic group $\mathrm{O}_{2m}(\overline{\mathbb{F}}_p)$, and the group obtained in this way is not a subgroup of $\mathrm{GL}_{2m}(q)$ but is naturally a subgroup of $\mathrm{O}_{2m}^{+}(q^2)$. This viewpoint allows one to exploit the theory of algebraic groups, in particular, Shintani descent. In this chapter, we need to translate between these two (isomorphic) groups and the isomorphism Ψ from Lemma 2.6.17 is the key tool for this.

Let us now turn to the organisation of this chapter. To prove Theorems 5A and 5B, we consider two natural cases

I $\theta \in \mathrm{PGO}^{\varepsilon}_{2m}(q)$

II $\theta \in \mathrm{Aut}(T) \setminus \mathrm{PGO}^{\varepsilon}_{2m}(q)$.

In both Cases I and II, we define the following two subcases

(a) $G \cap \mathrm{PGO}^{\varepsilon}_{2m}(q) \leqslant \mathrm{PDO}^{\varepsilon}_{2m}(q)$

(b) $G \cap \mathrm{PGO}^{\varepsilon}_{2m}(q) \not\leqslant \mathrm{PDO}^{\varepsilon}_{2m}(q)$.

Recall that $\mathrm{PDO}^{\varepsilon}_{2m}(q)$ is our nonstandard notation for the group defined in Section 2.2.6. In (2.20) in Section 2.6.5, we observed that $\mathrm{PDO}^{\varepsilon}_{2m}(q) = \mathrm{Inndiag}(\mathrm{P}\Omega^{\varepsilon}_{2m}(q))$.

In short, Cases I(b) and II(b) are more difficult than Cases I(a) and II(a). In Case I(b) we encounter the obstacle of graph automorphisms we discussed above, and Case II(b) is exactly the situation in which Shintani descent does not apply directly.

The structure of this chapter mirrors that of Chapter 4. In particular, in Section 5.1, we will determine the precise cases that must be considered, then Theorems 5A and 5B in Cases I and II will be proved in Sections 5.2 and 5.3.

Remark. In the definition of $\mathcal{T}$, we exclude $\mathrm{P}\Omega^{+}_{8}(q)$. This is the most exotic classical simple group since it admits a *triality* automorphism. Consequently, there are additional almost simple groups to consider in this case (see Remark 5.1.15) and while the techniques of Shintani descent that feature in this chapter are general enough to encompass these cases, the triality automorphism imposes further restrictions on how we may select the element s (see Remark 5.3.26).

Moreover, the effects of triality can be seen even when we consider extensions G of $\mathrm{P}\Omega^{+}_{8}(q)$ by field and involutory graph automorphisms. In particular, there are subgroups of G that one might not expect to be $\mathrm{Aut}(T)$-conjugate (for example, subgroups in different geometric families) that are conjugate under triality. This, together with the usual restrictions imposed by working with a group of small rank, has the consequence of making the analysis of these groups more intricate.

Almost simple groups with socle $\mathrm{P}\Omega^{+}_{8}(q)$ will be the focus of future work.

5.1 Automorphisms

Let $T \in \mathcal{T}$. The main result of this section is Proposition 5.1.12, which details the automorphisms $\theta \in \mathrm{Aut}(T)$ it suffices to consider in order to prove Theorems 5A and 5B.

For the entire section, write $n = 2m$, $q = p^f$ and $V = \mathbb{F}_q^n$. Further, let $\mathcal{B}^\varepsilon$ be the basis from (2.5) or (2.6). Write $\mathbb{F}_q^\times = \langle \alpha \rangle$. In addition, if q is odd, then let $\beta \in \mathbb{F}_q^\times$ with $|\beta| = (q-1)_2$ and note that $\alpha, \beta \notin (\mathbb{F}_q^\times)^2$.

5.1.1 Plus-type

Let $T = \mathrm{P}\Omega^+_{2m}(q)$ and assume that $m \geqslant 5$. The automorphism group of T was recorded in Lemma 2.6.18(iii). We now describe $\mathrm{Out}(T)$ in more detail.

For this section, we fix the standard Frobenius endomorphism $\varphi = \varphi_{\mathcal{B}^+} \colon (a_{ij}) \mapsto (a_{ij}^p)$ and the reflection $r \in \mathrm{PO}^+_{2m}(q)$ from Definitions 2.6.9 and 2.6.15. It will be useful to fix $r_\square$ and $r_\boxtimes$ as the images in $\mathrm{PO}^+_{2m}(q)$ of reflections in vectors of square and nonsquare norm respectively (evidently, if q is even, then we do not use the notation $r_\boxtimes$). In [43, Section 2], the symbols $r_\square$ and $r_\boxtimes$ (and also δ, introduced below) refer to elements of $\mathrm{GO}^+_{2m}(q)$, but we prefer to use these symbols for elements of $\mathrm{PGO}^+_{2m}(q)$.

If q is odd, then observe that the element $\delta^+ \in \mathrm{PGL}_{2m}(q)$ defined in Definition 4.1.3 is an element of $\mathrm{PDO}^+_{2m}(q)$. We make use of the element δ^+ in this chapter also. As in Chapter 4, we will refer to δ^+ simply as δ if the sign is understood. (A different element $\delta^- \in \mathrm{PDO}^-_{2m}(q)$ will be introduced in Section 5.1.2.) The information in Remark 4.1.4 holds true in the context of plus-type orthogonal groups.

A description of $\mathrm{Out}(T)$ is given in [43, Proposition 2.7.3].

Lemma 5.1.1. *Let $T = \mathrm{P}\Omega^+_{2m}(q)$ and assume that $m \geqslant 5$. Then*

$$\mathrm{Out}(T) = \begin{cases} \langle \ddot{r}_\square \rangle \times \langle \ddot{\varphi} \rangle \cong C_2 \times C_f & \text{if } q \text{ is even} \\ \langle \ddot{\delta} \rangle \times \langle \ddot{r}_\square \rangle \times \langle \ddot{\varphi} \rangle \cong C_2 \times C_2 \times C_f & \text{if } q \text{ is odd and } D(Q) = \boxtimes \\ \langle \ddot{\delta}, \ddot{r}_\square, \ddot{r}_\boxtimes, \ddot{\varphi} \rangle \cong D_8 \times C_f & \text{if } q \text{ is odd and } D(Q) = \square. \end{cases}$$

Remark 5.1.2. Let $T = \mathrm{P}\Omega^+_{2m}(q)$. Assume that q is odd and $D(Q) = \square$. By [43, Proposition 2.7.3(iii)], $\langle \ddot{r}_\square, \ddot{r}_\boxtimes, \ddot{\delta} \rangle \cong D_8$. Moreover, if m is even, then

$$|\ddot{r}_\square \ddot{\delta}| = 4, \quad |\ddot{\delta}| = 2, \quad (\ddot{r}_\square \ddot{\delta})^{\ddot{\delta}} = (\ddot{r}_\square \ddot{\delta})^{-1}, \quad (\ddot{r}_\square \ddot{\delta})^2 = \ddot{r}_\square \ddot{r}_\boxtimes$$

and if m is odd, then

$$|\ddot{\delta}| = 4, \quad |\ddot{r}_\square \ddot{\delta}| = 2, \quad \ddot{\delta}^{\ddot{r}_\square \ddot{\delta}} = \ddot{\delta}^{-1}, \quad \ddot{\delta}^2 = \ddot{r}_\square \ddot{r}_\boxtimes.$$

In both cases, $Z(\langle \ddot{r}_\square, \ddot{r}_\boxtimes, \ddot{\delta} \rangle) = \langle \ddot{r}_\square \ddot{r}_\boxtimes \rangle$.

Since φ arises from an automorphism of $\mathrm{GL}_{2m}(q)$, $\mathrm{Out}(T)$ splits as the semidirect product $\langle \ddot{r}_\square, \ddot{r}_\boxtimes, \ddot{\delta} \rangle : \langle \ddot{\varphi} \rangle$. If $\ddot{\varphi} \in Z(\mathrm{Out}(T))$, then evidently $\mathrm{Out}(T) \cong D_8 \times C_f$. However, $\ddot{\varphi}$ need

not be central in $\mathrm{Out}(T)$. In particular, by [43, Proposition 2.7.3(iii)],

$$[\ddot{r}_{\square}, \ddot{\varphi}] = [\ddot{r}_{\boxtimes}, \ddot{\varphi}] = 1$$

but

$$\ddot{\varphi} \notin Z(\mathrm{Out}(T)) \iff [\ddot{\delta}, \ddot{\varphi}] \neq 1 \iff m \text{ is odd and } p \equiv 3 \pmod 4.$$

If $\ddot{\varphi} \notin Z(\mathrm{Out}(T))$, then $\ddot{\delta}$ has order 4 and $\ddot{\delta}^{\ddot{\varphi}} = \ddot{\delta}^{-1}$, which implies that $\mathrm{Out}(T) = \langle \ddot{r}_{\square}, \ddot{r}_{\boxtimes}, \ddot{\delta} \rangle \times \langle \ddot{r}_{\square}\ddot{\varphi} \rangle$. In this case, $p \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$, so f is even and $\ddot{r}_{\square}\ddot{\varphi}$ has order f; this shows that $\mathrm{Out}(T) \cong D_8 \times C_f$ in this case also.

The following lemma provides further information when q is odd and $D(Q) = \square$. It is useful to record the following set of conditions

$$m \text{ is odd } \textit{ and } \ p \equiv 3 \pmod 4 \ \textit{ and } \ i \text{ is odd } \textit{ and } \ f \text{ is even.} \tag{5.3}$$

Lemma 5.1.3. *Let $T = \mathrm{P}\Omega^+_{2m}(q)$. Assume that q is odd and $D(Q) = \square$. For $0 \leqslant i < f$, the following hold*

(i) $\ddot{\delta}\ddot{\varphi}^i$ *and* $\ddot{r}_{\square}\ddot{r}_{\boxtimes}\ddot{\delta}\ddot{\varphi}^i$ *are* $\mathrm{Out}(T)$*-conjugate*

(ii) $\ddot{\delta}\ddot{r}_{\square}\ddot{\varphi}^i$ *and* $\ddot{\delta}\ddot{r}_{\boxtimes}\ddot{\varphi}^i$ *are* $\mathrm{Out}(T)$*-conjugate*

(iii) $\ddot{\varphi}^i$ *and* $\ddot{r}_{\square}\ddot{r}_{\boxtimes}\ddot{\varphi}^i$ *are* $\mathrm{Out}(T)$*-conjugate if* (5.3) *holds*

(iv) $\ddot{r}_{\square}\ddot{\varphi}^i$ *and* $\ddot{r}_{\boxtimes}\ddot{\varphi}^i$ *are* $\mathrm{Out}(T)$*-conjugate if* (5.3) *does not hold.*

Proof. Write $A = \langle \ddot{r}_{\square}, \ddot{r}_{\boxtimes}, \ddot{\delta} \rangle$. From the description of $\mathrm{Out}(T)$ in Remark 5.1.2, the conjugacy classes of A are

$$\{\ddot{1}\}, \ \{\ddot{r}_{\square}\ddot{r}_{\boxtimes}\}, \ \{\ddot{r}_{\square}, \ddot{r}_{\boxtimes}\}, \ \{\ddot{\delta}, \ddot{r}_{\square}\ddot{r}_{\boxtimes}\ddot{\delta}\}, \ \{\ddot{\delta}\ddot{r}_{\square}, \ddot{\delta}\ddot{r}_{\boxtimes}\}.$$

If the condition (5.3) is not satisfied, then $\ddot{\varphi} \in Z(\mathrm{Out}(T))$ and (i), (ii) and (iv) follow. Now assume that condition (5.3) is satisfied. In this case $\ddot{r}_{\square}\ddot{\varphi} \in Z(\mathrm{Out}(T))$. Writing

$$\begin{aligned}
\ddot{\delta}\ddot{\varphi}^i = \ddot{r}_{\boxtimes}\ddot{\delta}(\ddot{r}_{\square}\ddot{\varphi}^i) \quad &\text{and} \quad \ddot{r}_{\square}\ddot{r}_{\boxtimes}\ddot{\delta}\ddot{\varphi}^i = \ddot{r}_{\square}\ddot{\delta}(\ddot{r}_{\square}\ddot{\varphi}^i) \\
\ddot{\delta}\ddot{r}_{\square}\ddot{\varphi}^i = \ddot{\delta}(\ddot{r}_{\square}\ddot{\varphi}^i) \quad &\text{and} \quad \ddot{\delta}\ddot{r}_{\boxtimes}\ddot{\varphi}^i = \ddot{r}_{\square}\ddot{r}_{\boxtimes}\ddot{\delta}(\ddot{r}_{\square}\ddot{\varphi}^i) \\
\ddot{\varphi}^i = \ddot{r}_{\square}(\ddot{r}_{\square}\ddot{\varphi}^i) \quad &\text{and} \quad \ddot{r}_{\square}\ddot{r}_{\boxtimes}\ddot{\varphi}^i = \ddot{r}_{\boxtimes}(\ddot{r}_{\square}\ddot{\varphi}^i)
\end{aligned}$$

reveals that (i), (ii) and (iii) hold. □

Recall the definition of $\mathrm{PDO}^+_{2m}(q)$ from Section 2.2.6 (see (2.11) and (2.12)). The following is [43, Proposition 2.7.4], but it can be quickly deduced from (2.20).

Lemma 5.1.4. *Let $T = \mathrm{P}\Omega^+_{2m}(q)$. Then*

$$\mathrm{Inndiag}(T) = \mathrm{PDO}^+_{2m}(q) = \begin{cases} T & \text{if } q \text{ is even} \\ \langle T, \delta \rangle & \text{if } q \text{ is odd and } D(Q) = \boxtimes \\ \langle T, r_{\square}r_{\boxtimes}, \delta \rangle & \text{if } q \text{ is odd and } D(Q) = \square. \end{cases}$$

5.1.2 Minus-type

Now let $T = P\Omega^-_{2m}(q)$ and assume that $m \geqslant 4$. The automorphism group of T was recorded in Lemma 2.6.21. To describe $\mathrm{Out}(T)$ in this case we deviate from [43] and work more in the spirit of [31]. This is because we want to work with a copy of $P\Omega^-_{2m}(q)$ that arises naturally from the perspective of algebraic groups. However, we do want to be able to concretely work with the action of $P\Omega^-_{2m}(q)$ on the natural module $\mathbb{F}_q^{2m}$, so we will recover some of the key results from [43, Section 2.8] in our context. In this section, the isomorphism Ψ from Lemma 2.6.17 will be the key tool for relating our two viewpoints.

Recall the standard Frobenius endomorphism $\varphi = \varphi_{\mathcal{B}^+} : (a_{ij}) \mapsto (a_{ij}^p)$ and the reflection $r \in \mathrm{PO}^+_{2m}(q)$ from Definitions 2.6.9 and 2.6.15. Define $\psi = \Psi \circ \varphi \circ \Psi^{-1}$ (see (2.21)) and note that $\psi^f = r$ (see Lemma 2.6.23). We use $r_\square$ and $r_\boxtimes$ as in plus-type, but we often, instead, work with the reflection r, which we may assume is contained in $\{r_\square, r_\boxtimes\}$.

If q is odd, then we define a further element.

Definition 5.1.5. Let q be odd. With respect to the basis $\mathcal{B}^+$, define $\Delta \in \mathrm{GO}^+_{2m}(q^2)$ as $\beta I_{m-1} \oplus I_{m-1} \perp [\beta_2, \beta_2^q]$, centralising $\langle e_1, \ldots, e_{m-1}\rangle \oplus \langle f_1, \ldots, f_{m-1}\rangle \perp \langle e_m, f_m\rangle$, where $\beta_2 \in \mathbb{F}_{q^2}^\times$ has order $(q^2-1)_2$. Let $\hat{\delta}^- = \Psi(\Delta)$ and let $\delta^- \in \mathrm{PGO}^-_{2m}(q^2)$ be the image of $\hat{\delta}^-$.

Remark 5.1.6. We comment on Definition 5.1.5.

(i) If the sign $-$ is understood, then we omit reference to it.

(ii) That $\Delta \in \mathrm{GO}^+_{2m}(q^2)$ is fixed by the automorphism $r\varphi^f$ implies that $\hat{\delta} \in \mathrm{GO}^-_{2m}(q)$.

(iii) Evidently, $\det(\Delta) = \beta^m$ and Ψ, being simply a change of basis, keeps the determinant invariant, so $\det(\hat{\delta}) = \beta^m$.

(iv) It is also straightforward to verify that $\tau(\Delta) = \beta_2^{q+1} = \beta$, with respect to the standard plus-type form on $\mathbb{F}_{q^2}^{2m}$ (defined in terms of $\mathcal{B}^+$). From the definition of Ψ, this implies that $\tau(\hat{\delta}) = \beta$ with respect to the standard minus-type form on $\mathbb{F}_q^{2m}$ (defined in terms of $\mathcal{B}^-$).

Let us describe the innerdiagonal group.

Lemma 5.1.7. *Let $T = P\Omega^-_{2m}(q)$. Then*

$$\mathrm{Inndiag}(T) = \mathrm{PDO}^-_{2m}(q) = \begin{cases} T & \text{if } q \text{ is even} \\ \langle T, \delta\rangle & \text{if } q \text{ is odd.} \end{cases}$$

Proof. By (2.20), $\mathrm{Inndiag}(T) = \mathrm{PDO}^-_{2m}(q)$. If q is even, then $\mathrm{PDO}^-_{2m}(q) = T$ (see (2.12)). Now assume that q is odd. Note that $\tau(\hat{\delta}) = \beta$, which is not a square in $\mathbb{F}_q^\times$. Therefore, by Lemma 2.2.6, $\delta \notin \mathrm{PO}^-_{2m}(q)$. Since $|\mathrm{PGO}^-_{2m}(q) : \mathrm{PO}^-_{2m}(q)| = 2$, we deduce that $\mathrm{PGO}^-_{2m}(q) = \langle \mathrm{PO}^-_{2m}(q), \delta\rangle$. Now $\mathrm{PDO}^-_{2m}(q) \cap \mathrm{PO}^-_{2m}(q) = \mathrm{PSO}^-_{2m}(q)$ and $\delta^- \in \mathrm{PDO}^-_{2m}(q)$ since $\det(\hat{\delta}) = \beta^m = \tau(\hat{\delta})^m$, so $\mathrm{PDO}^-_{2m}(q) = \langle \mathrm{PSO}^-_{2m}(q), \delta\rangle$. Since $\mathrm{Inndiag}(T)/T$ is cyclic (see [31, Theorem 2.5.12]) in fact, $\mathrm{PDO}^-_{2m}(q) = \langle T, \delta\rangle$, which completes the proof. □

Remark 5.1.8. In light of Lemma 5.1.7, let us compare our notation for $\mathrm{PGO}^-_{2m}(q)$ with the notation in [43, Section 2.8]. Their symbol $\ddot{r}_\square$ is also our $\ddot{r}_\square$, but their $\ddot{\delta}$ is our $\ddot{r}^m\ddot{\delta}$. Therefore, we may conclude from [43, Section 2.8] that, in our notation, if $D(Q) = \boxtimes$ then $|\ddot{\delta}| = 2$, and if $D(Q) = \square$ then $|\ddot{\delta}| = 4$ with $\ddot{\delta}^2 = \ddot{r}_\square\ddot{r}_\boxtimes$.

Let us describe $\mathrm{Out}(T)$.

Lemma 5.1.9. *Let $T = \mathrm{P}\Omega^-_{2m}(q)$. Then*

$$\mathrm{Out}(T) = \begin{cases} \langle\ddot{\psi}\rangle \cong C_{2f} & \text{if } q \text{ is even} \\ \langle\ddot{\delta}\rangle \times \langle\ddot{\psi}\rangle \cong C_2 \times C_{2f} & \text{if } q \text{ is odd and } D(Q) = \boxtimes \\ \langle\ddot{\delta}\rangle{:}\langle\ddot{\psi}\rangle \cong C_4{:}C_{2f} & \text{if } q \text{ is odd and } D(Q) = \square \end{cases}$$

Proof. By Lemma 2.6.21, $\mathrm{Aut}(T) = \mathrm{Inndiag}(T){:}\langle\psi\rangle$. From the description of $\mathrm{Inndiag}(T)$ in Lemma 5.1.7 we see that $\mathrm{Out}(T) = \langle\ddot{\psi}\rangle$ when q is even and $\mathrm{Out}(T) = \langle\ddot{\delta}\rangle{:}\langle\ddot{\psi}\rangle$ when q is odd. By Lemma 2.6.23, $|\ddot{\psi}| = |\psi| = 2f$, so we have proved the claim when q is even.

Now assume that q is odd. If $D(Q) = \boxtimes$, then, by Remark 5.1.8, $|\ddot{\delta}| = 2$, so $\ddot{\psi}$ centralises $\ddot{\delta}$. It remains to assume that $D(Q) = \square$. In this case, f is necessarily odd (see (2.9) in Remark 2.2.2), so $\langle\ddot{\psi}\rangle = \langle\ddot{r}\ddot{\psi}^2\rangle$, since $\psi^f = r$. By Remark 5.1.8, $|\ddot{\delta}| = 4$, so $\ddot{\psi}^2$, having odd order, centralises $\ddot{\delta}$. Since $r_v^\delta = r_{v\delta}$, for any $v \in V$, we know that $\ddot{r}_\square^{\ddot{\delta}} = \ddot{r}_\boxtimes$. Therefore,

$$\ddot{\delta}^{\ddot{\psi}} = \ddot{\delta}^{\ddot{r}} = \ddot{\delta}\ddot{r}_\square\ddot{r}_\boxtimes = \ddot{\delta}^{-1}.$$

This completes the proof. □

Remark 5.1.10. Let $T = \mathrm{P}\Omega^-_{2m}(q)$. Assume that q is odd and $D(Q) = \square$. From the proof of Lemma 5.1.9, $|\ddot{\delta}| = 4$, $|\ddot{r}_\square| = 2$ and $\ddot{\delta}^{\ddot{r}_\square} = \ddot{\delta}^{-1}$, so $\langle\ddot{\delta}, \ddot{r}\rangle \cong D_8$. Moreover, $[\ddot{\delta}, \psi^2] = 1$, so

$$\mathrm{Out}(T) \cong \langle\ddot{\delta}, \ddot{r}\rangle \times \langle\ddot{\psi}^2\rangle \cong D_8 \times C_f.$$

Let us record further information in the case where q is odd and $D(Q) = \square$.

Lemma 5.1.11. *Let $T = \mathrm{P}\Omega^-_{2m}(q)$. Assume that q is odd and $D(Q) = \square$. For $0 \leqslant i < 2f$, the following hold*

(i) *$\ddot{\delta}\ddot{\psi}^i$ and $\ddot{\delta}^{-1}\ddot{\psi}^i$ are $\mathrm{Out}(T)$-conjugate*

(ii) *if i is odd, then $\ddot{\psi}^i$ and $\ddot{r}_\square\ddot{r}_\boxtimes\ddot{\psi}^i$ are $\mathrm{Out}(T)$-conjugate.*

Proof. From Remark 5.1.10, $\ddot{\delta}^{\ddot{r}} = \ddot{\delta}^{-1}$ and $[\ddot{r}, \ddot{\psi}] = 1$, so $(\ddot{\delta}\ddot{\psi}^i)^{\ddot{r}} = \ddot{\delta}^{-1}\ddot{\psi}^i$. Moreover, if i is odd, then $(\ddot{\psi}^i)^{\ddot{\delta}} = \ddot{\delta}^{-1}\ddot{\delta}^{\ddot{\psi}^i}\ddot{\psi}^i = \ddot{\delta}^{-1}\ddot{\delta}^{-1}\ddot{\psi}^i = \ddot{r}_\square\ddot{r}_\boxtimes\ddot{\psi}^i$. □

5.1.3 Cases to consider

For this section, define

$$d = \begin{cases} 1 & \text{if } \varepsilon = + \\ 2 & \text{if } \varepsilon = - \end{cases} \tag{5.4}$$

Table 5.1: The relevant automorphisms θ in type D_m

	I(a)	I(b)	II(i)	II(ii)	II(iii)	II(iv)	II(v)	
ε			$+$	$+$	$+$	$-$	$-$	
	1	ιr	φ^i	$r\varphi^i$	$\iota r\varphi^i$	ψ^i	$\iota\psi^i$	(1)
θ	$\iota\delta$	$\iota\delta r$	$\iota\delta\varphi^i$	$\iota\delta r\varphi^i$	$\iota\delta r\varphi^i$	$\iota\delta\psi^i$	$\iota\delta\psi^i$	(2)
	$r_\square r_\boxtimes$		$r_\square r_\boxtimes\varphi^i$	$r_\square r_\boxtimes r\varphi^i$		$r_\square r_\boxtimes\psi^i$		(3)
df/i			any	even	odd	odd	even	
notes			$\star$	†				

[i is a proper divisor of df, the notes are given in Remark 5.1.13]

We can now enumerate the automorphisms that it suffices to consider in order to prove Theorems 5A and 5B.

Proposition 5.1.12. *Let $T = \mathrm{P}\Omega^\varepsilon_{2m}(q) \in \mathcal{T}$. To prove that $u(G) \geqslant k$ for all $G \in \mathcal{A}$ with socle T, it suffices to show that $u(\langle T, \theta\rangle) \geqslant k$ for all of the following*

(i) *θ in Row (1) of Table 5.1*

(ii) *θ in Row (2) of Table 5.1, if q is odd*

(iii) *θ in Row (3) of Table 5.1, if q is odd and $D(Q) = \square$.*

Before proving Proposition 5.1.12 we must comment on Table 5.1.

Remark 5.1.13. Let us explain how to read Table 5.1.

(i) The symbol ι should be interpreted as 1, unless q is odd and $D(Q) = \square$, in which it suffices to consider either the automorphism θ obtained by letting ι be 1 or by letting ι be $r_\square r_\boxtimes$. We will exploit this flexibility in our later arguments.

(ii) In Case I, the description is uniform for both signs ε, but we have noted which of Cases I(a) and I(b) the automorphism θ arises in.

(iii) In Case II, the possibilities for θ depend on whether ε is $+$ or $-$. Moreover, we have used the conditions on ε and i to define five subcases. Observe that Case II(a) is the union of Cases II(i), II(ii) and II(iv), whereas Case II(b) is the union of Cases II(iii) and II(v). We will often refer to these subcases.

(iv) We now comment on the notes.

- $\star$ We need only consider one of φ^i and $r_\square r_\boxtimes\varphi^i$ in the very special case when the condition (5.3) holds.
- † We need only consider one of $r\varphi^i$ and $r_\square r_\boxtimes r\varphi^i$ *unless* the condition (5.3) holds.

Proof of Proposition 5.1.12. Let $g \in \mathrm{Aut}(T)$ and write $G = \langle T, g\rangle$. Begin by assuming that $\varepsilon = +$. By inspecting the structure of $\mathrm{Out}(T)$ given above, it is manifest that we may write $g = th\varphi^i$ where $t \in T$ and h is a product of diagonal and graph automorphisms. Since $\langle T, th\varphi^i\rangle = \langle T, h\varphi^i\rangle$, we may assume, in fact, that $g = h\varphi^i$. Assume for now that $i > 0$. Since $\langle Th, T\varphi\rangle = \langle Th\rangle{:}\langle T\varphi\rangle$, by Lemma 4.1.2, there exist $j, k \in \mathbb{N}$ with k dividing f such that $\langle Th\varphi^i\rangle = \langle Th^j\varphi^k\rangle$ and, consequently, $\langle T, h\varphi^i\rangle = \langle T, h^j\varphi^k\rangle$. Therefore, we may assume that i divides f.

To summarise, for all $G \in \mathcal{A}$ with socle T, we may, and will, write $G = \langle T, g\rangle$ for an automorphism $g = h\varphi^i$ where h is a product of diagonal and graph automorphisms and where either $i = 0$ or i divides f.

Let us now fix an automorphism θ from the statement of the proposition, such that $\ddot{g} = \ddot{h}\ddot{\varphi}^i$ is $\mathrm{Out}(T)$-conjugate to $\ddot{\theta}$. We can evidently do this if q is even or q is odd with $D(Q) = \boxtimes$. Moreover, if q is odd and $D(Q) = \square$, then Lemma 5.1.3 implies that we can still do this. Now, by Lemma 4.1.1, $\langle T, g\rangle$ and $\langle T, \theta\rangle$ are $\mathrm{Aut}(T)$-conjugate. In particular, $u(\langle T, g\rangle) = u(\langle T, \theta\rangle)$. This proves the result when $\varepsilon = +$.

Now assume that $\varepsilon = -$. As in plus-type, we can assume that $g = h\psi^i$ where h is a diagonal automorphism and where either $i = 0$ or i divides $2f$. Noting that $\psi^f = r$, it follows that $\ddot{g}$ is $\mathrm{Out}(T)$-conjugate to an automorphism $\ddot{\theta}$ in the statement, where we apply Lemma 5.1.11 when q is odd and $D(Q) = \square$. Therefore, $\langle T, g\rangle$ and $\langle T, \theta\rangle$ are $\mathrm{Aut}(T)$-conjugate and the result follows as in the previous case. □

Remark 5.1.14. We note in passing that our approach of considering each simple group T and each automorphism $\theta \in \mathrm{Aut}(T)$ (with the reductions justified by Proposition 5.1.12) allows us to avoid mentioning the classical groups that Bray, Holt and Roney-Dougal [6] highlight are not well-defined (such as the one often referred to as $\mathrm{P\Sigma O}^+_{2m}(q)$).

Remark 5.1.15. Let us comment on the almost simple groups with socle $T = \mathrm{P\Omega}^+_8(q)$, which are excluded from our main theorems. The group $\mathrm{P\Omega}^+_8(q)$ has a *triality* automorphism τ such that $C_G(\tau) \cong G_2(q)$ (see [23, pp.200–202]). By [42, Section 1.4],

$$\mathrm{Out}(T) = \begin{cases} \langle \ddot{r}_\square, \ddot{\tau}\rangle \times \langle \ddot{\varphi}\rangle \cong S_3 \times C_f & \text{if } q \text{ is even} \\ \langle \ddot{r}_\square, \ddot{\tau}, \ddot{\delta}\rangle \times \langle \ddot{\varphi}\rangle \cong S_4 \times C_f & \text{if } q \text{ is odd.} \end{cases} \tag{5.5}$$

In particular, $\ddot{\tau}^{\mathrm{Out}(T)}$ is the unique conjugacy class of elements in $\mathrm{Out}(T) \setminus (\mathrm{P\Gamma O}^+_8(q)/T)$. Therefore, to show that $u(G) \geqslant k$ for all groups $G = \langle T, \theta\rangle$ with $\theta \in \mathrm{Aut}(T)$, it suffices to assume that θ appears in Proposition 5.1.12 or θ is $\tau\varphi^i$ for a divisor i of f. If θ appears in Proposition 5.1.12, then the general approach is the same as for the plus-type orthogonal groups that are handled in this paper, but we will need to work with different elements. In Remark 5.3.26, we outline how we will approach the case $\theta = \tau\varphi^i$ in future work.

5.2 Case I

Having established the cases to consider, we now turn to the proofs of Theorems 5A and 5B. In this section, we begin with Case I. Accordingly, write $G = \langle T, \theta \rangle$ where $T = P\Omega^{\varepsilon}_{2m}(q)$ for $m \geqslant 4$ and $\varepsilon \in \{+, -\}$ and where $\theta \in PGO^{\varepsilon}_{2m}(q)$. Recall that we assume that $T \neq P\Omega^{+}_{8}(q)$.

We make the case distinction

(a) $G \leqslant PDO^{\varepsilon}_{2m}(q)$

(b) $G \not\leqslant PDO^{\varepsilon}_{2m}(q)$.

We will continue to refer to the types of elements introduced in Section 2.3.6, and in Section 5.2.1 we define some further elements that we will use in this chapter. Then we consider Cases I(a) and I(b) in Sections 5.2.2 and 5.2.3, with the aim of proving Theorems 5A and 5B in Case I.

5.2.1 Further element definitions

To choose the elements in Cases I(b) and II(b) we need to introduce more elements.

Recall that the standard bases $\mathcal{B}^+$ and $\mathcal{B}^-$ were introduced in (2.5) and (2.6). If q is odd, $\beta \in \mathbb{F}_q^\times$ has order $(q-1)_2$, so $\beta \notin (\mathbb{F}_q^\times)^2$. If $\varepsilon = -$, then we will make use of the isomorphism $\Psi\colon \langle X_{r\varphi^f}, r \rangle \to PGO^{-}_{2m}(q)$ (see Lemma 2.6.17).

Definition 5.2.1. With respect to the basis $\mathcal{B}^\varepsilon$ for $\mathbb{F}_q^2$, define

$$r^\varepsilon = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in O^{\varepsilon}_2(q)$$

and if q is odd, then also

$$^{\Delta}r^{+}_{q} = \begin{pmatrix} 0 & \beta \\ 1 & 0 \end{pmatrix} \in GO^{+}_2(q)$$

and

$$^{\Delta}r^{-}_{q} = \Psi(R) \in GO^{-}_2(q) \quad \text{where} \quad R = \begin{pmatrix} 0 & \beta_2 \\ \beta_2^q & 0 \end{pmatrix} \in GO^{+}_2(q^2)$$

and where $\beta_2 \in \mathbb{F}_{q^2}^\times$ has order $(q^2-1)_2$.

Let us establish some properties of the elements introduced in Definition 5.2.1.

Lemma 5.2.2. *Let q be even and let F be a finite extension of $\mathbb{F}_q$. Then r^ε is a reflection that stabilises a unique (nonsingular) 1-space of F^2.*

Proof. Evidently r^ε is the reflection that stabilises the nonsingular 1-space $\langle e_1 + f_1 \rangle$ if $\varepsilon = +$ and $\langle u_1 + v_1 \rangle$ if $\varepsilon = -$. Moreover, it is easy to check that this 1-space is the unique subspace stabilised by r^ε. □

Lemma 5.2.3. *Let q be odd and let F be a finite extension of $\mathbb{F}_q$. Then*

(i) *r^+ is a reflection in a vector of norm -2*

(ii) *r^- is a reflection in a vector of norm $-2\lambda^2$ for some $\lambda \in \mathbb{F}_q^\times$*

(iii) *r^ε stabilises exactly two (orthogonal nondegenerate) 1-spaces of F^2.*

(iv) *${}^\Delta r^\varepsilon$ acts irreducibly on F^2 if $|F : \mathbb{F}_q|$ is odd*

(v) *${}^\Delta r^\varepsilon$ stabilises exactly two (orthogonal nondegenerate) 1-spaces of F^2 if $|F : \mathbb{F}_q|$ is even*

(vi) *$\tau({}^\Delta r^\varepsilon) = \beta$ and $\det({}^\Delta r^\varepsilon) = -\beta$.*

Proof. Observe that $r^+ = r_{e_1 - f_1}$ and $(e_1 - f_1, e_1 - f_1) = -2$. Similarly, $r^- = r_{u_1 - v_1}$ and

$$(u_1 - v_1, u_1 - v_1) = 2 - 2(\xi^2 + \xi^{-2}) + 2 = -2(\xi - \xi^{-1})^2$$

(see the definition of $\mathcal{B}^-$ in (2.6)). This proves (i) and (ii).

For (iii), the characteristic polynomial of r^ε is $X^2 - 1$, so r^ε has a 1-dimensional 1- and -1-eigenspace and these two 1-spaces are exactly the proper nonzero subspaces stabilised by r^ε. Smilarly, (iv) and (v) hold since the characteristic polynomial of ${}^\Delta r^\varepsilon$ is $X^2 - \beta$.

Finally consider (vi). If $\varepsilon = +$, then this is a straightforward calculation. If $\varepsilon = -$, then we easily see that $\det([\beta_2, \beta_2^q]) = -\beta_2^{q+1} = -\beta$ and Ψ is induced by conjugation, so $\det({}^\Delta r^\varepsilon) = -\beta$. Similarly, $\tau([\beta_2, \beta_2^q]) = \beta_2^{q+1} = \beta$, with respect to the standard plus-type form on $\mathbb{F}_{q^2}^{2m}$ (defined in terms of $\mathcal{B}^+$) and the definition of Ψ implies that $\tau(\hat{\delta}) = \beta$ with respect to the standard minus-type form on $\mathbb{F}_q^{2m}$ (defined in terms of $\mathcal{B}^-$). □

Remark 5.2.4. Let us comment on reflections.

(i) The element $r \in \mathrm{GO}_{2m}(\overline{\mathbb{F}}_p)$ from Definition 2.6.15 is simply $I_{2m-2} \perp r^+$, centralising $\langle e_1, \ldots, f_{m-1}\rangle \perp \langle e_m, f_m\rangle$. Additionally, $\Psi(r) = I_{2m-2} \perp r^-$, centralising $\langle e_1, \ldots, f_{m-1}\rangle \perp \langle u_m, v_m\rangle$. Thus, we often identify r and r^ε as elements of $\mathrm{O}_{2m}^\varepsilon(q)$.

(ii) Assume q is odd. By Lemma 5.2.3, the norm of r^ε is square if and only if $-2 \in (\mathbb{F}_q^\times)^2$. This latter condition holds if and only if

$$f \text{ is even or } p \equiv 1 \text{ or } 3 \pmod 8. \tag{5.6}$$

Therefore, $\ddot{r}^\varepsilon$ is $\ddot{r}_\square$ if (5.6) holds and $\ddot{r}^\varepsilon$ is $\ddot{r}_\boxtimes$ otherwise.

(iii) If q is odd, then ${}^\Delta r^+ = \delta^+ r$ and ${}^\Delta r^- = \delta^- r$ (see Definitions 4.1.3 and 5.1.5).

5.2.2 Case I(a)

Let $m \geqslant 4$ and $\varepsilon \in \{+,-\}$, and assume that $(m,\varepsilon) \neq (4,+)$. In this section, we focus on the groups $\mathrm{P}\Omega^{\varepsilon}_{2m}(q) \leqslant G \leqslant \mathrm{PDO}^{\varepsilon}_{2m}(q)$ and prove two results, which establish Theorems 5A and 5B in Case I(a). Our approach is similar to that of Section 4.2.

Proposition 5.2.5. *Let $G = \langle \mathrm{P}\Omega^{\varepsilon}_{2m}(q), \theta\rangle \in \mathcal{A}$ where $\theta \in \mathrm{PDO}^{\varepsilon}_{2m}(q)$. Then*

(i) $u(G) \geqslant 2$

(ii) $u(G) \to \infty$ *as* $q \to \infty$.

Proof. Consider part (i). In the proofs of [10, Propositions 5.13–5.18], it is shown that for all prime order elements $x \in T$, $P(x,s) < \frac{1}{2}$, for a suitable semisimple element $s \in T$. In each case, by Lemmas 2.3.18, 2.3.18 and 2.3.20, there exists $g \in T\theta$ such that a suitable power of g is s. As in the proof of Proposition 4.2.1, we can verify that for all $x \in G$, we also have $P(x,g) < \frac{1}{2}$ and consequently $u(G) \geqslant 2$. For part (ii), we proceed in the same manner, except we use the element s from [33, Proposition 4.1], where it is shown that $P(x,s) \to 0$ as $q \to \infty$. This gives the desired result.

For an example, let $\varepsilon = +$, let $m \geqslant 7$ be odd, let q be odd and let $\theta \in \{\delta, r_{\square} r_{\boxtimes} \delta\}$. Let V be the natural module for T. By Lemma 2.3.20, there exists $x = x_1 \perp x_2 \in \mathrm{DO}^{+}_{2m}(q)$ centralising $V_1 \perp V_2$, where V_1 and V_2 are nondegenerate subspaces of dimensions $m-1$ and $m+1$, x_1 has order $(q-1)(q^{(m-1)/2}+1)$ acting irreducibly on V_1, x_2 has order $(q-1)(q^{(m+1)/2}+1)$ acting irreducibly on V_2 and $\tau(x_1) = \tau(x_2) = \alpha$ (where $\mathbb{F}_q^{\times} = \langle \alpha \rangle$). Since $\tau(x) = \alpha \notin (\mathbb{F}_q^{\times})^2$, by Lemma 2.2.6, $g = xZ(\mathrm{DO}^{+}_{2m}(q)) \in \mathrm{PDO}^{+}_{2m}(q) \setminus \mathrm{PSO}^{+}_{2m}(q)$. Consequently, $g \in T\iota\delta$ for some choice of $\iota \in \{1, r_{\square} r_{\boxtimes}\}$.

The order of g is divisible a primitive prime divisor ℓ of $q^{m+1}-1$, which by Lemma 2.3.15 we may assume satisfies $\ell > 2m+3$. Therefore, by Theorem 2.5.5, all of the subgroups in $\mathcal{M}(G,g)$ are reducible, subfield or field extension subgroups. Since $m+1 > m$ and $(m+1,m) = 1$, the prime ℓ does not divide the order of any subfield or field extension subgroup of G. Therefore, we conclude that $\mathcal{M}(G,g)$ contains only reducible subgroups. Moreover, Lemma 2.3.3 implies that the only proper nonzero subspaces of V that are stabilised by g are V_1 and V_2. Consequently, $\mathcal{M}(G,g) = \{H\}$, where H has type $\mathrm{O}^{-}_{m-1}(q) \times \mathrm{O}^{-}_{m+1}(q)$.

Now Theorem 3.1.1 implies that for each prime order element $x \in G$ we have

$$P(x,g) \leqslant \mathrm{fpr}(x, G//H) < \frac{1}{q^{(m+1)/2}} + \frac{2}{q^{m-2}} + \frac{2}{q^{m-1}} < \frac{1}{2},$$

so by Lemma 2.1.1 we conclude that $u(G) \geqslant 2$. □

We will now prove an asymptotic statement, to the end of ultimately proving Theorem 5B.

Proposition 5.2.6. *Let (G_i) be a sequence in $\mathcal{A}$ and write $T_i = \mathrm{soc}(G_i) = \mathrm{P}\Omega^{\varepsilon_i}_{2m_i}(q_i)$. Assume that $G_i \leqslant \mathrm{PDO}^{\varepsilon_i}_{2m_i}(q_i)$. Then $u(G_i) \to \infty$ if $m_i \to \infty$.*

Proof. Fix $G_i = G = \langle T, \theta \rangle$ with $T = \mathrm{P}\Omega^{\varepsilon}_{2m}(q)$. The condition $G \leqslant \mathrm{PDO}^{\varepsilon}_{2m}(q)$ implies that we are in Case I(a). By Proposition 5.1.12, we may assume that θ appears in Table 5.1. Assume that $m \geqslant 40$ and fix a positive integer $m/2 < d < 3m/4$ and for which $m - d$ is odd and $(d, m-d) = 1$. Let $y \in \mathrm{PDO}^{\varepsilon}_{2m}(q)$ have type ${}^{a}(2d)^{-} \perp {}^{b}(2m-2d)^{-\varepsilon}$.

We claim that $y \in T\theta$. If $\theta = 1$, then y has type $(2d)^{-} \perp (2m-2d)^{-\varepsilon}$, so Lemma 2.3.30 implies that $y \in T$. If $\theta = r_{\square} r_{\boxtimes}$, then y has type $(2d)^{-} \perp {}^{\Sigma}(2m-2d)^{-\varepsilon}$, so, in light of the definition of elements of type ${}^{\Sigma}(2k)^{\pm}$ in Definition 2.3.34, $y \in T r_{\square} r_{\boxtimes}$. Finally, assume that $\theta = \iota\delta$. In this case, y has type ${}^{\Delta}(2d)^{-} \perp {}^{\Delta}(2m-2d)^{-\varepsilon}$. Recalling Definition 2.3.32, we see that $\tau(y)$ is nonsquare in $\mathbb{F}_q^{\times}$. Therefore, $y \in \mathrm{PSO}^{\varepsilon}_{2m}(q)\delta$, which is exactly to say that $y \in T\iota\delta$ for a suitable choice of $\iota \in \{1, r_{\square} r_{\boxtimes}\}$. In summary, in every case, $y \in T\theta$.

Since $d > m/2$ a power z of y has type $(2d)^{-} \perp I_{2m-2d}$ and the order of z is a primitive prime divisor ℓ of $q^{2d} - 1$, where $2d > m$. By Lemma 2.3.15, since $2d > 20$, we may assume that $\ell \geqslant 4d + 1$. By Theorem 2.5.5, all of the subgroups in $\mathcal{M}(G, g)$ are reducible, subfield or field extension subgroups. Since $d > m$ and $(d, m) = 1$, the prime ℓ does not divide the order of any subfield or field extension subgroup of G. Thus, we may conclude, by Lemma 2.3.3, that $\mathcal{M}(G, y)$ consists of a subgroup of type $\mathrm{O}^{-}_{2d}(q) \times \mathrm{O}^{-\varepsilon}_{2m-2d}(q)$ and if $\varepsilon = -$ also two P_{m-d} parabolic subgroups. Now the bounds in Theorem 3.1.1 imply that for all prime order elements $x \in G$,

$$P(x, y) \leqslant \frac{11}{q^{m-2}} + \frac{2}{q^{m/2}} \to 0$$

as $m \to \infty$. Therefore, $u(G) \to \infty$ as $m \to \infty$. □

5.2.3 Case I(b)

We now turn to Case I(b). Therefore, by Proposition 5.1.12, we may assume that G is $\langle T, \theta \rangle$ where $T \in \mathcal{T}$ and $\theta \in \{r, \iota\delta r\}$ (recall that we write $\iota \in \{1, r_{\square} r_{\boxtimes}\}$).

Recall the reflection r^{ε} defined in Definition 2.6.15, and if q is odd, the diagonal element δ^{ε} defined in Definitions 4.1.3 and 5.1.5. Unless there is ambiguity, we write $r = r^{\varepsilon}$ and $\delta = \delta^{\varepsilon}$. If q is odd, fix the the element $\beta \in \mathbb{F}_q^{\times}$ of order $(q-1)_2$ and note that $\beta \notin (\mathbb{F}_q^{\times})^2$.

Remark 5.2.7. A computation in MAGMA proves that $u(G) \geqslant 2$ when G is one of

$$\mathrm{O}^{-}_{8}(2), \ \mathrm{PO}^{-}_{8}(3), \ \mathrm{O}^{\pm}_{10}(2), \ \mathrm{O}^{\pm}_{12}(2). \tag{5.7}$$

See Section 2.8 for further details of our computational methods. Therefore, for the remainder of this section, we may assume that G does not appear in (5.7).

We apply the probabilistic method, so we begin by selecting an element. Let

$$y = \begin{cases} A \perp r & \text{if } \theta = r \\ {}^{\Delta}(2m-2)^{-} \perp {}^{\Delta}r & \text{if } \theta = \iota\delta r \end{cases}$$

where A has type $(2m-2)^{-}$, unless $q = 2$, in which case A has order $2^{m-1} + 1$.

Table 5.2: Case I(b): Description of $\mathcal{M}(G, y)$

type of H	$m(H)$	conditions
$O_2^{-\varepsilon}(q) \times O_{2m-2}^-(q)$	1	
$O_{2m-1}(q)$	2	q odd, $\theta = r$
$Sp_{2m-2}(q)$	1	q even
$O_m(q^2)$	4	q odd, m odd, $\theta = \iota\delta r$

Proposition 5.2.8. *Let $G = \langle T, \theta \rangle$ for $T \in \mathcal{T}$ and $\theta \in \{r, \iota\delta r\}$. Assume that G is not one of the groups in* (5.7).

(i) *If $\theta = r$, then $y \in Tr$.*

(ii) *If q is odd and y has type ${}^{\Delta}(2m-2)^- \perp {}^{\Delta}r$, then $y \in T\iota\delta r$ for a suitable choice of $\iota \in \{1, r_\square r_\boxtimes\}$.*

Proof. Part (i) is immediate since $I_2 \perp (2m-2)^- \in T$, by Lemma 2.3.30, and $I_2 \perp A$ is clearly in T when $q = 2$. Now consider part (ii), so q is odd. Let $x_1 \in DO_{2m-2}^-(q)$ have type ${}^{\Delta}(2m-2)^-$, so $\tau(x_1) = \beta$ and $\det(x_1) = \beta^{m-1}$. Additionally, by Lemma 5.2.3(vi), $\tau({}^{\Delta}r^{-\varepsilon}) = \beta$ and $\det({}^{\Delta}r^{-\varepsilon}) = -\beta$. Therefore, the element $x = x_1 \perp {}^{\Delta}r^{-\varepsilon}$ has type ${}^{\Delta}(2m-2)^- \perp {}^{\Delta}r^{-\varepsilon}$ and satisfies $\tau(x) = \beta$ and $\det(x) = -\beta^m$. Let $y = xZ(DO_{2m}^{\varepsilon}(q))$. Now $\tau(r) = 1$ and $\det(r) = -1$. Moreover, we saw in Remarks 4.1.4 and 5.1.6 that $\tau(\delta) = \beta$ and $\det(\delta) = \beta^m$. Therefore, $\tau(\delta r) = \beta$ and $\det(\delta r) = -\beta^m$. Consequently, $y \in PSO_{2m}^{\varepsilon}(q)\delta r$, or in other words $y \in T\iota\delta r$ for a suitable choice of $\iota \in \{1, r_\square r_\boxtimes\}$. □

We now determine the maximal overgroups of y in G.

Theorem 5.2.9. *The maximal subgroups of G that contain y are listed in Table 5.2, where $m(H)$ is an upper bound on the multiplicity of the subgroups of type H in $\mathcal{M}(G, y)$.*

We will prove Theorem 5.2.9 in two parts, considering the reducible and irreducible maximal overgroups of y separately. We begin with reducible subgroups.

Proposition 5.2.10. *Theorem 5.2.9 is true for reducible subgroups.*

Proof. First assume that q is odd and $\theta = \iota\delta r$. Then y centralises an orthogonal decomposition $V = U \perp U^\perp$, where U is a nondegenerate 2-space. Moreover, y acts irreducibly on U and $U^\perp$ (see Lemma 5.2.3(iv)). Therefore, by Lemma 2.3.3, the only proper nonzero subspaces of V stabilised by y are U and $U^\perp$, so the only reducible maximal overgroup of y is one of type $O_2^{-\varepsilon}(q) \times O_{2m-2}^-(q)$.

Next assume that q is odd and $\theta = r$. In this case, the element y centralises a decomposition $V = U_1 \perp U_2 \perp (U_1 + U_2)^\perp$, where U_1 and U_2 are nondegenerate 1-spaces. Moreover, y acts irreducibly on $(U_1 + U_2)^\perp$, and acts as 1 and -1 on U_1 and U_2, respectively. Therefore, by Lemma 2.3.3, the only subspaces stabilised by y are direct sums of

U_1, U_2 and $(U_1+U_2)^\perp$. Consequently, the reducible maximal overgroups of y are two of type $\mathrm{O}_{2m-1}(q)$ (the stabilisers of U_1 and U_2) and one of type $\mathrm{O}_2^{-\varepsilon}(q)\times\mathrm{O}^-_{2m-2}(q)$ (the stabiliser U_1+U_2).

Finally assume that q is even and $\theta=r$. In this case, y centralises the decomposition $V=U\perp U^\perp$, where U is a nondegenerate 2-space. In this case, y acts irreducibly on $U^\perp$. However, y acts indecomposably on U and stabilises a unique 1-dimensional (nonsingular) subspace W of U (see Lemma 5.2.2). Since there are no $\mathbb{F}_q\langle y\rangle$-homomorphisms between $U^\perp$ and any $\mathbb{F}_q\langle y\rangle$-subquotient of U, Corollary 2.3.2 implies that the only proper nonzero subspaces of V stabilised by y are W, U, $U^\perp$ and $U^\perp+W$. From this we deduce that the reducible maximal overgroups of y are one of type $\mathrm{Sp}_{2m-2}(q)$ (the stabiliser of W) and one of type $\mathrm{O}_2^{-\varepsilon}(q)\times\mathrm{O}^-_{2m-2}(q)$ (the stabiliser of U). □

We now turn to the irreducible maximal overgroups of y.

Proposition 5.2.11. *Theorem 5.2.9 is true for irreducible subgroups.*

Proof. Let $H\in\mathcal{M}(G,y)$ be an irreducible subgroup. If $\theta=r$, then $y=y_1\perp r$ where $|y_1|$ is divisible by a primitive prime divisor of $q^{2m-2}-1$ (in fact, $|y_1|\in\mathrm{ppd}(q,2m-2)$ unless $q=2$). Now assume that q is odd and $\theta=\iota\delta r$. Recall that ${}^\Delta r$ has order $2(q-1)_2$ and $|y_1|=(q^{m-1}+1)_2(q-1)_2\ell$ for $\ell\in\mathrm{ppd}(q,2m-2)$. Therefore, $y^{(q^m+1)_2(q-1)_2}$ has order ℓ. Consequently, in both cases, we can fix a power z of y of order $\ell\in\mathrm{ppd}(q,2m-2)$.

Let us also note that if $\theta=r$, then a power of y^ℓ is r and $\nu(r)=1$.

We begin by considering the geometric maximal overgroups H of y in G. Since y has order divisible by $\ell\in\mathrm{ppd}(q,2m-2)$, the main theorem of [35] implies that the possibilities for H feature in [35, Examples 2.1–2.5]. Let us consider these possibilities in turn.

For orthogonal groups, Example 2.1 consists of subfield subgroups, none of which arise since for all proper divisors k of f, if $q_0=p^k$, then ℓ does not divide

$$|\mathrm{O}^\varepsilon_{2m}(q_0)|=2q_0^{m^2-m}(q_0^m-\varepsilon)\prod_{i=1}^{m-1}(q_0^{2i}-1).$$

All subgroups in Example 2.2 are reducible.

Example 2.3 features the imprimitive subgroups of type $\mathrm{O}_1(q)\wr S_n$. For these we insist that $\varepsilon=+$, $q=p\geqslant 3$ and $\ell=2m-1$; however, by Lemma 2.3.15, this implies that $m=4$, which is a case that we are not considering.

The only possible field extension subgroup H in Example 2.4 is $\mathrm{O}^\eta_m(q^2)$ where $\eta=\varepsilon$ if m is even and $\eta=\circ$ if m is odd. If $\theta=r$, then $\nu(y^\ell)=1$, so y is not contained in such a subgroup, by Lemma 2.5.7. Now assume that $\theta=\iota\delta r$. If m is even, then ℓ does not divide the order of H.

Therefore, if H is a field extension subgroup containing y, then q is odd, $\theta = \iota\delta r$, m is odd and H has type $\mathrm{O}_m(q^2)$. We will now prove that, in this case, y is contained in four G-conjugates of H. Note that y is a semisimple element with eigenvalue multiset $\Lambda \cup \Lambda^q \cup \{\mu, \mu^q\}$, where $\Lambda = \{\lambda^{q^{2i}} \mid 0 \leqslant i \leqslant m-1\}$ for a scalar $\lambda \in \overline{\mathbb{F}}_p^\times$ of order $(q^m+1)_2(q-1)_2\ell$ (where $\ell \in \mathrm{ppd}(q, 2m)$) and $\mu \in \overline{\mathbb{F}}_p^\times$ has order $2(q-1)_2$. Let $\pi\colon H \to G$ be the field extension embedding and write $H = B.\phi$, where ϕ is the field automorphism $\xi \mapsto \xi^q$. By Lemma 2.5.7, if $\pi(\tilde{y}) = y$, then $\tilde{y}$ has one of the following eigenvalue sets

$$S_1 = \Lambda \cup \{\mu\}, \quad S_2 = \Lambda \cup \{\mu^q\}, \quad S_3 = \Lambda^q \cup \{\mu^q\}, \quad S_4 = \Lambda^q \cup \{\mu\}.$$

Let $\tilde{y}_i$ have eigenvalue set S_i. By Lemma 2.4.3,

$$y^G \cap H = \bigcup_{i=1}^{4} \tilde{y}_i^B$$

Note that ϕ fuses $\tilde{y}_1^B$ with $\tilde{y}_3^B$ and fuses $\tilde{y}_2^B$ with $\tilde{y}_4^B$. Therefore, $y^G \cap H = \tilde{y}_1^H \cup \tilde{y}_2^H$. Since an element of type ${}^{\Delta}r^{\varepsilon}$ is self-centralising in $\mathrm{GO}_2^{\varepsilon}(q)$, Corollary 2.3.5 and Lemma 2.4.4 yield

$$|C_G(y)| = (q^{m-1}+1)(q-1)2 = 2|C_H(y)|,$$

Now Lemma 2.1.1 implies that the number of G-conjugates of H that contain y is

$$\frac{|y^G \cap H|}{|y^G|}\frac{|G|}{|H|} = \frac{2|C_G(y)|}{|C_H(y)|} = 4.$$

We now consider subgroups H contained in the $\mathcal{S}$ family. First assume that $\theta = r$. Since $\nu(y^\ell) = 1$, Theorem 2.5.14 implies that q is prime and H arises from the fully deleted permutation module ([14, Table 2.3] highlights that no exceptions from part (iii) arise). If $q > 2$, then, by Lemma 2.3.15, y has order 2ℓ where $\ell \geqslant 4m-3$ is prime. If $q = 2$, then y has order $2(2^{m-1}+1)$, which is divisible by a prime at least $2m-1$. In both cases, S_{2m+2} does not contain an element of order $|y|$, so we conclude that $H \notin \mathcal{S}$.

Now assume that $\theta = \iota\delta r$. Since $T \neq \mathrm{P}\Omega_8^-(3)$ (see Remark 5.2.7), by Theorem 2.3.14, $\ell > 4m-3$. Consequently, Theorem 2.5.5 forces us to have $T = \mathrm{P}\Omega_8^-(q)$ and H being an exception featured in (iii). Consulting [7, Table 8.53], we see that the only possibility for H is a subgroup with socle $\mathrm{PSL}_3(q)$ if $q \equiv 2 \pmod 3$ or $\mathrm{PSU}_3(q)$ if $q \equiv 1 \pmod 3$. However, we also see from this table that such subgroups are not maximal in $G = \langle T, \delta r\rangle$. Therefore, no $\mathcal{S}$ family subgroups occur in this case either. □

Next we handle a special case in a more concrete fashion.

Proposition 5.2.12. *Let $G = \langle T, r\rangle$ with $m \geqslant 5$. Let $x_1, x_2 \in G$ have prime order and satisfy $\nu(x_1) = 1$ and $\nu(x_2) \leqslant 2$. Then there exists $g \in G$ such that $\langle x_1, y^g\rangle = \langle x_2, y^g\rangle = G$.*

Proof. We prove the claim when q is odd; the case where q is even is similar. We work in terms of the bases $\mathcal{B}^\varepsilon$ in (2.5) and (2.6).

It will be useful to fix three particular vectors. First let $t_1, t_{m-1} \in \langle e_1, f_1, e_{m-1}, f_{m-1}\rangle$ be nonsingular vectors such that $(e_i - f_i, t_i) = 0$ and $\langle e_i - f_i, t_i\rangle$ is a nondegenerate minus-type 2-space. Next let $t_2 \in \langle e_1, f_1, e_2 - f_2, e_{m-1}, f_{m-1}\rangle^\perp$ with the property that $\langle e_2 - f_2, t_2\rangle$ is a nondegenerate minus-type 2-space.

Recall that the element y has type $r^\varepsilon \perp (2m-2)^-$, centralising a decomposition $U_1 \perp U_2$. If $\varepsilon = -$, then we may assume that $r^+ = r_{e_1 - f_1}$ and

$$U_1 = \langle e_1, f_1\rangle \quad \text{and} \quad U_2 = \langle e_2, \ldots, f_{m-1}, u_m, v_m\rangle.$$

If $\varepsilon = +$, then we may assume that $r^- = r_{e_1 - f_1}$ and

$$U_1 = \langle e_1 - f_1, t_1\rangle \quad \text{and} \quad U_2 = \langle e_2, \ldots, f_{m-2}, e_{m-1} - f_{m-1}, t_{m-1}, e_m, f_m\rangle.$$

Case 1: $\nu(x_2) = 1$

Lemma 3.2.6 implies that x_1 and x_2 are reflections in nonsingular vectors. If u_1 and u_2 are nonsingular vectors, then $r_{u_1} = r_{u_2}$ if and only if $\langle u_1\rangle = \langle u_2\rangle$. Therefore, it suffices to prove the claim for $x_1 = r_{u_1}$ and $x_2 = r_{u_2}$ for orbit representatives $(\langle u_1\rangle, \langle u_2\rangle)$ for the action of G on pairs of distinct nonsingular 1-spaces of V. We may assume that $u_1 = e_1 - f_1$. Now $V = \langle u_1\rangle \perp \langle u_1\rangle^\perp$ and $G_{\langle u_1\rangle}$ acts transitively on the sets of nonzero vectors of a given norm in $\langle u_1\rangle^\perp$. Therefore, we may assume that $u_2 = \xi u_1 + \eta(e_1 + f_1)$ or $u_2 = \xi u_1 + \eta e_3$ for scalars $\xi, \eta \in \mathbb{F}_q$. This amounts to the following two cases

(i) $u_2 = e_1 - \lambda f_1$ for $\lambda \in \mathbb{F}_q \setminus \{0, 1\}$

(ii) $u_2 = e_1 + f_1 + \lambda e_3$ for $\lambda \in \mathbb{F}_q^\times$

First assume that $\varepsilon = -$. Let z have type $r_v \perp (2m-2)^-$ centralising the decomposition $\langle v, w\rangle \perp \langle v, w\rangle^\perp$ where $v = e_1 + e_2 - f_2$ and $w = e_1 + e_2 + f_2$. Note that v is nonsingular and $\langle v, w\rangle$ is a nondegenerate plus-type 2-space. By Theorem 5.2.9, $\mathcal{M}(G, z) \subseteq \{G_{\langle v\rangle}, G_{\langle w\rangle}, G_{\langle v,w\rangle}\}$. Observe that $vx_1 = f_1 + e_2 + f_2$ and $wx_1 = f_1 + e_2 - f_2$, neither of which is contained in $\langle v, w\rangle$. Therefore, x_1 does not stabilise $\langle v\rangle$, $\langle w\rangle$ nor $\langle v, w\rangle$. Consequently, $\langle x_1, z\rangle = G$. Moreover, in the two possible cases above

(i) $vx_2 = \lambda f_1 + e_2 + f_2$ and $wx_2 = \lambda f_1 + e_2 - f_2$

(ii) $vx_2 = -f_1 + e_2 + f_2 - \lambda e_3$ and $wx_2 = -f_1 + e_2 + f_2 - \lambda e_3$

In both cases, vx_2 and wx_2 are not contained in $\langle v, w\rangle$, so, as above, $\langle x_2, z\rangle = G$. It remains to observe that since $Q(e_1 - f_1) = -2 = Q(e_1 + e_2 - f_2)$, there exists $g \in G$ such that $\langle e_1, f_1\rangle g = \langle v, w\rangle$ and $(e_1 - f_1)g = e_1 + e_2 - f_2$. This implies that $r_{(e_1 - f_1)g} = r_v$ and $y^g = z$.

Now assume that $\varepsilon = +$. In this case, let z have type $r_v \perp (2m-2)^-$ centralising $\langle v, w\rangle \perp \langle v, w\rangle^\perp$ where $v = e_1 + e_2 - f_2$ and $w = e_1 + t_2$, noting that $\langle v, w\rangle$ is a nondegenerate minus-type 2-space. Arguing as in the previous case we see that $\langle x_1, z\rangle = \langle x_2, z\rangle = G$.

Moreover, there exists $g \in G$ such that $\langle e_1 + f_1, t_1 \rangle g = \langle v, w \rangle$ and $(e_1 - f_1)g = e_1 + e_2 - f_2$, so $y^g = z$. This completes the proof in Case 1.

Case 2: $\nu(x_2) = 2$ *and* x_2 *is semisimple*

In this case, x_1 is a reflection and x_2 centralises a decomposition $W \perp W^\perp$ where W is a nondegenerate 2-space. Moreover, if $|x_2| = 2$, then we may assume that $x_2 = -I_2 \perp I_{2m-2}$ and if $|x_2|$ is odd, then $x_2 = A \perp I_{2m-2}$ where A is irreducible. As in Case 1, it suffices to assume that $x_1 = r_u$ where $u = e_1 - f_1$ and consider orbit representatives W of the action of $G_{\langle u \rangle}$ on nondegenerate 2-subspaces of V. Considering that W is either plus- or minus-type, and by separating into the cases where

$$\text{(i) } \langle u \rangle \leqslant W \qquad \text{(ii) } W \leqslant \langle u \rangle^\perp \qquad \text{(iii) } \langle u \rangle \not\leqslant W \not\leqslant \langle u \rangle^\perp$$

we may assume that W is one of the following

(i) $W = \langle e_1, f_1 \rangle$ or $W = \langle e_1 - f_1, t_1 \rangle$

(ii) $W = \langle e_2, f_2 \rangle$ or $W = \langle e_2 - f_2, t_2 \rangle$

(iii) $W = \langle e_2 - f_2 + \lambda u, e_2 + f_2 \rangle$ or $W = \langle e_2 - f_2 + \lambda u, t_2 \rangle$ where $\lambda \in \mathbb{F}_q^\times$.

As in Case 1, let z be an element of type $r_v \perp (2m-2)^-$, centralising a decomposition $\langle v, w \rangle \perp \langle v, w \rangle^\perp$ where $v = e_1 + e_2 - f_2$. Moreover, let $w = e_1 + e_2 + f_2$ if $\varepsilon = -$ and $w = e_1 + t_2$ if $\varepsilon = +$. Note that $\langle v, w \rangle$ is a nondegenerate $(-\varepsilon)$-type 2-space. Consequently, we have $\langle x_1, z \rangle = G$. Since x_2 fixes $W^\perp$ pointwise and either negates or acts irreducibly on W, we see that $\langle x_2, z \rangle = G$ also.

Case 3: $\nu(x_2) = 2$ *and* x_2 *is unipotent*

By Lemma 2.4.7, we need to consider the cases where x_2 has Jordan form $[J_2^2, J_1^{2m-4}]$ and $[J_3, J_1^{2m-3}]$. The latter case is very similar to Case 2, so we provide the details in the case where x_2 has Jordan form $[J_2^2, J_1^{2m-4}]$.

As before, x_1 is a reflection. In this case, x_2 centralises a decomposition $W \perp W^\perp$ where $W = W_1 \oplus W_2$ for totally singular 2-spaces W_1 and W_2. Moreover, x_2 acts trivially on $W^\perp$ and acts indecomposably on W_i stabilising a unique 1-space $\langle w_i \rangle \leqslant W_i$. As in the previous cases, it suffices to assume that $x_1 = r_u$ where $u = e_1 - f_1$ and consider orbits of the action of $G_{\langle u \rangle}$. In this way, we may assume that one of the following holds

(i) $W_1 = \langle e_1, e_2 \rangle$ with $w_1 = e_1$ and $W_2 = \langle f_1, f_2 \rangle$ with $w_2 = f_2$

(ii) $W_1 = \langle e_1, e_2 \rangle$ with $w_1 = e_1 + e_2$ and $W_2 = \langle f_1, f_2 \rangle$ with $w_2 = f_2$

(iii) $W_1 = \langle e_2, e_3 \rangle$ with $w_1 = e_2$, and $W_2 = \langle f_2, f_3 \rangle$ with $w_2 = f_3$

(iv) $W_1 = \langle e_2, e_1 + e_3 \rangle$ with $w_1 = e_2$ and $W_2 = \langle f_2, f_3 \rangle$ with $w_2 = f_3$

(v) $W_1 = \langle e_1 + e_2, e_3 \rangle$ with $w_1 = e_1 + e_2$ and $W_2 = \langle f_2, f_3 \rangle$ with $w_2 = f_3$

As in the previous cases, let z have type $r_v \perp (2m-2)^-$ centralising a decomposition $\langle v, w\rangle \perp \langle v, w\rangle^\perp$ where $v = e_1 + e_2 - f_2$, and let $w = e_1 + e_2 + f_2$ if $\varepsilon = -$ and $w = e_1 + t_2$ if $\varepsilon = +$. Consequently, we have $\langle x_1, z\rangle = G$. It is also easy to see that the action of x_2 on the decomposition $(W_1 \oplus W_2) \perp W^\perp$ ensures that x_2 stabilises none of $\langle v\rangle$, $\langle w\rangle$ and $\langle v, w\rangle$.

For example, consider case (i). Here

$$x_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \oplus \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \perp I_{2m-4}.$$

with respect to $(\langle e_1, e_2\rangle \oplus \langle f_1, f_2\rangle) \perp \langle e_1, f_1, e_2, f_2\rangle^\perp$. Therefore, x_2 fixes e_1 and f_2 and maps $e_2 \mapsto e_1 + e_2$ and $f_1 \mapsto f_1 - f_2$. Therefore, $vx_2, wx_2 \notin \langle v, w\rangle$. Therefore, we conclude that $\langle x_2, z\rangle = G$. □

Proposition 5.2.13. *Let $G = \langle \mathrm{P}\Omega^\varepsilon_{2m}(q), \theta\rangle \in \mathcal{A}$ where $\theta \in \mathrm{PGO}^\varepsilon_{2m}(q) \setminus \mathrm{PDO}^\varepsilon_{2m}(q)$. Then*

(i) $u(G) \geqslant 2$

(ii) $u(G) \to \infty$ *as* $q \to \infty$.

Proof. We will apply the probabilistic method encapsulated by Lemma 2.1.1. Theorem 5.2.9 gives the members of $\mathcal{M}(G, y)$. Let $x \in G$ have prime order. We now use fixed point ratio bounds from Section 3.1 to obtain an upper bound on $P(x, y)$.

If $\theta = \delta r$, then q is odd and

$$P(x,y) \leqslant \frac{1}{q^2} + \frac{1}{q^{m-1}-1} + \frac{4}{q^{2m-3}} + \frac{1}{q^{2m-2}} + N_m \frac{2}{q^{m-2}} < \frac{1}{2}$$

where N_m is 4 if m is odd and 0 if m is even. In addition, $P(x, y) \to 0$ as $q \to \infty$.

From now on we may assume that $\theta = r$. By Remark 5.2.7, we may assume that G does not appear in (5.7). First assume that q is odd. For brevity, write

$$P_1(m,q) = \frac{1}{q^{m-1}-1} + \frac{4}{q^m - 1} + \frac{4}{q^{2m-3}}.$$

In this case,

$$P(x,y) \leqslant 2q^{-1} + q^{-2} + q^{-(2m-2)} + 2q^{-(2m-1)} + P_1(m,q).$$

Now $P(x, y) \to 0$ as $q \to \infty$, and if $q > 3$, then $P(x, y) < \frac{1}{2}$. Now assume that $q = 3$ and therefore $m \geqslant 5$. Making use of the dependence on $\nu(x)$ in the fixed point ratio bounds in Proposition 3.1.4, we obtain

$$P(x,y) \leqslant \begin{cases} 2q^{-3} + q^{-6} + q^{-(2m-6)} + 2q^{-(2m-3)} + P_1(m,q) < 0.120 & \text{if } \nu(x) \geqslant 3 \\ 2q^{-2} + q^{-4} + q^{-(2m-4)} + 2q^{-(2m-2)} + P_1(m,q) < 0.268 & \text{if } \nu(x) = 2 \\ 2q^{-1} + q^{-2} + q^{-(2m-2)} + 2q^{-(2m-1)} + P_1(m,q) < 0.809 & \text{if } \nu(x) = 1 \end{cases}$$

Now let $x_1, x_2 \in G$ have prime order. If

$$P(x_1, y) + P(x_2, y) > 1$$

then we can assume that $\nu(x_1) = 1$ and $\nu(x_2) \leqslant 2$. In the latter case, Proposition 5.2.12 implies that there exists $y \in G$ such that $\langle x_1, y\rangle = \langle x_2, y\rangle = G$. Therefore, $u(G) \geqslant 2$.

Now assume that q is even. We proceed as when q is odd. In this case, write

$$P_2(m, q) = \frac{1}{q^{m-1} - 1} + \frac{2}{q^m - 1} + \frac{4}{q^{2m-3}}.$$

Here

$$P(x, y) \leqslant q^{-1} + q^{-2} + P_2(m, q).$$

Now $P(x, y) \to 0$ as $q \to \infty$, and if $q > 2$, then $P(x, y) < \frac{1}{2}$. Now assume that $q = 2$ and therefore $m \geqslant 7$. Now

$$P(x, y) \leqslant \begin{cases} q^{-3} + q^{-6} + P_2(m, q) < 0.175 & \text{if } \nu(x) \geqslant 3 \\ q^{-2} + q^{-4} + P_2(m, q) < 0.347 & \text{if } \nu(x) = 2 \\ q^{-1} + q^{-2} + P_2(m, q) < 0.784 & \text{if } \nu(x) = 1 \end{cases}$$

As above, for $x_1, x_2 \in G$ of prime order, if

$$P(x_1, y) + P(x_2, y) > 1$$

then we can assume that $\nu(x_1) = 1$ and $\nu(x_2) \leqslant 2$, in which case, Proposition 5.2.12 implies that there exists $y \in G$ such that $\langle x_1, y\rangle = \langle x_2, y\rangle = G$. Therefore, $u(G) \geqslant 2$. $\square$

5.3 Case II

In this section, we will prove Theorems 5A and 5B in Case II. To this end, write $G = \langle T, \theta \rangle$ where $T = \mathrm{P}\Omega^{\varepsilon}_{2m}(q)$ for $m \geqslant 4$ and $\theta \in \mathrm{Aut}(T) \setminus \mathrm{PGO}^{\varepsilon}_{2m}(q)$. Assume that $T \neq \mathrm{P}\Omega^{+}_{8}(q)$.

Recall that we make the case distinction

(a) $G \cap \mathrm{PGO}^{\varepsilon}_{2m}(q) \leqslant \mathrm{PDO}^{\varepsilon}_{2m}(q)$

(b) $G \cap \mathrm{PGO}^{\varepsilon}_{2m}(q) \not\leqslant \mathrm{PDO}^{\varepsilon}_{2m}(q)$.

The main motivation for this case distinction is that Shintani descent applies directly in Case II(a) but in Case II(b) we need to use this technique in a more flexible manner. A side effect of this distinction is that in Case II(a), as in Case I(a), $v(x) > 1$ for all $x \in G \cap \mathrm{PGL}(V)$ and this makes the probabilistic method easier to apply.

Recall that Table 5.1 further partitions Cases II(a) and II(b). In particular, II(a) is the union of II(i), (ii) and (iv), and II(b) is the union of II(iii) and (v), where Cases II(i)-(v) are defined in terms of the sign ε and the automorphism θ, as summarised in Table 5.3.

We consider Cases II(a) and II(b) in Sections 5.3.1 and 5.3.2. In both sections, we begin by defining an element $t\theta \in T\theta$ for each automorphism θ in Table 5.1 (in Case II), and then we use $t\theta$ to study the uniform spread of $G = \langle T, \theta \rangle$. In doing this we will complete the proofs of Theorems 5A and 5B in Case II.

5.3.1 Case II(a)

In this section, we first we identify an element $t\theta \in G$, then we determine $\mathcal{M}(G, t\theta)$ and apply the probabilistic method. We will conclude with an asymptotic result.

Element selection

As in Case II of Chapter 4, Shintani descent (see Section 2.7) is the central tool in the identification of the element $t\theta$. Consequently, we need to fix our notation relating to Shintani descent in Case II(a).

Table 5.3: Definition of Cases II(i)–(v)

case	ε	θ	condition
(i)	$+$	$\theta_0\varphi^i$	none
(ii)		$\theta_0 r\varphi^i$	f/i is even
(iii)			f/i is odd
(iv)	$-$	$\theta_0\psi^i$	$2f/i$ is odd
(v)			$2f/i$ is even

[$\theta_0 \in \mathrm{Inndiag}(T)$]

Notation 5.3.1. Write $q = p^f$ where $f \geqslant 2$.

Let $V = \mathbb{F}_q^{2m}$ be the natural module for T.

Fix the simple algebraic group

$$X = \begin{cases} \Omega_{2m}(\overline{\mathbb{F}}_2) & \text{if } p = 2 \\ \mathrm{PSO}_{2m}(\overline{\mathbb{F}}_p) & \text{if } p \text{ is odd.} \end{cases}$$

Fix the standard Frobenius endomorphism $\varphi = \varphi_{\mathcal{B}^+}$ of X, defined with respect to the standard basis $\mathcal{B}^+$, as $(a_{ij}) \mapsto (a_{ij}^p)$, modulo scalars.

Fix the diagonal element δ^+ and the reflection r (see Definitions 2.6.15 and 4.1.3).

If $\varepsilon = -$, fix the map Ψ from Lemma 2.6.17, which restricts to an isomorphism $\Psi\colon \langle X_{r\varphi^f}, r\rangle \to \mathrm{PGO}_{2m}^-(q)$. Moreover, fix $\psi = \Psi \circ \varphi \circ \Psi^{-1}$ and $\delta^- = \Psi(\delta^+)$ (see (2.21) and Definition 5.1.5).

As a consequence of Proposition 5.1.12, we can assume that $\theta \in \mathrm{PGO}_{2m}^+(q)\varphi^i$ when $\varepsilon = +$ and $\theta \in \mathrm{PGO}_{2m}^-(q)\psi^i$ when $\varepsilon = -$. In the latter case, the definition of Case II(a) ensures that $2f/i$ is odd, so i is even and it is straightforward to show, for $j = i/2$, we have $2f/(2f, f+j) = 2f/(2f, i)$. Consequently, when $\varepsilon = -$, we may, and will, work with

$$\theta = \theta_0\psi^{f+j} = \theta_0 r\psi^j$$

instead of $\theta_0\psi^i$, noting that j divides f and $2f/i = f/j$ is odd.

Notation 5.3.1. (continued) Write $q = q_0^e$, where (η, σ, e) are as follows

case	η	σ	e
(i)	$+$	φ^i	f/i
(ii)	$-$	$r\varphi^i$	f/i
(iv)	$-$	$r\varphi^j$	$2f/i$

Let F be the Shintani map of (X, σ, e), so

$$F\colon \{(g\widetilde{\sigma})^{X_{\sigma^e}} \mid g \in X_{\sigma^e}\} \to \{x^{X_\sigma} \mid x \in X_\sigma\}.$$

Observe that $X_{\sigma^e} \cong \mathrm{Inndiag}(T)$ and $X_\sigma = \mathrm{Inndiag}(T_0)$ for a subgroup T_0 of T isomorphic to $\mathrm{P}\Omega_{2m}^\eta(q_0)$. We will harmlessly identify T_0 with $\mathrm{P}\Omega_{2m}^\eta(q_0)$ and write $\mathrm{Inndiag}(T_0) = \mathrm{PDO}_{2m}^\eta(q_0) = \langle \mathrm{PSO}_{2m}^\eta(q_0), \delta_0\rangle$.

Remark 5.3.2. Let us make some observations regarding Notation 5.3.1.

(i) The definition of Case II(a) implies that $\varepsilon = \eta^e$.

(ii) If $\varepsilon = +$, then $\mathrm{Inndiag}(T)\theta = X_{\sigma^e}\widetilde{\sigma}$.

(iii) If $\varepsilon = -$, then, via the isomorphism Ψ, we can identify X_{σ^e} with $\mathrm{Inndiag}(T)$ and we can identify $\widetilde{\sigma} = r\varphi^j$ with $\theta = r\psi^j$, so $\mathrm{Inndiag}(T)\theta = X_{\sigma^e}\widetilde{\sigma}$ in this case also.

In light of Remark 5.3.2, the main idea is to select the element $t\theta \in T\theta$ as the preimage under F of a carefully chosen element $y \in \mathrm{Inndiag}(T_0)$. If q is even, then $\mathrm{Inndiag}(T) = T$ and this is straightforward. When q is odd, we use the following two results.

Lemma 5.3.3. *Let q be odd. The Shintani map F restricts to bijections*

(i) $F_1\colon \{(g\widetilde{\sigma})^{\mathrm{PDO}^{\varepsilon}_{2m}(q)} \mid g \in \mathrm{PSO}^{\varepsilon}_{2m}(q)\} \to \{x^{\mathrm{PDO}^{\eta}_{2m}(q_0)} \mid x \in \mathrm{PSO}^{\eta}_{2m}(q_0)\}$

(ii) $F_2\colon \{(g\delta\widetilde{\sigma})^{\mathrm{PDO}^{\varepsilon}_{2m}(q)} \mid g \in \mathrm{PSO}^{\varepsilon}_{2m}(q)\} \to \{(x\delta_0)^{\mathrm{PDO}^{\eta}_{2m}(q_0)} \mid x \in \mathrm{PSO}^{\eta}_{2m}(q_0)\}$.

Proof. This is Lemma 2.7.4 with $\pi\colon \mathrm{SO}_{2m}(\overline{\mathbb{F}}_q) \to \mathrm{PSO}_{2m}(\overline{\mathbb{F}}_q)$, noting that $\langle \mathrm{PSO}^{\varepsilon}_{2m}(q), \widetilde{\sigma}\rangle$ and $\mathrm{PSO}^{\eta}_{2m}(q_0)$ are index two subgroups of $\langle \mathrm{PDO}^{\varepsilon}_{2m}(q), \widetilde{\sigma}\rangle$ and $\mathrm{PDO}^{\eta}_{2m}(q_0)$. □

Lemma 5.3.4. *Let q be odd and assume that $q_0^m \equiv \eta \pmod 4$. The map F_1 restricts to bijections*

(i) $F_{11}\colon \{(g\widetilde{\sigma})^{\mathrm{PDO}^{\varepsilon}_{2m}(q)} \mid g \in T\} \to \{x^{\mathrm{PDO}^{\eta}_{2m}(q_0)} \mid x \in T_0\}$

(ii) $F_{12}\colon \{(g\widetilde{\sigma})^{\mathrm{PDO}^{\varepsilon}_{2m}(q)} \mid g \in \mathrm{PSO}^{\varepsilon}_{2m}(q) \setminus T\} \to \{x^{\mathrm{PDO}^{\eta}_{2m}(q_0)} \mid x \in \mathrm{PSO}^{\eta}_{2m}(q_0) \setminus T_0\}$.

Proof. The condition $q_0^m \equiv \eta \pmod 4$ ensures $|\mathrm{PSO}^{\eta}_{2m}(q_0) : T_0| = 2$ (see (2.9)). We claim $|\mathrm{PSO}^{\varepsilon}_{2m}(q) : T| = 2$. If $\varepsilon = \eta = +$, then $q^m \equiv 1 \pmod 4$ and $|\mathrm{PSO}^{+}_{2m}(q) : T| = 2$. Next, if $\varepsilon = +$ and $\eta = -$, then e is even, so again $q^m \equiv 1 \pmod 4$ and $|\mathrm{PSO}^{+}_{2m}(q) : T| = 2$. Finally, if $\varepsilon = \eta = -$, then e is odd and $q^m \equiv 3 \pmod 4$, so $|\mathrm{PSO}^{-}_{2m}(q) : T| = 2$.

Write $W = \mathrm{Spin}_{2m}(\overline{\mathbb{F}}_q)$ and let $\pi\colon W \to X$ be the natural isogeny (see Section 2.6.2). Now $\pi(W_{\sigma^e}) = T$ where $W_{\sigma^e} = \mathrm{Spin}^{\varepsilon}_{2m}(q)$, and $\pi(W_\sigma) = T_0$ where $W_\sigma = \mathrm{Spin}^{\eta}_{2m}(q_0)$ (see Theorem 2.6.3(iii)). Evidently, $T_0 \trianglelefteqslant \mathrm{Inndiag}(T_0)$. Moreover, if $\varepsilon = +$, then the condition $q_0^m \equiv \eta \pmod 4$ implies that condition (5.3) is satisfied, so, in light of Remark 5.1.2, $\langle \ddot{\sigma}\rangle \trianglelefteqslant \langle \mathrm{Inndiag}(T)/T, \ddot{\sigma}\rangle$ and hence $\langle T, \widetilde{\sigma}\rangle \trianglelefteqslant \langle \mathrm{Inndiag}(T), \widetilde{\sigma}\rangle$. Similarly, if $\varepsilon = -$, then i is even, so $[\ddot{\psi}^i, \ddot{\delta}] = 1$ (see Lemma 5.1.9), which implies that $\langle \ddot{\sigma}\rangle \trianglelefteqslant \langle \mathrm{Inndiag}(T)/T, \ddot{\sigma}\rangle$ and hence, again, $\langle T, \widetilde{\sigma}\rangle \trianglelefteqslant \langle \mathrm{Inndiag}(T), \widetilde{\sigma}\rangle$. Therefore, by Lemma 2.7.4, the Shintani map F of (X, σ, e) restricts to the map F_{11}. By Lemma 5.3.3, F restricts to F_1, so, in fact, F_1 restricts to the bijections F_{11} and F_{12}, as required. □

We are now in a position to define the elements we will use in our proof of Theorem 5A in Case II(a).

Proposition 5.3.5. *Let $T = \mathrm{P}\Omega^{\varepsilon}_{2m}(q)$ and let θ be an automorphism in Table 5.1 (in Case II(i), II(ii) or II(iv)). Let $y \in \mathrm{PDO}^{\eta}_{2m}(q_0)$ be the element in Table 5.4, unless $(\eta, m) = (-, 5)$, in which case let y have type ${}^{a}(4)^{-} \perp {}^{c}(6)^{+}$. Then there exists $t \in T$ such that $(t\theta)^e$ is X-conjugate to y.*

Table 5.4: Case II(a): The element y for the automorphism θ

$m \pmod 4$	y	
	$\eta = +$	$\eta = -$
0	${}^c(m)^- \perp {}^a(m-2)^+ \perp {}^a(2)^-$	${}^c(2m-2)^+ \perp {}^a(2)^-$
2	${}^c(m)^+ \perp {}^a(m-2)^- \perp {}^a(2)^-$	
3	${}^c(2m-2)^- \perp {}^a(2)^-$	${}^c(m+1)^- \perp {}^a(m-3)^- \perp {}^a(2)^-$
1		${}^c(m+3)^- \perp {}^a(m-5)^- \perp {}^a(2)^-$

[we exclude $(\eta, m) = (-, 5)$ in this table, we describe y by specifying its type over $\mathbb{F}_{q_0}$]

Remark 5.3.6. Let us comment on how to read Tables 5.1 and 5.4 (and later Table 5.6) in conjunction with Proposition 5.3.5 (and later Proposition 5.3.17).

(i) In Table 5.4 and elsewhere in Chapter 5, we will use symbols a, b and c introduced in (4.9), (4.10) and (4.11), but now we refer to the Rows (1)–(3) in Table 5.1 (rather than Table 4.1).

(ii) For each of Cases II(i)–(v), each of Rows (1)–(3) (in Table 5.1) and each valid choice of i, there is at most one choice of (X, σ, e) (giving a Shintani map) and an at most one choice of element $y \in \mathrm{PDO}^{\eta}_{2m}(q_0)$. However, when q is odd and $D(Q) = \square$, then recall that we use the notation ι for "1 or $r_{\square} r_{\boxtimes}$". In this case, there may be two possibilities for θ (for instance ψ^{42} and $r_{\square} r_{\boxtimes} \psi^{42}$). The point is that Proposition 5.1.12 informs us that we can consider either of these possibilities for θ: we only need to consider one of them and it does not matter which one (see Remark 5.1.13(iii)). In this case, Proposition 5.3.5 states that for one of these possibilities for θ, there exists $t \in T$ such that $(t\theta)^e$ is X-conjugate to y. We do not know which choice of θ works and it does not matter. It does, however, mean that we need to carry around lots of iotas in our arguments.

Proof of Proposition 5.3.5. Since $y \in \mathrm{PDO}^{\eta}_{2m}(q_0) = X_{\sigma}$, by Theorem 2.7.1, there exists $g \in \mathrm{Inndiag}(T)$ such that $(g\widetilde{\sigma})^e$ is X-conjugate to y. Therefore, the aim of this proof is to demonstrate that $g\widetilde{\sigma}$ is contained in the coset $T\theta$. By arguments akin to those in the proof of Proposition 5.2.6, it is routine to determine $\tau(y)$, and if $y \in \mathrm{PSO}^{\eta}_{2m}(q_0)$ to also determine $\mathrm{sp}(y)$, and, therefore gain information about which coset of T_0 contains y. We will use Shintani descent (in particular Lemmas 5.3.3 and 5.3.4) to deduce information about which coset of T contains $g\widetilde{\sigma}$.

If q is even, then $\widetilde{\sigma} = \theta$ (one of φ^i, $r\varphi^i$ and ψ^i) and $X_{\sigma^e} = T$, so $g\widetilde{\sigma} \in T\theta$.

Therefore, from now on we may assume that q is odd. Assume that θ appears in Row (2). Then $\tau(y) = \beta_0$, so $y \in \mathrm{PSO}^{\eta}_{2m}(q_0)\delta_0$. By Lemma 5.3.3, this implies that $g\widetilde{\sigma} \in \mathrm{PSO}^{\varepsilon}_{2m}(q)\delta\widetilde{\sigma}$. Therefore, $g\widetilde{\sigma} = t\theta$ where $t \in T$ and $\theta = \iota\delta\widetilde{\sigma}$. In Case II(i), $\theta = \iota\delta\varphi^i$, in Case II(ii) $\theta = \iota\delta r\varphi^i$ and in Case II(iv) $\theta = \iota\delta\psi^i$, which suffices to prove the claim.

Now assume θ appears in Row (1) or (3). Then $\tau(y) = 1$, so $y \in \mathrm{PSO}^{\eta}_{2m}(q_0)$ and $g\widetilde{\sigma} \in \mathrm{PSO}^{\varepsilon}_{2m}(q)\widetilde{\sigma}$, by Lemma 5.3.3. If $D(Q) = \boxtimes$, then $\widetilde{\sigma} = \theta$ (one of φ^i, $r\varphi^i$ and ψ^i) and $T = \mathrm{PSO}^{\varepsilon}_{2m}(q)$, so $g\widetilde{\sigma} \in T\theta$.

Therefore, it remains to assume that $D(Q) = \square$. In this case, $q^m \equiv \varepsilon \pmod 4$. For now assume that $q_0^m \equiv \eta \pmod 4$, so that we may apply Lemma 5.3.4 (this always holds when $\varepsilon = -$). By the choice of a and c, if θ is in Row (1), then $\mathrm{sp}(y) = \square$, so $y \in \mathrm{P}\Omega^{\eta}_{2m}(q_0)$ and $g\widetilde{\sigma} \in T\widetilde{\sigma}$, by Lemma 5.3.4, and, since $\theta = \widetilde{\sigma}$ (one of φ^i, $r\varphi^i$ and ψ^i), we conclude that $g\widetilde{\sigma} \in T\theta$. Similarly, if θ is in Row (3), then $y \in \mathrm{PSO}^{\eta}_{2m}(q_0) \setminus \mathrm{P}\Omega^{\eta}_{2m}(q_0)$ and $g\widetilde{\sigma} \in Tr_{\square}r_{\boxtimes}\widetilde{\sigma}$, so $g\widetilde{\sigma} \in T\theta$ since $\theta = \widetilde{\sigma}$ (one of $r_{\square}r_{\boxtimes}\varphi^i$, $r_{\square}r_{\boxtimes}r\varphi^i$ or $r_{\square}r_{\boxtimes}\psi^i$).

We now need to assume that $q^m \equiv \varepsilon \pmod 4$ but $q_0^m \not\equiv \eta \pmod 4$. In this case $\varepsilon = +$. First assume that $\eta = +$. Therefore, $q_0 \equiv 3 \pmod 4$ and m is odd. This forces $q \equiv 1 \pmod 4$. Together this implies that m is odd, $p \equiv 3 \pmod 4$, i is odd, f is even. Under these conditions, we need only consider one of φ^i and $r_{\square}r_{\boxtimes}\varphi^i$ (see Remark 5.1.13(iv)), so we can choose θ such that $g\widetilde{\sigma} \in T\theta$. Now assume that $\eta = -$. Therefore, $q_0 \equiv 1 \pmod 4$, so m is even or i is even or $p \equiv 1 \pmod 4$. This allows us to only consider one of $r\varphi^i$ and $r_{\square}r_{\boxtimes}r\varphi^i$ (see Remark 5.1.13(iv)), so, as above, we can choose θ such that $g\widetilde{\sigma} \in T\theta$. This completes the proof. □

Probabilistic method

Continue to let T be the simple group $\mathrm{P}\Omega^{\varepsilon}_{2m}(q)$ and let θ be an automorphism from Table 5.1. Fix $y \in \mathrm{PDO}^{\eta}_{2m}(q_0)$ from Table 5.4 and $t\theta \in G = \langle T, \theta \rangle$ from Proposition 5.3.5. We will now study the set $\mathcal{M}(G, t\theta)$ of maximal overgroups of $t\theta$ in G.

Theorem 5.3.7. *The maximal subgroups of G which contain $t\theta$ are listed in Table 5.5, where $m(H)$ is an upper bound on the multiplicity of the subgroups of type H in $\mathcal{M}(G, t\theta)$.*

We will present a result on multiplicities of subgroups in $\mathcal{M}(G, t\theta)$, before proving Theorem 5.3.7 in three parts, by considering the cases where $H \in \mathcal{M}(G, t\theta)$ is reducible, irreducible imprimitive and primitive. As in Chapter 4, we write

$$\widetilde{G} = \langle X_{\sigma^e}, \widetilde{\sigma} \rangle$$

noting that $\mathrm{Inndiag}(T) \leqslant \widetilde{G} \leqslant \mathrm{Aut}(T)$ and $G \leqslant \widetilde{G}$.

The following result will apply to Case II(b) also.

Proposition 5.3.8. *Let $T \leqslant A \leqslant \mathrm{Aut}(T)$ and let H be a maximal $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$ or $\mathcal{C}_5$ subgroup of A. Then there is a unique $\widetilde{G}$-conjugacy class of subgroups of type H, unless H has one of the following types, in which case there are two $\widetilde{G}$-classes:*

type	P_m	$\mathrm{GL}_m(q)$	$\mathrm{GU}_m(q)$	$\mathrm{O}^+_m(q^2)$	$\mathrm{O}_m(q^2)$
ε	$+$	$+$	$+$	$+$	$-$
m	*any*	*odd*	*even*	*even*	*odd*

Table 5.5: Case II(a): Description of $\mathcal{M}(G, t\theta)$

	type of H	$m(H)$	conditions
$\mathcal{C}_1$	$\mathrm{O}_2^v(q) \times \mathrm{O}_{2m-2}^{\varepsilon v}(q)$	1	$(\eta, m) \neq (-, 5)$
	$P_{m/2}$	2	$\eta = +$ and $m \equiv 0 \pmod 4$
	$P_{m/2-1}$	2	$\eta = +$ and $m \equiv 2 \pmod 4$
	$\mathrm{O}_{m-2}^v(q) \times \mathrm{O}_{m+2}^{\varepsilon v}(q)$	1	$\eta = +$ and m even
	P_{m-1}	2	$\eta = -$ and m even
	$\mathrm{O}_{m-3}^v(q) \times \mathrm{O}_{m+3}^{\varepsilon v}(q)$	1	$\eta = -$ and m odd
	$\mathrm{O}_{m-5}^v(q) \times \mathrm{O}_{m+5}^{\varepsilon v}(q)$	1	$\eta = -$ and $m \equiv 1 \pmod 4$ with $m \neq 5$
	$\mathrm{O}_{m-1}^v(q) \times \mathrm{O}_{m+1}^{\varepsilon v}(q)$	1	$\eta = -$ and $m \equiv 3 \pmod 4$
	$\mathrm{O}_4^v(q) \times \mathrm{O}_6^{\varepsilon v}(q)$	1	$\eta = -$ and $m = 5$
	P_3	2	$\eta = -$ and $m = 5$
$\mathcal{C}_2$	$\mathrm{O}_{2m/k}^v(q) \wr S_k$	N	$k \mid m,\ k > 1,\ v^k = \varepsilon$
	$\mathrm{O}_{2m/k}(q) \wr S_k$	N	$k \mid 2m,\ 2m/k > 1$ odd
	$\mathrm{GL}_m(q)$	$2N$	$\eta = +,\ m$ even
		N	$\varepsilon = +,\ \eta = -,\ m$ odd
$\mathcal{C}_3$	$\mathrm{O}_m(q^2)$	$2N$	$m > 5$ odd
	$\mathrm{GU}_m(q)$	$2N$	$\varepsilon = \eta = +,\ m$ even
		N	$\varepsilon = \eta = -,\ m$ odd
$\mathcal{C}_5$	$\mathrm{O}_{2m}^v(q^{1/k})$	N	$k \mid f,\ k$ is prime, $v^k = \varepsilon$
$\mathcal{S}$	$\mathrm{PSp}_4(q)$	$2N$	$\eta = -,\ m = 5,\ q \equiv \varepsilon \pmod 4$

[$N = |C_{\mathrm{PDO}_{2m}^{\eta}(q_0)}(y)|$, in $\mathcal{C}_1$ there is a unique choice of v]

Proof. If $m \leqslant 6$, then the result follows from the tables in [7, Chapter 8]. Now assume that $m \geqslant 7$. We will apply the Main Theorem of [43], which we described Section 2.5.1 (see Example 2.5.3 and also the proof of Proposition 4.3.8).

Let H be a maximal geometric subgroup of G. Recall $\pi\colon \mathrm{Out}(T) \to S_c$ associated to the action of $\mathrm{Out}(T)$ on the set representatives of the c distinct T-classes of subgroups of T of the same type as H. By [43, Tables 3.5E and 3.5G], $\pi(\widetilde{G}/T)$ is transitive, except for the exceptional cases in the statement, when $c = 2$ and $\pi(\widetilde{G}/T)$ is intransitive. This proves the statement, but we provide some examples, with $\varepsilon = +$.

For example, consider the case where m is odd, H has type $\mathrm{O}_{2m}^-(q^{1/2})$ and $p \equiv 1 \pmod 4$. In this situation, $c = 4$, $\ker(\pi) = \langle \ddot{\varphi} \rangle$ and the stabiliser of H_1 is $\langle \ddot{\varphi}, \ddot{r}_\Box \rangle$. Therefore, $\pi(\widetilde{G}/T) = \langle \ddot{\delta} \rangle \cong C_4$ is transitive, so there is exactly one $\widetilde{G}$-class of subgroups of G of the same type as H.

For another example, let m be even and let H have type $\mathrm{GL}_m(q)$. In this situation, $c = 2$, $\ker(\pi) = \langle \mathrm{Inndiag}(T)/T, \ddot{\varphi} \rangle$ and the stabiliser of H_1 is $\langle \ddot{\varphi}, \ddot{r}_\Box \rangle$. Therefore, $\pi(\widetilde{G}/T) = 1$, so there are exactly two $\widetilde{G}$-classes of subgroups of G of the same type as H. □

Proposition 5.3.9. *Theorem 5.3.7 is true for reducible subgroups.*

Proof. The proof is almost identical to the proof of Proposition 4.3.9, so we summarise the argument. If H is a maximal parabolic subgroup of G, then $H \leqslant \langle Y_\sigma, \widetilde{\sigma} \rangle$ for a (closed connected) σ-stable parabolic subgroup Y of X, so Lemma 2.7.9 implies that the number of X_{σ^e}-conjugates of H which contain $t\theta$ is equal to the number of X_σ-conjugates of $H \cap X_\sigma$ that contain $F(t\theta)$, which can be easily determined by inspecting the maximal reducible overgroups of y in X_σ, using Lemma 2.3.3. If H is the stabiliser of a nondegenerate k-space, then we let $L = \mathrm{SL}_{2m}(\overline{\mathbb{F}}_p)/\langle -I_{2m} \rangle$ and the result follows by applying Lemma 2.7.9 to the Shintani map of (L, σ, e) as described in detail in the proof of Proposition 4.3.9. □

Proposition 5.3.10. *Theorem 5.3.7 is true for irreducible imprimitive subgroups.*

Proof. By [43, Table 3.5.E], the possible types of irreducible imprimitive subgroup are the types featured in Table 5.5. If $\varepsilon = +$, then we claim that maximal subgroups of type $\mathrm{GL}_m(q)$ only arise if $\eta = +$ and m is even, or $\eta = -$ and m is odd.

First consider $\eta = +$ and m odd. In this case, $G \leqslant \langle \mathrm{Inndiag}(T), \varphi^i \rangle$, so there are no elements in G which interchange the totally singular subspaces $\langle e_1, \dots, e_m \rangle$ and $\langle f_1, \dots, f_m \rangle$ (see Remark 2.3.23). Therefore, a subgroup of G of type $\mathrm{GL}_m(q)$ is contained in two subgroups of type of P_m, and no maximal subgroups of type $\mathrm{GL}_m(q)$ occur.

Now consider $\eta = -$ and m even. In this case, $G \not\leqslant \langle \mathrm{Inndiag}(T), \varphi^i \rangle$, so by [43, Tables 3.5.E and 3.5.G], any subgroup of G of type $\mathrm{GL}_m(q)$ is contained in a proper normal subgroup of G and is, therefore, not maximal.

The multiplicities follow quickly from Lemma 2.7.11 and Proposition 5.3.8. □

The following lemma can be proved in exactly the same manner as Lemma 4.3.18

Lemma 5.3.11. *Assume that $(\eta, m) \neq (-, 5)$. A suitable power of y has type $A \perp I_{n-2}$ where*

$$A = \begin{cases} (2)^-_{q_0} & \text{if } q_0 \text{ is not Mersenne} \\ -I_2 & \text{otherwise.} \end{cases}$$

Proposition 5.3.12. *Theorem 5.3.7 is true for primitive subgroups.*

Proof. For now assume that $(\eta, m) \neq (-, 5)$. By construction, a suitable power of $t\theta$ is X-conjugate to y. By Lemma 5.3.11, we may fix a power $z = z_1 \perp I_{2m-2}$ of y where

$$z_1 = \begin{cases} (2)^-_{q_0} & \text{if } q_0 \text{ is not Mersenne} \\ -I_2 & \text{otherwise,} \end{cases}$$

noting that $z \in T$ has prime order.

Now let $H \in \mathcal{M}(G, t\theta)$ be primitive. By Theorem 2.5.1, H is contained in one of the geometric families $\mathcal{C}_3, \ldots, \mathcal{C}_8$ or is an almost simple irreducible group in the $\mathcal{S}$ family. As in the proof of Theorem 4.3.7, we consider each family in turn.

Consider $\mathcal{C}_3$ subgroups. First suppose that H has type $\mathrm{O}^v_{2m/k}(q^k)$ for a prime divisor k of $2m$ and a sign $v \in \{\circ, \varepsilon\}$. Write $H \cap T = B.k$. From the definition of z, Lemma 2.5.7(ii) implies that $z \in B$. Moreover, since $\nu(z) = 2$, Lemma 2.5.7(i) implies that $k = 2$. Therefore, to verify the claim in Table 5.5, we can assume that m is even. In this case, a power of y has type $(2d)^+ \perp I_{2m-2d}$, where $d \in \{\frac{m}{2}, \frac{m-2}{2}, m-1\}$ is odd, which contradicts Corollary 2.5.9. Therefore, H does not have type $\mathrm{O}^v_{2m/k}(q^k)$ unless m is odd and $k = 2$.

Now suppose that H has type $\mathrm{GU}_m(q)$. These maximal subgroups only occur when $\varepsilon = +$ and m is even, or $\varepsilon = -$ and m is odd (see [43, Tables 3.5.E and 3.5.F]). Suppose that $\varepsilon = +$ but $\eta = -$ (and m is even). In this case a power of y has type $I_2 \perp (2m-2)^-$, but this is a contradiction to Corollary 2.5.9(ii)(a). Therefore, H has type $\mathrm{GU}_m(q)$ and $\varepsilon = \eta = (-)^m$.

Now let us turn to $\mathcal{C}_4$ subgroups. Suppose that H is the centraliser of a decomposition $V_1 \otimes V_2$ where $\dim V_1 \geqslant \dim V_2 > 1$. Since $z \in H$, we may write $z = z_1 \otimes z_2$. Since $\nu(z) = 2$, Lemma 2.5.13 implies that $\nu(z_1) = 1$, $\nu(z_2) = 0$ and $\dim V_2 = 2$. Inspecting the conditions on $\dim V_1$ and $\dim V_2$ in [43, Tables 3.5.E and 3.5.F], this is impossible unless $\varepsilon = +$ and H has type $\mathrm{Sp}_2(q) \otimes \mathrm{Sp}_m(q)$. Since $\nu(z_2) = 0$, Lemma 2.5.10 implies that z_1 is a semisimple element of $\mathrm{Sp}_m(q)$ such that $\nu(z_1) = 1$, and there are no such elements. Therefore, $H \notin \mathcal{C}_4$.

If $H \in \mathcal{C}_5$, then H has type $\mathrm{O}^v_{2m}(q_1)$ where $q = q_1^k$ for a prime divisor k of f and a sign $v \in \{+, -\}$ such that $v^k = \varepsilon$.

The $\mathcal{C}_6$ family is empty since q is not prime.

We now treat $\mathcal{C}_7$ subgroups, which only arise when $\varepsilon = +$. Suppose that H is the stabiliser of a decomposition $U_1 \otimes U_2 \otimes \cdots \otimes U_k$ with $\dim U_i > 1$. Let $H_0 = H \cap \mathrm{PGL}(V)$ and write $H_0 = B.S_k$. Since z does not centralise a tensor product decomposition (see the discussion of $\mathcal{C}_4$ subgroups), $z \notin B$. Therefore, z cyclically permutes the k factors. However, z has prime order and exactly two nontrivial eigenvalues which contradicts the eigenvalue pattern required by Lemma 2.5.11. Therefore, $H \notin \mathcal{C}_7$.

The $\mathcal{C}_8$ family is empty.

Finally, consider the $\mathcal{S}$ family. Since $\nu(z) = 2$, $2m \geqslant 10$ and q is not prime, Theorem 2.5.14 implies that no such subgroups arise.

It remains to assume that $(\eta, m) = (-, 5)$. To prove the result in this case, we simply note that y has type ${}^a(4)^- \perp {}^c(6)^+$, so a power of y has type $(6)^+ \perp I_4$, which, in light of Corollary 2.5.9, implies that y is not contained in subgroups of type $\mathrm{O}_5(q^2)$ or $\mathrm{GU}_5(q)$.

To complete the proof, we note that the stated upper bounds on the multiplicities of nonsubspace subgroups follow from Lemma 2.7.11 and Proposition 5.3.8. □

We have now proved Theorem 5.3.7 and are, consequently, in the position to prove Theorem 5A in Case II(a).

Proposition 5.3.13. *Let $G = \langle T, \theta \rangle \in \mathcal{A}$ where $T = \mathrm{P}\Omega^{\varepsilon}_{2m}(q)$ and $\theta \notin \mathrm{PGO}^{\varepsilon}_{2m}(q)$. In Case II(a),*

(i) $u(G) \geqslant 2$

(ii) $u(G) \to \infty$ *as* $q \to \infty$.

Proof. We will use Lemma 2.1.1. Let $x \in G$ have prime order.

Theorem 5.3.7 gives a superset of $\mathcal{M}(G, t\theta)$. Moreover, referring to Table 5.5, it is straightforward to show that

$$N = |C_{\mathrm{PDO}^{\eta}_{2m}(q_0)}(y)| \leqslant 2q_0^m.$$

For instance, if $\eta = -$ and m is even, then Corollary 2.3.5 and Lemma 2.4.4 imply that

$$|C_{X_\sigma}(y)| \leqslant (q_0 + 1)(q_0^{m-1} - 1) \leqslant 2q_0^m.$$

The relevant fixed point ratios are given in Theorem 3.1.1 and Proposition 3.2.4, where we make use of the observation that $\nu(x) \geqslant 2$ for all $x \in G \cap \mathrm{PGO}^{\varepsilon}_{2m}(q) \leqslant \mathrm{PDO}^{\varepsilon}_{2m}(q)$.

With this information, we will prove that $P(x, t\theta) < \frac{1}{2}$ and $P(x, t\theta) \to 0$ as $q \to \infty$, where, as usual,

$$P(x, t\theta) \leqslant \sum_{H \in \mathcal{M}(G, t\theta)} \mathrm{fpr}(x, G/H).$$

By Lemma 2.1.1, this will establish the desired result.

Write $d(n)$ for the number of proper divisors of a number n.

First assume that $\eta = +$ and m is odd, or $\eta = -$ and m is even. Then

$$P(x, t\theta) \leqslant \frac{1}{q^2} + \frac{7}{q^{m-2}} + \frac{5}{q^{m-1}} + (2 + \log\log q + 2d(2m)) \cdot 2q_0^m \cdot \frac{3}{q^{2m-5}},$$

which proves $P(x, t\theta) \to 0$ as $q \to \infty$ and $P(x, t\theta) < \frac{1}{2}$ unless $(\eta, m, q) = (+, 5, 4)$. (Here we make use of the fact that when $\varepsilon = -$, we know that $2f/i$ is odd, so $i > 1$ and consequently $q_0 > p$.)

In the exceptional case, $t\theta$ is not contained in a maximal parabolic subgroup, and we can discount subgroups of type $\mathrm{O}^{-}_{10}(2)$ since they do not contain elements of order $|y| = 51$. These observations, together with a refined bound on the centraliser $|C_{X_\sigma}(y)|$, give

$$P(x, t\theta) \leqslant \frac{1}{4^2} + \frac{3}{4^3} + \frac{1}{4^4} + (1 + 1) \cdot (2 + 1)(2^4 + 1) \cdot \frac{3}{4^5} < \frac{1}{2}.$$

Next assume that $\eta = +$ and m is even. Then

$$P(x,t\theta) \leqslant \frac{1}{q^2} + \frac{3}{q^{m/2-1}} + \frac{14}{q^{m-2}} + (1 + \log\log q + 2d(2m)) \cdot 2q_0^m \cdot \frac{3}{q^{2m-5}} + 8q_0^m \cdot \frac{3}{q^{2m-7}},$$

and we conclude that $P(x,t\theta) \to 0$ as $q \to \infty$ and $P(x,t\theta) < \frac{1}{2}$, unless $(m,q) = (6,4)$.

In this exceptional case, we will show that $t\theta$ is contained in no subgroups of type $\mathrm{GL}_6(4)$ or $\mathrm{GU}_6(4)$; omitting the corresponding term gives $P(x,\theta) < \frac{1}{2}$. The type of y is $2_2^- \perp 4_2^- \perp 6_2^+$. First suppose that y is contained in a subgroup H of type $\mathrm{GU}_6(4)$. Write $H \cap \mathrm{PGL}(V) = B.2$. A power y_1 of y has type $2_2^- \perp I_{10}$, whose order is 3. Therefore, $y_1 \in B$; however, $e = 2$, so this contradicts Corollary 2.5.9, so $t\theta$ is not contained in a $\mathrm{GU}_6(4)$ subgroup. Next suppose that y is contained in a subgroup H of type $\mathrm{GL}_6(4)$. Again we write $H \cap \mathrm{PGL}(V) = B.2$. A power y_2 of y has type $4_2^- \perp I_8$, whose order is 5. Therefore $y_2 \in B$. This implies that $y_2 = M \oplus M^{-\mathsf{T}}$. The four nontrivial eigenvalues of y_2 are $\lambda, \lambda^2, \lambda^{2^2}, \lambda^{2^3}$, where $|\lambda| = 5$. Without loss of generality, λ is an eigenvalue of M. On the one hand, λ^4 must be an eigenvalue of M, but, on the other hand, $\lambda^{-1} = \lambda^4$ is an eigenvalue of $M^{-\mathsf{T}}$, which is a contradiction. Therefore, $t\theta$ is not contained in a $\mathrm{GL}_6(4)$ subgroup.

Now assume that $\eta = -$ and $m \geqslant 7$ is odd. Then

$$\begin{aligned} P(x,t\theta) \leqslant \frac{1}{q^2} + \frac{2}{q^{(m-1)/2}} + \frac{11}{q^{m-3}} + \frac{1}{q^{m-5}} \\ + (2 + \log\log q + 2d(2m)) \cdot 2q_0^m \cdot \frac{3}{q^{2m-5}} + 2q_0^m \cdot \frac{3}{q^{2m-7}} < \frac{1}{2} \end{aligned}$$

and $P(x,t\theta) \to 0$ as $q \to \infty$.

Finally assume that $(\eta, m) = (-,5)$. Then

$$P(x,t\theta) \leqslant \frac{1}{q^2} + \frac{8}{q^3} + \frac{4}{q^4} + (6 + \log\log q) \cdot 2q_0^5 \cdot \frac{3}{q^5} + 2q_0^5 \cdot \frac{3}{q^3},$$

which proves $P(x,t\theta) \to 0$ as $q \to \infty$ and $P(x,t\theta) < \frac{1}{2}$ unless $\varepsilon = +$ and $e = 2$. By arguing as above we can show that y is not contained in a subgroup of type $\mathrm{GL}_5(q)$ and omitting the corresponding term gives $P(x,t\theta) < \frac{1}{2}$ unless $q = 4$. In this case, we can discount subgroups of type $\mathrm{O}_{10}^+(2)$ since they do not contain elements of order $|y| = 35$ and, by Lemma 2.7.12, $t\theta$ is contained in at most $e^2 = 4$ subgroups of type $\mathrm{O}_{10}^-(2)$. Therefore,

$$P(x,t\theta) \leqslant \frac{1}{4^2} + \frac{8}{4^3} + \frac{4}{4^4} + (2 \cdot (2^2+1)(2^3-1) + 4) \cdot \frac{3}{4^5} < \frac{1}{2}.$$

and $P(x,t\theta) \to 0$ as $q \to \infty$. This completes the proof. □

Asymptotic result

We now now record an asymptotic result that will feed into the eventual proof of Theorem 5B in Section 5.3.3. The result, and its proof, is similar to the analogous result for symplectic groups (see Proposition 4.3.23).

Proposition 5.3.14. *Let (G_i) be a sequence in $\mathcal{A}$ with $\mathrm{soc}(G_i) = \mathrm{P}\Omega^{\varepsilon_i}_{2m_i}(q_i)$. For all i, assume that $G_i \not\leqslant \mathrm{PGO}^{\varepsilon_i}_{2m_i}(q_i)$ and $G_i \cap \mathrm{PGO}^{\varepsilon_i}_{2m_i}(q) \leqslant \mathrm{PDO}^{\varepsilon_i}_{2m_i}(q_i)$. Then $u(G_i) \to \infty$ if $m_i \to \infty$.*

Proof. Fix $G_i = G = \langle T, \theta \rangle$ with $T = \mathrm{P}\Omega^{\varepsilon}_{2m}(q)$. The conditions $G \not\leqslant \mathrm{PGO}^{\varepsilon}_{2m}(q)$ and $G \cap \mathrm{PGO}^{\varepsilon}_{2m}(q) \leqslant \mathrm{PDO}^{\varepsilon}_{2m}(q)$ imply that we are in Case II(a) and we can, therefore, use the notation from earlier in this section. In particular, by Proposition 5.1.12, we may assume that θ appears in Table 5.1.

We apply Lemma 2.1.1. Assume that m is large enough so that we may fix a positive integer d for which $1 \leqslant \sqrt{2m}/8 < d < \sqrt{2m}/4$ and $m - d$ is odd. Let $y \in \mathrm{PDO}^{\eta}_{2m}(q_0)$ have type ${}^{a}(2d)^{-} \perp {}^{b}(2m-2d)^{-\eta}$. By the proof of Proposition 5.3.5, there exists $t \in T$ such that $t\theta$ is X-conjugate to y.

The $\mathcal{C}_1$ subgroups of G containing $t\theta$ are one of type $\mathrm{O}^{v}_{2d}(q) \times \mathrm{O}^{\varepsilon v}_{2m-2d}(q)$ and, if $\eta = -$, two of type P_{m-d} (see the proof of Proposition 5.3.9). There are at most $4m$ types of maximal subgroup in each of $\mathcal{C}_2$, $\mathcal{C}_3$, $\mathcal{C}_4$, $\mathcal{C}_7$ and at most $1 + \log\log q$ in $\mathcal{C}_5$. Moreover, by Lemma 2.7.11 and Proposition 5.3.8, there are at most $(q_0^d + 1)(q_0^{m-d} + \eta) \leqslant 2q^{m/2}$ subgroups of each type in $\mathcal{M}(G, t\theta)$. Now $\mathcal{C}_6$ and $\mathcal{C}_8$ are empty and, since a power z of y has type $(2d)^{-} \perp I_{2m-2d}$ and satisfies $\nu(z) = 2d < \sqrt{2m}/2$, Theorem 2.5.14 implies that $\mathcal{M}(G, t\theta)$ contains no subgroups from $\mathcal{S}$.

Now Theorem 3.1.1 and Proposition 3.2.4 imply that for all prime order elements $x \in G$,

$$P(x, t\theta) \leqslant \frac{11}{q^{m-2}} + \frac{1}{q^{\sqrt{2m}/4}} + \frac{1}{q^{m-\sqrt{2m}/4-1}} + (16m + 1 + \log\log q) \cdot 2q^{m/2} \cdot \frac{2}{q^{m-3}} \to 0$$

as $m \to \infty$. Therefore, $u(G) \to \infty$ as $m \to \infty$. □

5.3.2 Case II(b)

Element selection

For Case II(b), we cannot select an element $t\theta \in T\theta$ by directly considering a Shintani map as we did in Case II(a). Indeed, this is precisely the reason for the distinction between Cases II(a) and II(b). Nevertheless, we can use Shintani descent indirectly to select appropriate elements in $T\theta$ by applying Lemma 2.7.13 (see Example 2.7.14).

Notation 5.3.15. Write $q = p^f$ where $f \geqslant 2$.

Let $V = \mathbb{F}_q^{2m}$ be the natural module for $\mathrm{O}^+_{2m}(q)$.

Fix the simple algebraic group

$$X = \begin{cases} \Omega_{2m}(\overline{\mathbb{F}}_2) & \text{if } p = 2 \\ \mathrm{PSO}_{2m}(\overline{\mathbb{F}}_p) & \text{if } p \text{ is odd.} \end{cases}$$

Fix the standard Frobenius endomorphism $\varphi = \varphi_{\mathcal{B}^+}$ of X, defined with respect to the standard basis $\mathcal{B}^+$, as $(a_{ij}) \mapsto (a_{ij}^p)$, modulo scalars.

With respect to the $\mathcal{B}^+$, write $V_E = \langle e_1, \ldots, e_{m-1} \rangle$ and $V_F = \langle f_1, \ldots, f_{m-1} \rangle$. With respect to the decomposition

$$V = (V_E \oplus V_F) \perp \langle e_m, f_m \rangle$$

recall that $r = I_{2m-2} \perp r^+$ and $\delta = \delta^+ = (\beta I_{m-1} \oplus I_{m-1}) \perp [\beta, 1]$, where, in the latter case q is odd and $\beta \in \mathbb{F}_q^\times$ has order $(q-1)_2$.

Fix $Z_1 = X_{(\langle e_m, f_m \rangle)} \cong \mathrm{SO}_{2m-2}(\overline{\mathbb{F}}_p)$ and $Z_2 = (Z_1)_{(V_E \oplus V_F)} \cong \mathrm{GL}_{m-1}(\overline{\mathbb{F}}_p)$, so Z_1 acts trivially on $\langle e_m, f_m \rangle$ and $Z_2 \leqslant Z_1$ centralises $V_E \oplus V_F$.

By Proposition 5.1.12, assume $\theta \in \mathrm{PGO}^+_{2m}(q)\varphi^i$ if $\varepsilon = +$ and $\theta \in \mathrm{PGO}^-_{2m}(q)\psi^i$ if $\varepsilon = -$.

Notation 5.3.15. (continued) Write $q = q_0^e$ and $e = f/i$.

Fix (σ, γ, d, Z) as follows, where $\Delta = \delta\delta^{\sigma^{-1}}\delta^{\sigma^{-2}} \cdots \delta^{\sigma^{-(e-1)}}$

ε	θ	σ	γ	d	Z
$+$	$\iota r\varphi^i$	$r\varphi^i$	r	2	Z_1
	$\iota\delta^- r\varphi^i$	$\delta r\varphi^i$	$r\Delta^{-1}$	$2(q_0-1)_2$	Z_2
$-$	$\iota\psi^i$	φ^i	r	2	Z_1
	$\iota\delta^-\psi^i$	$\delta\varphi^i$	$r\Delta^{-1}$	$2(q_0-1)_2$	Z_2

Table 5.6: Case II(b): The element y for the automorphism θ

Generic case	
$m \pmod 4$	y
0 or 2	${}^a(2m-2)^+ \perp {}^a r^\varepsilon$
1	${}^a(m-3)^+ \perp {}^a(m+1)^+ \perp {}^a r^\varepsilon$
3	${}^a(m-5)^+ \perp {}^a(m+3)^+ \perp {}^a r^\varepsilon$

Specific cases		
m	θ	y
5 or 7	$\imath r\varphi^i, \imath\psi^i$	$(4)^- \perp (2m-6)^- \perp r^\varepsilon$
	$\imath\delta r\varphi^i, \imath\delta\psi^i$	$D^+_{2m-2} \perp {}^\Delta r^\varepsilon$

[we describe y by specifying its type over $\mathbb{F}_{q_0}$, D^+_{2m-2} is defined in Remark 5.3.18(ii)]

Remark 5.3.16. Let us comment on Notation 5.3.15.

(i) Note that Z_1 and Z_2 are connected φ-stable subgroups of X.

(ii) We have $Z_1 \leqslant C_X(r)$ since the map r is supported on $\langle e_m, f_m\rangle$.

(iii) If q is odd, then $Z_2 \leqslant C_{Z_1}(\delta|_{V_E\oplus V_F})$ since $\delta|_{V_E\oplus V_F}$ centralises the decomposition $V_E \oplus V_F$ and acts as a scalar on each summand.

(iv) The automorphisms ψ and δ^- of $\mathrm{P}\Omega^-_{2m}(q)$, where q is odd in the latter case, were introduced in (2.21) and Definition 5.1.5.

(v) Write $\widetilde{\sigma} = \sigma|_{X_{\gamma\sigma^e}}$ and $\widetilde{\gamma} = \gamma|_{X_{\gamma\sigma^e}}$. Observe that $X_{\gamma\sigma^e}\widetilde{\sigma} = \mathrm{PDO}^\varepsilon_{2m}(q)\theta$, noting that when $\varepsilon = -$ we are making the usual identifications justified by the isomorphism $\Psi\colon X_{r\varphi^f} \to \mathrm{PDO}^-_{2m}(q)$ given in Lemma 2.6.17 (see Remark 5.3.2(iii)).

We now choose the elements for Case II(b) in the following proposition (see Remark 5.1.13 for an explanation of the statement and Table 5.6).

Proposition 5.3.17. *Let $T = \mathrm{P}\Omega^\varepsilon_{2m}(q)$ and let θ be an automorphism from Table 5.1 (in Case II(iii) or (v)). If y is the element in Table 5.6, then there exists $t \in T$ that centralises the decomposition $\langle e_1, \dots, f_{m-1}\rangle \perp \langle e_m, f_m\rangle$ such that $(t\theta)^e$ is X-conjugate to y. Moreover, if $H \leqslant G$, then the number of G-conjugates of H that contain $t\theta$ is at most $|C_{\mathrm{PDO}^{-\varepsilon}_{2m}(q_0)}(y^d)|$.*

Proof. In each case, $(\gamma\sigma^e)^d = \sigma^{ed}$. For instance, if $\varepsilon = +$ and $\theta = \imath\delta r\varphi^i$, then

$$(\gamma\sigma^e)^d = (r\Delta^{-1}\Delta(r\varphi^i)^e)^d = (\varphi^f)^{2(q_0-1)_2} = (\varphi^{2f})^{(q_0-1)_2}$$

and

$$\sigma^{ed} = (\delta r\varphi^i)^{ed} = (\Delta(r\varphi^i)^e)^d = (\Delta r\varphi^f)^d = (\Delta\Delta^r\varphi^{2f})^{(q_0-1)_2} = (\varphi^{2f})^{(q_0-1)_2}.$$

It is also easy to verify that $y\widetilde{\gamma} \in Z_\sigma$. Therefore, Lemma 2.7.13 implies that there exists $g \in Z_{\sigma^e} \leqslant \mathrm{PSO}^\varepsilon_{2m}(q) \leqslant X_{\gamma\sigma^e}$ such that $(g\widetilde{\sigma})^e$ is X-conjugate (indeed Z-conjugate) to y and if $H \leqslant G$, then the number of conjugates of H that contain $g\widetilde{\sigma}$ is at most $|\mathrm{C}_{\mathrm{PDO}^{-\varepsilon}_{2m}(q_0)}(y^d)|$.

If $q^m \not\equiv \varepsilon \pmod 4$, then $\mathrm{PSO}^\varepsilon_{2m}(q) = T$ and $\widetilde{\sigma} = \theta$, so $g\widetilde{\sigma} \in T\theta$, as required (see (2.9)). Otherwise, $g \in \mathrm{PSO}^\varepsilon_{2m}(q) = T \cup Tr_\square r_\boxtimes$, so we may choose $\theta \in \{\widetilde{\sigma}, \iota\widetilde{\sigma}\}$ such that $g\widetilde{\sigma} \in T\theta$, which is sufficient to prove the claim. □

Remark 5.3.18. We comment on the definition of $t\theta$ when $m \in \{5, 7\}$.

(i) Let q be odd and let $\theta \in \{\iota\delta r\varphi^i, \iota\delta\psi^i\}$. We need to define D^+_{2m-2}. We define D^+_{2m-2} to be an element $\beta A \perp A^{-\mathsf{T}}$ where A is an irreducible element, whose order is a primitive prime divisor of $q_0^{m-1} - 1$. This is like, but not exactly the same as, an element of type ${}^\Delta(2m-2)^+$ (which does not exist when m is odd).

(ii) Let $m = 5$ and let $\theta \in \{\iota r\varphi^i, \iota\psi^i\}$. By Table 5.6, $y = y_1 \perp y_2 \perp r^-$, centralising a decomposition $\mathbb{F}^{10}_{q_0} = U_1 \perp U_2 \perp U_3$, where y_1 and y_2 both have type ${}^\Delta(4)^-$. By Lemma 2.3.15, we can fix a primitive prime divisor ℓ of $q_0^4 - 1$ that is strictly greater than 5. Let Λ be the set of elements of order ℓ in $\mathbb{F}^\times_{q_0}$. Then $|\Lambda| \geqslant 8$, so we can, and will, assume that y_1 and y_2 have distinct sets of eigenvalues. This implies that U_1 and U_2 are nonisomorphic $\mathbb{F}_{q_0}\langle y\rangle$-modules.

Probabilistic method

Continue to let T be the simple group $\mathrm{P}\Omega^\varepsilon_{2m}(q)$ and let θ be an automorphism from Table 5.1. Fix the element y from Table 5.6 and $t\theta \in G = \langle T, \theta\rangle$ from Proposition 5.3.17. The following result describes $\mathcal{M}(G, t\theta)$.

Theorem 5.3.19. *The maximal subgroups of G which contain $t\theta$ are listed in Tables 5.7 and 5.8, where $m(H)$ is an upper bound on the multiplicity of the subgroups of type H in $\mathcal{M}(G, t\theta)$.*

Theorem 5.3.19 will be proved in parts. As before, write $\widetilde{G} = \langle X_{\sigma^e}, \widetilde{\sigma}\rangle$. We will make use of Proposition 5.3.8 in this section. We begin with reducible subgroups.

Proposition 5.3.20. *Theorem 5.3.19 is true for reducible subgroups.*

Proof. Let us divide this proof into four parts.

Part 1: Setup

Let $\mathcal{D}$ be the decomposition

$$V = V_1 \perp V_2 \quad \text{where} \quad V_1 = \langle e_1, \ldots, f_{m-1}\rangle \quad \text{and} \quad V_2 = \langle e_m, f_m\rangle.$$

Observe that θ centralises $\mathcal{D}$, and write $\theta_i = \theta|_{V_i}$. By Proposition 5.3.17, t also centralises $\mathcal{D}$, so we may write $t\theta = t_1\theta_1 \perp t_2\theta_2$ with respect to $\mathcal{D}$. Let us also write $y = y_1 \perp {}^a r^\varepsilon$. We begin by studying the $\langle t_i\theta_i\rangle$-invariant subspaces of V_i.

Table 5.7: Case II(b): Description of $\mathcal{M}(G, t\theta)$ for $m \notin \{5, 7\}$

	type of H	$m(H)$	conditions	
$\mathcal{C}_1$			$m \pmod 4$	q
	$\mathrm{O}_2^v(q) \times \mathrm{O}_{2m-2}^{\varepsilon v}(q)$	1		
	$\mathrm{Sp}_{2m-2}(q)$	1		even
	$\mathrm{O}_{2m-1}(q)$	2		odd
	P_{m-1}	2	even	
		4	odd	
	$\mathrm{O}_{m-3}^v(q) \times \mathrm{O}_{m+3}^{\varepsilon v}(q)$	1	1	
	$\mathrm{O}_{m-2} \times \mathrm{O}_{m+2}$	2	1	odd
	$\mathrm{O}_{m-1}^v(q) \times \mathrm{O}_{m+1}^{\varepsilon v}(q)$	1	1	
	$P_{(m-3)/2}$	2	1	
	$P_{(m+1)/2}$	2	1	
	$\mathrm{O}_{m-5}^v(q) \times \mathrm{O}_{m+5}^{\varepsilon v}(q)$	1	3	
	$\mathrm{O}_{m-4} \times \mathrm{O}_{m+4}$	2	3	odd
	$\mathrm{O}_{m-3}^v(q) \times \mathrm{O}_{m+3}^{\varepsilon v}(q)$	1	3	
	$P_{(m-5)/2}$	2	3	
	$P_{(m+3)/2}$	2	3	
$\mathcal{C}_2$	$\mathrm{O}_{2m/k}^v(q) \wr S_k$	N	$k \mid m,\ k > 1,\ v^k \in \varepsilon$	
	$\mathrm{O}_{2m/k}(q) \wr S_k$	N	$k \mid 2m,\ 2m/k > 1$ odd	
	$\mathrm{GL}_m(q)$	N	m odd, $\varepsilon = +$	
$\mathcal{C}_5$	$\mathrm{O}_{2m}^v(q^{1/k})$	N	$k \mid f,\ k$ is prime, $v^k = \varepsilon$	

[$N = |C_{\mathrm{PDO}_{2m}^{-\varepsilon}(q_0)}(y^2)|$, in $\mathcal{C}_1$ there is a unique choice of v]

Part 2: Subspaces of V_1

Let U_1 be a $\langle t_1\theta_1 \rangle$-invariant subspace of V_1. The key part of the proof of Lemma 2.7.13 gives us that $F(t_1\theta_1) = y_1$, where F is the Shintani map of (Z, σ, e). Therefore, we can use Lemma 2.7.9 applied to F.

For the sake of exposition, let us assume that $m \geqslant 9$ and $m \equiv 1 \pmod 4$; the other cases are very similar and we comment on them below. In this case, the element y_1 has type ${}^a(m-3)_{q_0}^+ \perp {}^a(m+1)_{q_0}^+$, where a is empty or Δ. Write $S = \langle e_1, \ldots, f_{m-1} \rangle_{\mathbb{F}_{q_0}}$. Then y_1 centralises a decomposition $S = (S_1 \oplus S_2) \perp (S_3 \oplus S_4)$, where the S_i are pairwise nonisomorphic irreducible $\mathbb{F}_{q_0}\langle y_1 \rangle$-modules (here $\dim S_1 = \dim S_2 = \frac{m-3}{2}$ and $\dim S_3 = \dim S_4 = \frac{m+1}{2}$). Therefore, by Lemma 2.3.3, the only $\langle y_1 \rangle$-invariant subspaces of W are direct sums of S_1, S_2, S_3 and S_4.

Table 5.8: Case II(b): Description of $\mathcal{M}(G, t\theta)$ for $m \in \{5, 7\}$

	type of H	$m(H)$	conditions		
$\mathcal{C}_1$			θ	m	q
	$\mathrm{O}_2^v(q) \times \mathrm{O}_{2m-2}^{\varepsilon v}(q)$	1			
	$\mathrm{O}_{2m-1}(q)$	2			odd
	$\mathrm{Sp}_{2m-1}(q)$	1			even
	P_{m-1}	2	$\iota\delta r\varphi^i$ or $\iota\delta\psi^i$		
	$\mathrm{O}_4^v(q) \times \mathrm{O}_{2m-4}^{\varepsilon v}(q)$	1	$\iota r\varphi^i$ or $\iota\psi^i$		
	$\mathrm{O}_6^v(q) \times \mathrm{O}_{2m-6}^{\varepsilon v}(q)$	1	$\iota r\varphi^i$ or $\iota\psi^i$		
	$\mathrm{O}_5(q) \times \mathrm{O}_7(q)$	2	$\iota r\varphi^i$ or $\iota\psi^i$	7	odd
$\mathcal{C}_2$	$\mathrm{O}_2^-(q) \wr S_m$	N	e is even, $\varepsilon = -$ ($e = 2$ only if $m = 5$ and $\theta \in \{\iota r\varphi^i, \iota\psi^i\}$)		
	$\mathrm{O}_m(q) \wr S_2$	N	q is odd		
$\mathcal{C}_3$	$\mathrm{O}_m(q^2)$	N	$\theta \in \{\iota\delta r\varphi^i, \iota\delta\psi^i\}$, e is odd		
	$\mathrm{GU}_m(q)$	N	$\theta \in \{\iota\delta r\varphi^i, \iota\delta\psi^i\}$, e is odd, $\varepsilon = -$		
$\mathcal{C}_5$	$\mathrm{O}_{2m}^v(q^{1/k})$	N	$k \mid f$, k is prime, $v^k = \varepsilon$		

$$[\, N = |C_{\mathrm{PDO}_{2m}^{-\varepsilon}(q_0)}(y^2)| \,]$$

We now proceed as in the proof of Proposition 4.3.9 (see that proof for more details). Lemma 2.7.9 establishes that the only possibilities for U_1 are direct sums of four pairwise nonisomorphic irreducible $\langle t\theta_1\rangle$-invariant subspaces $U_{1,1}$, $U_{1,2}$, $U_{1,3}$ and $U_{1,4}$ (where $\dim U_{1,1} = \dim U_{1,2} = \frac{m-3}{2}$ and $\dim U_{1,3} = \dim U_{1,4} = \frac{m+1}{2}$). Moreover, we can deduce that these subspaces are totally singular but $U_{1,1} \oplus U_{1,2}$ and $U_{1,3} \oplus U_{1,4}$ are nondegenerate.

The other cases are very similar. In all cases U_1 is a direct sum of pairwise nonisomorphic irreducible $\mathbb{F}_q\langle y_1\rangle$-submodules of dimension at least three. In particular, this implies that

$$\dim V_1 - \dim U_1 \notin \{1, 2\}. \tag{5.8}$$

Part 3: Subspaces of V_2

Next let U_2 be a $\langle t_2\theta_2\rangle$-invariant subspace of V_2. Note that a power of $t_2\theta_2$ is ${}^a r^\varepsilon$. Therefore, if q is even, then Lemma 5.2.2 implies that there is at most one proper nonzero $\mathbb{F}_q\langle t_2\theta_2\rangle$-invariant subspace of V_2. Similarly, if q is odd, then Lemma 5.2.3 implies that there are at most two $\mathbb{F}_q\langle t_2\theta_2\rangle$-invariant proper nonzero subspaces of V_2.

Part 4: Subspaces of V

Now let U be a $\langle t\theta\rangle$-invariant subspace of V. Let $\pi_i \colon U \to V_i$ be the projection map of U onto V_i. Then $U_i = \pi_i(U)$ is a $\langle t_i\theta_i\rangle$-invariant subspace of V_i.

Suppose that $U_2 \neq 0$ and $U_2 \not\leqslant U$. We mimic the proof of Lemma 2.3.1. Let $W_i = U \cap U_i$. Let $u_1 \in U_1$ and let $u_2, v_2 \in U_2$ satisfy $u_1 + u_2 \in U$ and $u_1 + v_2 \in U$. Then $u_2 - v_2 \in U$, so $u_2 - v_2 \in W_2$. Therefore, there is a well-defined function $L\colon U_1 \to U_2/W_2$ where $L(u_1) = \{u_2 \in U_2 \mid u_1 + u_2 \in U\}$.

If $u_1, v_1 \in U_1$ and $u_2, v_2 \in U_2$ satisfy $u_1 + u_2 \in U$ and $v_1 + v_2 \in U$, then for all $\lambda \in \overline{\mathbb{F}}_q$ we have $(u_1 + u_2) + \lambda(v_1 + v_2) = (u_1 + \lambda v_1) + (u_2 + \lambda v_2)$, so

$$L(u_1 + \lambda v_1) = W + (u_2 + \lambda v_2) = L(u_1) + \lambda L(v_1).$$

Therefore, L is linear.

For $u_1 \in U_1$, $L(u_1) = W_2$ if and only if $u_1 \in U$, so $\ker L = W_1$. Since $U_2 \not\leqslant U$ we know that $U_2/W_2 \neq 0$. This implies that $\dim W_1 = \dim U_1 - \dim U_2/W_2 \in \{2m-3, 2m-4\}$. However, W_1 is a $\langle t_1\theta_1\rangle$-invariant subspace of V_1 and (5.8) implies that V_1 does not have a $\langle t_1\theta_1\rangle$-invariant subspace of dimension $2m-3$ or $2m-4$, so we have obtained a contradiction.

Therefore, either $U_2 = 0$ or $U_2 \leqslant U$. This implies that $U = U_1 \oplus U_2$, the possibilities for which follow from Parts 2 and 3. These exactly correspond to the subgroups given in Tables 5.7 and 5.8. □

We now turn to irreducible subgroups.

Proposition 5.3.21. *Theorem 5.3.19 is true for irreducible subgroups when $m \notin \{5, 7\}$.*

Proof. By construction, a suitable power of $t\theta$ is X-conjugate to y. We begin by demonstrating that we can fix a power z of y satisfying $|z| = 2$ and $1 \leqslant \nu(z) \leqslant 2$. If $(\varepsilon, \theta) \in \{(+, \imath r\varphi^i), (-, \imath\psi^i)\}$, then a power z of y has type $I_{2m-2} \perp r^\varepsilon$ and evidently $\nu(z) = 1$. Otherwise $(\varepsilon, \theta) \in \{(+, \imath\delta r\varphi^i), (-, \imath\delta\psi^i)\}$ and raising $y^{(q-1)_2}$ to a suitable power gives an element of type $I_{2m-2} \perp -I_2$ and $\nu(z) = 2$.

Let $H \in \mathcal{M}(G, t\theta)$ be irreducible. We proceed as in the proof of Proposition 5.3.12, using Theorem 2.5.1. In particular, let us quickly handle the cases that are essentially identical to those in that previous proof. Observe that $\mathcal{C}_6$ and $\mathcal{C}_8$ are empty, z is not contained in an $\mathcal{S}$ family subgroup by Theorem 2.5.14 and $\mathcal{C}_5$ subgroups have type $\mathrm{O}^v_{2m}(q_1)$ where $q = q_1^k$ for a prime k and a sign $v \in \{+, -\}$ such that $v^k = \varepsilon$.

The possible types of $\mathcal{C}_2$ subgroups are those given in Table 5.7 (see [43, Tables 3.5.E and 3.5.F]). The restriction on $\mathrm{GL}_m(q)$ subgroups arises for the reason given in the proof of Proposition 5.3.10 for $(\varepsilon, \eta) = (+, -)$.

Consider $\mathcal{C}_3$ subgroups. In this case, H is a field extension subgroup of type $\mathrm{O}^v_{2m/k}(q^k)$ or $\mathrm{GU}_m(q)$. Write $H \cap T = B.k$. Lemma 2.5.7(ii) implies that $z \in B$, and Lemma 2.5.7(i) implies that $k = 2$ since $\nu(z) \leqslant 2$. Now let w be a power of y of type $(2d)^+ \perp I_{2m-2d}$ where $d \in \{m-1, \frac{m+1}{2}, \frac{m+3}{2}\}$ is odd. Lemma 2.5.7(ii) implies that $w \in B$ and Corollary 2.5.9 implies that $z \notin B$ since d is odd, which is a contradiction. Therefore, $H \notin \mathcal{C}_3$.

For $\mathcal{C}_4$ subgroups, suppose that H is the centraliser of a decomposition $V_1 \otimes V_2$ where $\dim V_1 \geqslant \dim V_2 > 1$. Since $z \in H$, we may write $z = z_1 \otimes z_2$. If $\nu(z) = 1$, then we have a contradiction to Lemma 2.5.13. Otherwise $z = -I_2 \perp I_{2m-2}$ and we quickly deduce that $\varepsilon = +$, H has type $\mathrm{Sp}_2(q) \otimes \mathrm{Sp}_m(q)$ and $\nu(z_1) = 1$, which is not possible. Therefore, $H \notin \mathcal{C}_4$.

For $\mathcal{C}_7$ subgroups we may assume that $\varepsilon = +$. Suppose that $H = B.S_k$ is the stabiliser of a decomposition $U_1 \otimes U_2 \otimes \cdots \otimes U_k$. From the previous paragraph, $z \notin B$. However, Lemma 2.5.11 implies that z does not cyclically permute the k factors, which is a contradiction. Therefore, $H \notin \mathcal{C}_7$.

To complete the proof, we note that the stated upper bounds on the multiplicities of nonsubspace subgroups follow from Propositions 5.3.8 and 5.3.17. □

Proposition 5.3.22. *Theorem 5.3.19 is true for irreducible subgroups when $m \in \{5, 7\}$.*

Proof. Let $H \in \mathcal{M}(G, t\theta)$ be irreducible. We proceed as in the proof of the previous proposition. In particular, note that a power z of y satisfies $\nu(z) \leqslant 2$, so by Theorem 2.5.14 $H \notin \mathcal{S}$. Therefore, H is a geometric subgroup and by considering the possible types we see that it suffices to consider subgroups in $\mathcal{C}_2$, $\mathcal{C}_3$ and $\mathcal{C}_5$. The result is clear for $\mathcal{C}_5$ subgroups. Note also that the multiplicities, as usual, follow from Propositions 5.3.8 and 5.3.17.

First assume that H has type $\mathrm{O}_2^\varepsilon(q) \wr S_m$ stabilising a decomposition $\mathcal{D}$ of V into m nondegenerate 2-spaces. If e is odd, then a power of y has one of the following types:

$$I_2 \perp (4)_q^- \perp (2m-6)_q^-, \quad I_2 \perp (8)_q^+, \quad I_2 \perp (12)_q^+, \quad I_2 \perp (6)_q^+ \perp (6)_q^+.$$

By Lemma 2.5.6, y must centralise $\mathcal{D}$, which is a contradiction, since elements of these types act irreducibly on a space of dimension strictly greater than 2. Therefore, e is even. Now assume that $m = 7$ or $\theta \in \{\iota\delta r_\square \varphi^i, \iota\delta\psi^i\}$. If $e = 2$, then a power of y has one of the following types

$$I_6 \perp (4)_q^- \perp (4)_q^-, \quad I_2 \perp (4)_q^+ \perp (4)_q^+, \quad I_2 \perp (6)_q^+ \perp (6)_q^+,$$

and again we obtain a contradiction.

Next assume that $\varepsilon = +$ and H has type $\mathrm{GL}_m(q)$. Let H be the stabiliser of the decomposition $V = V_1 \oplus V_2$, where V_1 and V_2 are maximal totally singular subspaces of V. Record that e is odd since $\varepsilon = +$. If $\theta \in \{\iota r\varphi^i, \iota\psi^i\}$, then a power of y has type $I_2 \perp (4)_q^- \perp (2m-6)_q^-$, noting that $2m - 6 \in \{4, 8\}$, so y has odd order and does not stabilise a maximal totally singular subspace, which is a contradiction. Now assume that $\theta \in \{\iota\delta r_\square \varphi^i, \iota\delta\psi^i\}$. In this case, y has type ${}^\Delta r \perp {}^\Delta(2m-2)_{q_0}^+$. Therefore, y has type $M \perp (8)_q^+$ or $M \perp (6)_q^+ \perp (6)_q^+$, depending on whether m is 5 or 7, where M acts irreducibly on a 2-space (see Lemma 5.2.3). Now y^2 centralises the decomposition and we may assume that $U \subseteq V_1$, where U is a totally singular subspace of dimension 4 or

3 that is stabilised by y^2 and on which y^2 acts irreducibly. However, U is stabilised by y, so y stabilises V_1 and hence centralises the decomposition. However, since M is irreducible, y does not stabilise a maximal totally singular subspace, which is a contradiction. Therefore, $t\theta$ is not contained in a subgroup of type $\mathrm{GL}_m(q)$.

Now we may assume that H is a $\mathcal{C}_3$ subgroup. If $\theta \in \{\imath r\varphi^i, \imath\psi^i\}$, then a power z of y satisfies $\nu(z) = 1$, so y is not contained in H (see Lemma 2.5.7). Now assume $\theta \in \{\imath\delta r\varphi^i, \imath\delta\psi^i\}$ and H has type $\mathrm{O}_m(q)$ or $\mathrm{GU}_m(q)$. Note that $\varepsilon = -$ in the latter case (see [43, Table 3.5.E]). Since y has type ${}^{\Delta}(2m-2)^+_{q_0} \perp {}^{\Delta}r_{q_0}$, y has exactly two eigenvalues, λ and $-\lambda$, of order $2(q_0+1)_2$. Lemma 2.5.7 implies that y arises from an element $g \in \mathrm{CU}_m(q^2)$ (see Remark 2.2.3) or $\mathrm{GO}_m(q^2)$ with exactly one eigenvalue of order $2(q_0+1)_2$. Therefore, $\lambda^q = -\lambda$, so e is odd. This completes the proof. □

We have now proved Theorem 5.3.19 and are, consequently, in the position to prove Theorem 5A in Case II(b). We consider two cases depending on whether $m \in \{5,7\}$.

Proposition 5.3.23. *Let $G = \langle T, \theta\rangle \in \mathcal{A}$ where $T = \mathrm{P\Omega}^{\varepsilon}_{2m}(q)$ and $\theta \notin \mathrm{PGO}^{\varepsilon}_{2m}(q)$. In Case II(b) when $m \notin \{5,7\}$,*

(i) $u(G) \geqslant 2$

(ii) $u(G) \to \infty$ *as* $q \to \infty$.

Proof. Let $x \in G$ have prime order. Theorem 5.3.19 gives a superset of $\mathcal{M}(G, t\theta)$. Using the fixed point ratios from Theorem 3.1.1 and Proposition 3.2.4(i), we will prove that $P(x, t\theta) < \frac{1}{2}$ and $P(x, t\theta) \to 0$ as $q \to \infty$. For brevity, we will not explicitly note that $P(x, t\theta) \to 0$ as $q \to \infty$ separately in each case. Write $d(n)$ for the number of proper divisors of n.

Case 1: m is even

In this case,

$$P(x, t\theta) \leqslant \frac{(2, q-1)}{q} + \frac{1}{q^2} + \frac{20}{q^{m-2}} + (1 + \log\log q + 2d(2m)) \cdot (q_0+1)(q_0^{m-1} - 1) \cdot \frac{2}{q^{m-2}},$$

so $P(x, t\theta) < \frac{1}{2}$ unless either $(m, q) \in \{(4,8), (4,27), (6,8)\}$, or $e = f = 2$ and $m \leqslant 10$.

Consider the former case. The unique type of $\mathcal{C}_5$ subgroup is $\mathrm{O}^{\varepsilon}_{2m}(p)$. First assume $m = 6$ and $q = 8$, then a suitable power z of y has type $10^+_2 \perp I_2 = 10^+_8 \perp I_2$, which has odd prime order and acts irreducibly on a totally singular 5-space. This implies that z, and hence $t\theta$, is not contained in a $\mathcal{C}_2$ subgroup. Therefore, in this case,

$$P(x, t\theta) \leqslant \frac{1}{8} + \frac{1}{8^2} + \frac{20}{8^4} + (2+1)(2^5 - 1) \cdot \frac{2}{8^4} < \frac{1}{2}.$$

Next assume that $m = 4$ and $q \in \{8, 27\}$, so $\varepsilon = -$. The subgroups of type $\mathrm{O}^-_8(p)$ are the only nonsubspace subgroups containing $t\theta$. By Proposition 3.2.4, for subgroups H of

this type we have $\mathrm{fpr}(x, G/H) < 3/q^3$ provided that $\nu(x) \neq 1$ and a direct calculation demonstrates that this bound also holds when $\nu(x) = 1$ in this case (see Proposition 3.2.8). With this, together with better bounds extracted from Theorem 3.1.1, we obtain

$$P(x, t\theta) \leqslant \frac{(2, q-1)}{q} + \frac{9}{q^2} + \frac{14}{q^3} + (q_0+1)(q_0^3-1) \cdot \frac{3}{q^3} < \frac{1}{2}.$$

Now assume that $e = f = 2$ and $m \in \{4, 6, 8, 10\}$. Here $\varepsilon = -$ since e is even. Therefore, since $f = 2$, G has no $\mathcal{C}_5$ subgroups. We will now show that $t\theta$ is not contained in any $\mathcal{C}_2$ subgroups. Note that $D(Q) = \boxtimes$ since $q^m \equiv 1 \pmod 4$, so any $\mathcal{C}_2$ subgroup has type $\mathrm{O}^-_{2m/k}(q) \wr S_k$ where k is odd and $2m/k$ is even (see [43, Table 3.5.F]). If $m \in \{4, 8\}$, then no such subgroups arise. Now assume that $m \in \{6, 10\}$. The unique possible type of $\mathcal{C}_2$ subgroup is $\mathrm{O}^-_4(q) \wr S_{m/2}$. A power z of y has type $(2m-2)^+_{q_0} \perp I_2 = (2m-2)^+_q \perp I_2$ since $e = 2$ and $m-1$ is odd (see Lemma 2.3.36). By Lemma 2.5.6, z must centralise a decomposition $U_1 \perp \cdots \perp U_{m/2}$ where $\dim U_i = 4$, which is impossible since y acts irreducibly on a totally singular subspace of dimension $m - 1 \geqslant 5$. Therefore, $t\theta$ is contained in no nonsubspace subgroups. Accordingly,

$$P(x, t\theta) \leqslant \frac{(2, q-1)}{q} + \frac{1}{q^2} + \frac{20}{q^{m-2}},$$

so $P(x, t\theta) < \frac{1}{2}$ unless $(m, q) = (4, 4)$. If $T = \Omega^-_8(4)$, then $\theta = \psi$ and we can verify that $P(x, t\theta) < \frac{1}{2}$ in MAGMA (see Section 2.8).

Case 2: m is odd

If $m \equiv 1 \pmod 4$ and $m \geqslant 9$, then

$$\begin{aligned} P(x, t\theta) \leqslant{}& \frac{(2, q-1)}{q} + \frac{1}{q^2} + \frac{2}{q^{(m-3)/2}} + \frac{6}{q^{(m-1)/2}} + \frac{56}{q^{m-3}} \\ &+ (1 + \log\log q + 2d(2m) + q) \cdot (q_0+1)(q_0^{(m-3)/2}-1)(q_0^{(m+1)/2}-1) \cdot \frac{2}{q^{m-2}}, \end{aligned}$$

which proves that $P(x, t\theta) < \frac{1}{2}$ unless $(m, q) = (9, 4)$. In this exceptional case, $\varepsilon = -$ since e is even, so the only nonsubspace subgroup to arise has type $\mathrm{O}^-_2(q) \wr S_9$, so

$$P(x, t\theta) \leqslant \frac{1}{4} + \frac{1}{4^2} + \frac{2}{q^3} + \frac{6}{4^4} + \frac{56}{4^6} + (2+1)(2^3-1)(2^5-1) \cdot \frac{2}{4^7} < \frac{1}{2}.$$

If $m \equiv 3 \pmod 4$ and $m \geqslant 11$, then

$$\begin{aligned} P(x, t\theta) \leqslant{}& \frac{(2, q-1)}{q} + \frac{1}{q^2} + \frac{2}{q^{(m-5)/2}} + \frac{6}{q^{(m+1)/2}} + \frac{56}{q^{m-5}} \\ &+ (1 + \log\log q + 2d(2m) + q) \cdot (q_0+1)(q_0^{(m-5)/2}-1)(q_0^{(m+3)/2}-1) \cdot \frac{2}{q^{m-2}}, \end{aligned}$$

which proves that $P(x, t\theta) < \frac{1}{2}$ unless $(m, q) = (11, 4)$. In this case, as above, $\varepsilon = -$, the only type of nonsubspace subgroup to occur is $\mathrm{O}^-_2(q) \wr S_{11}$ and adjusting the bound accordingly demonstrates that $P(x, t\theta) < \frac{1}{2}$. This completes the proof. □

Proposition 5.3.24. *Let $G = \langle T, \theta \rangle \in \mathcal{A}$ where $T = \mathrm{P}\Omega^{\varepsilon}_{2m}(q)$ and $\theta \notin \mathrm{PGO}^{\varepsilon}_{2m}(q)$. In Case II(b) when $m \in \{5, 7\}$,*

(i) $u(G) \geqslant 2$

(ii) $u(G) \to \infty$ *as* $q \to \infty$.

Proof. Let $x \in G$ have prime order. We proceed as in the previous proof. Theorem 5.3.19 gives a superset of $\mathcal{M}(G, t\theta)$, Theorem 3.1.1 and Proposition 3.2.4 give bounds on the associated fixed point ratios, and we will use this information to prove that $P(x, t\theta) < \frac{1}{2}$ and $P(x, \theta) \to 0$ as $q \to \infty$.

Case 1: $\theta \in \{\iota\delta r\varphi^i, \iota\delta\psi^i\}$

In this case q is odd and

$$P(x, t\theta) \leqslant \frac{2}{q} + \frac{1}{q^2} + \frac{10}{q^{m-2}} + \frac{10}{q^{m-1}} + (3 + q + M) \cdot (q_0 + 1)(q_0^{m-1} - 1) \cdot \frac{2}{q^{m-2}},$$

where M is the number of types of subfield subgroups. Notice that

$$M \leqslant \begin{cases} 0 & \text{if } f \text{ is a power of 2} \\ 1 & \text{if } f \text{ is an odd prime power} \\ 1 + \log\log q & \text{otherwise} \end{cases}$$

where in the first case $\varepsilon = -$ since e is even. With this bound on M we see that $P(x, t\theta) < \frac{1}{2}$ unless $(m, q) \in \{(7, 3^2), (7, 5^2)\}$, or $m = 5$ and either $f = e = 3$ or $e = 2$. If $(m, q) \in \{(7, 3^2), (7, 5^2)\}$, then $t\theta$ is contained in no $\mathcal{C}_3$ or $\mathcal{C}_5$ subgroups; adjusting the bound on $P(x, t\theta)$ accordingly proves that $P(x, t\theta) < \frac{1}{2}$.

Next assume that $m = 5$ and $f = e = 3$. If $\varepsilon = +$, then there are no subgroups of type $\mathrm{GU}_m(q)$, so

$$P(x, t\theta) \leqslant \frac{2}{q} + \frac{1}{q^2} + \frac{10}{q^3} + \frac{10}{q^4} + 4 \cdot (q_0 + 1)(q_0^4 - 1) \cdot \frac{2}{q^3} < \frac{1}{2}.$$

Therefore, assume that $\varepsilon = -$. If $x \notin \mathrm{PGL}(V)$ or $\nu(x) \geqslant 2$, then by Proposition 3.2.4(ii)

$$P(x, t\theta) \leqslant \frac{2}{q} + \frac{1}{q^2} + \frac{10}{q^3} + \frac{10}{q^4} + (4 + q^2) \cdot (q_0 + 1)(q_0^4 - 1) \cdot \frac{3}{q^5} < \frac{1}{2},$$

while if $x \in \mathrm{PGL}(V)$ and $\nu(x) = 1$, then $\mathrm{fpr}(x, G/H) = 0$ for $\mathcal{C}_3$ subgroups H (see Lemma 2.5.7) and

$$P(x, t\theta) \leqslant \frac{2}{q} + \frac{1}{q^2} + \frac{10}{q^3} + \frac{10}{q^4} + 3 \cdot (q_0 + 1)(q_0^4 - 1) \cdot \frac{2}{q^3} < \frac{1}{2}.$$

Now assume that $m = 5$ and $e = 2$. In this case, the only type of nonsubspace subgroup to arise is $\mathrm{O}_5(q) \wr S_2$. We will now bound the number of subgroups of this type that contain $t\theta$. Note that a suitable power z of y has type

$$I_2 \perp (8)^+_{q_0} = I_2 \perp (4)^+_q \perp (4)^+_q.$$

Let E be the 1-eigenspace of z. Then z stabilises $q-1$ nondegenerate subspaces of E and consequently stablises exactly $2(q-1)$ nondegenerate 5-spaces of V (see Lemma 2.3.1). Therefore, z is contained in at most $q-1$ subgroups of type $O_5(q) \wr S_2$, and thus

$$P(x,t\theta) < \frac{2}{q} + \frac{1}{q^2} + \frac{10}{q^3} + \frac{10}{q^4} + (1+3(q-1)) \cdot \frac{2}{q^3} < \frac{1}{2}.$$

Case 2: $\theta \in \{\imath r\varphi^i, \imath\psi^i\}$

If q is even, then

$$\begin{aligned} P(x,t\theta) \leqslant \frac{1}{q} + \frac{1}{q^2} + \frac{1}{q^4} + \frac{1}{q^{(m-1)/2}} + \frac{1}{q^{m-3}} + \frac{9}{q^{m-2}} + \frac{6}{q^{m-1}} \\ + (2+\log\log q) \cdot (q_0+1)(q_0^2+1)(q_0^{m-3}+1) \cdot \frac{2}{q^{m-2}}, \end{aligned}$$

and if q is odd, then

$$\begin{aligned} P(x,t\theta) \leqslant \frac{2}{q} + \frac{1}{q^2} + \frac{1}{q^4} + \frac{2}{q^5} + \frac{1}{q^{(m-1)/2}} + \frac{3}{q^{m-3}} + \frac{15}{q^{m-2}} + \frac{10}{q^{m-1}} \\ + (3+\log\log q) \cdot (q_0+1)(q_0^2+1)(q_0^{m-3}+1) \cdot \frac{2}{q^{m-2}}. \end{aligned}$$

This proves that $P(x,t\theta) < \frac{1}{2}$ unless $(m,q) = (5,8)$ or $e = 2$. If $(m,q) = (5,8)$, then there is a unique type of subfield subgroups and $t\theta$ is not contained in a subgroup of type $O_2^\varepsilon(q) \wr S_5$; adjusting the bound accordingly gives $P(x,t\theta) < \frac{1}{2}$.

Finally assume that $e = 2$. In this case $\varepsilon = -$ and no subfield subgroups arise. If $m = 7$, then $t\theta$ is not contained in a subgroup of type $O_2^-(q) \wr S_7$, and adjusting the bound above accordingly, proves that $P(x,t\theta) < \frac{1}{2}$. If $m = 5$, then y has type

$$(4)^-_{q_0} \perp (4)^-_{q_0} \perp r^- = (2)^-_q \perp (2)^-_q \perp (2)^-_q \perp (2)^-_q \perp r^-,$$

so y is contained in a unique $\mathcal{C}_2$ subgroup of type $O_2^\varepsilon(q) \wr S_5$. Therefore, if q is even, then

$$P(x,t\theta) \leqslant \frac{1}{q} + \frac{3}{q^2} + \frac{9}{q^3} + \frac{7}{q^4} + \frac{2}{q^3} < \frac{1}{2}.$$

Now assume that q is odd. Let H be a subgroup of type $O_5(q) \wr S_2$ stabilising a decomposition $V_1 \perp V_2$. Now y^2 centralises the decomposition and we may assume that $U \subseteq V_1$, where U is one of the 2-spaces y^2 stabilises and on which y acts irreducibly. However, U is stabilised by y, so y stabilises V_1 and hence centralises the decomposition. However, by considering the number of choices for the stabilised 5-space containing the 1-eigenspace of y, we see that y is contained in at most $\binom{4}{2} = 6$ subgroups of type $O_5(q) \wr S_2$. Therefore,

$$P(x,t\theta) \leqslant \frac{2}{q} + \frac{3}{q^2} + \frac{1}{q^3} + \frac{4}{q^4} + \frac{15}{q^8} + 7 \cdot \frac{2}{q^{m-2}} < \frac{1}{2}.$$

This completes the proof. □

Remark 5.3.25. Let $G = \langle \mathrm{P}\Omega^{\varepsilon}_{2m}(q), \theta \rangle$ satisfy $G \cap \mathrm{PGO}^{\varepsilon}_{2m}(q) \not\leqslant \mathrm{PDO}^{\varepsilon}_{2m}(q)$. Let us comment on a possible approach to proving that $u(G)$ is bounded if q is. This idea is similar to the proof of Proposition 4.3.25. First we show that there exists some fixed k (independent of m) such that for all $g \in T\theta$ there exists a k-subspace of $\mathbb{F}_q^{2m}$ that is stabilised by g. Second we construct a set $\mathcal{X}$ of elements of G for which $|\mathcal{X}|$ is bounded independently of m (say as a polynomial in q) and every k-space of V is stabilised by some element of $\mathcal{X}$. This would imply that $u(G) < |\mathcal{X}|$. It is not difficult to see that every element in $\mathrm{PO}^{\varepsilon}_{2m}(q) \setminus \mathrm{PSO}^{\varepsilon}_{2m}(q)$ stabilises a 1-space.

5.3.3 Proofs of Main Results

We can now complete the proofs of Theorems 5A and 5B.

Proof of Theorem 5A. Proposition 5.1.12 details the groups $G = \langle T, \theta \rangle$ that must be considered in order to prove Theorem 5A. For each such group, the bound $u(G) \geqslant 2$ is established in one of Propositions 5.2.5, 5.2.13, 5.3.13 and 5.3.23. □

Proof of Theorem 5B. Let (G_i) be a sequence of groups in $\mathcal{A}$ such that $|G_i| \to \infty$, and write $T_i = \mathrm{soc}(G_i)$. Assume that (G_i) does not have an infinite subsequence of groups such that $G_i \cap \mathrm{PGO}^{\varepsilon_i}_{2m_i}(q) \not\leqslant \mathrm{PDO}^{\varepsilon_i}_{2m_i}(q_i)$ where $T_i = \mathrm{P}\Omega^{\varepsilon_i}_{2m_i}(q)$ for a fixed q. Then (G_i) is the union of three sequences: groups $G_i \leqslant \mathrm{PDO}^{\varepsilon_i}_{2m_i}(q_i)$, groups $G_i \not\leqslant \mathrm{PGO}^{\varepsilon_i}_{2m_i}$ but $G_i \cap \mathrm{PGO}^{\varepsilon_i}_{2m_i}(q_i) \leqslant \mathrm{PDO}^{\varepsilon_i}_{2m_i}(q_i)$ and groups for which the field size tends to infinity. In all three cases, the uniform spread diverges to infinity, by Propositions 5.2.6 and 5.3.14 in the first two cases, and Propositions 5.2.5, 5.2.13, 5.3.13 and 5.3.23 in the final case. □

In particular, we have now completed the proofs of Theorems A and B.

Let us comment on how the general approach in this thesis, and this section in particular, will apply in future work.

Remark 5.3.26. This remark continues on from Remark 5.1.15. Let $T = \mathrm{P}\Omega^{+}_{8}(q)$ and recall that T has a triality automorphism τ such that $C_G(\tau) \cong G_2(q)$. Moreover, to show that $u(G) \geqslant k$ for all groups $G = \langle T, \theta \rangle$ with $\theta \in \mathrm{Aut}(T)$, it suffices to assume that θ appears in Proposition 5.1.12 or θ is $\tau\varphi^i$ for a divisor i of f. We now comment on the latter case.

Assume that $\theta = \tau\varphi^i$ for a divisor i of f. To study the uniform spread of $G = \langle T, \theta \rangle$ we consider three cases.

(i) Assume that $i = f$. In this case, $\theta = \tau$ and we proceed as in Case I(b). That is, we carefully select an element $t \in C_T(\tau)$ and then work with the element $t\tau$, noting that $(t\tau)^3 = t^3$, so we can exploit properties of t in order to restrict the possible maximal overgroups of $t\tau$.

(ii) Assume that $i < f$. Let $X = \mathrm{PSO}_8(\overline{\mathbb{F}}_p)$, $\sigma = \theta = \varphi^i\tau$ and $e = f/i$. Write $q = q_0^e$ and let F be the Shintani map of (X, σ, e).

(a) Assume that 3 divides e. Here we can apply Shintani descent as in Case II(a). In particular, $X_{\sigma^e} = X_{\varphi^f} = \mathrm{Inndiag}(T)$ and

$$F\colon \{(g\theta)^{\mathrm{Inndiag}(T)} \mid g \in \mathrm{Inndiag}(T)\} \to \{x^{T_0} \mid x \in T_0\}$$

where T_0 is $C_T(\varphi^i\tau) = {}^3D_4(q_0)$, the *Steinberg triality group*.

(b) Assume that 3 does not divide e. We follow Case II(b). Let $Z = C_X(\tau) = G_2$, an exceptional simple algebraic group. Lemma 2.7.13, with $\gamma = \tau^{-1}$ and $d = 3$, implies that for all $x \in Z_{\varphi^i} = G_2(q_0) \leqslant \mathrm{Inndiag}(T)$, there exists $t \in \mathrm{Inndiag}(T)$ such that $(t\theta)^e$ is X-conjugate to τx.

Remark 5.3.27. The approach of using Lemma 2.7.13 when the Steinberg endomorphisms defining T and θ are inconsistent is a general one and applies to the remaining families of almost simple groups when Shintani descent cannot be applied directly.

In particular, we can work with unitary groups. For instance, assume that $T = \mathrm{PSU}_n(q)$ and $\theta = \varphi^i$, where φ is an automorphism of T for which $\varphi^f = \iota$, the inverse-transpose automorphism, and i is a proper divisor of $2f$. Let $X = \mathrm{PSL}_n(\overline{\mathbb{F}}_p)$.

(a) Assume that $2f/i$ is odd. Here we can apply Shintani descent as in Case II(a). In particular, since $2f/i$ is odd, we may write $\theta = \iota\varphi^j$, where $j = i/2$, noting that j divides f and f/j is odd. Let $\sigma = \theta = \iota\varphi^j$, $e = f/j$ and $q = q_0^e$. Now $X_{\sigma^e} = X_{\iota\varphi^f} = \mathrm{Inndiag}(T)$, $X_\sigma = X_{\iota\varphi^j} = \mathrm{Inndiag}(T_0)$ where $T_0 = \mathrm{PSU}_n(q_0)$ and

$$F\colon \{(g\theta)^{\mathrm{Inndiag}(T)} \mid g \in \mathrm{Inndiag}(T)\} \to \{x^{\mathrm{Inndiag}(T_0)} \mid x \in \mathrm{Inndiag}(T_0)\}.$$

(b) Assume that $2f/i$ is even. We follow Case II(b). Let $Z = C_X(\iota)$, which is $\mathrm{PSp}_n(\overline{\mathbb{F}}_p)$ if n is even, $\mathrm{PSp}_{n-1}(\overline{\mathbb{F}}_p)$ if n is odd and $p = 2$, and $\mathrm{SO}_n(\overline{\mathbb{F}}_p)$ if n is odd and p is odd. Since $2f/i$ is even, i divides f. Lemma 2.7.13, with $e = f/i$, $\sigma = \theta = \varphi^i$, $\gamma = \iota$ and $d = 2$, implies that for all $x \in Z_{\varphi^i} \leqslant \mathrm{Inndiag}(T)$, there exists $t \in \mathrm{Inndiag}(T)$ such that $(t\theta)^e$ is X-conjugate to ιx.

Let us now briefly mention the general framework for studying the uniform spread of the exceptional groups of Lie type. We expect to be able handle the untwisted groups E_7 and E_8 like the symplectic group $\mathrm{PSp}_{2m}(q)$, the untwisted group E_6 (admitting a graph automorphism) like the plus-type orthogonal group $\mathrm{P}\Omega^+_{2m}(q)$, the untwisted groups F_4 and G_2 (admitting a graph-field automorphism) like $\mathrm{Sp}_4(2^f)$ and the twisted groups ${}^2B_2$, ${}^3D_4$, ${}^2E_6$, ${}^2F_4$, ${}^2G_2$ like the minus-type orthogonal group $\mathrm{P}\Omega^-_{2m}(q)$.

This completes the thesis.

A

MAGMA Code

In this appendix, we present the MAGMA [5] code for our computational methods. See Section 2.8 for a brief summary of these methods and the previous work they build on.

The function `FixedPointRatio` calculates the fixed point ratio $\mathrm{fpr}(g, G/H)$ of an element $g \in G$ in the action of G on G/H. It takes as input a group G, a subgroup $H \leqslant G$ and an element $g \in G$. The function returns the fixed point ratio $\mathrm{fpr}(g, G/H)$.

```
function FixedPointRatio( G, H, g )
  count:=0;
  classreps:=Classes(H);
  for rep in classreps do
    if (rep[1] eq Order(g)) then
      if IsConjugate(G,g,rep[3]) then
        count:=count+rep[2];
      end if;
    end if;
  end for;
  return count*Order(Centraliser(G,g))/Order(G);
end function;
```

The function `MaximalOvergroups` provides information about the maximal overgroups of an element. The input is a group G and an element $s \in G$. The function returns a pair of lists $[H_1, \ldots, H_m]$ and $[k_1, \ldots, k_m]$ where H_i are pairwise non-conjugate maximal subgroups of G and k_i is the number of conjugates of H_i which contain s.

```
function MaximalOvergroups( G, s )
  groups:=[];
  mults:=[];
  maxes:=MaximalSubgroups(G : OrderMultipleOf:=Order(s));
  for M in maxes do
    H:=M`subgroup;
    count:=FixedPointRatio(G,H,s)*Order(G)/Order(H);
    if (count ne 0) then
      groups:=Append(groups,H);
      mults:=Append(mults,count);
    end if;
  end for;
  return <groups, mults>;
end function;
```

The function `ClassRepTuples` is based heavily on an algorithm of Breuer [9, Section 3.3]. The input is a group G and a list $[x_1, \ldots, x_k]$ of elements of G. The function returns a list of orbit representatives for the diagonal conjugation action of G on $x_1^G \times \cdots \times x_k^G$.

```
function ClassRepTuples( G, list )
  cents:=[];
  for x in list do
    cents:=Append(cents,Centraliser(G,x));
  end for;
  function OrbReps(G, reps, intersect, i, cents, list )
    if (i gt #list) then
      L:=[reps];
    else
      L:=[];
      for r in DoubleCosetRepresentatives(G, cents[i], intersect) do
        L:=L cat OrbReps(G, Append(reps,list[i]^r),
          (intersect meet cents[i]^r), i+1, cents, list );
      end for;
    end if;
    return L;
  end function;
  return OrbReps(G,[list[1]],cents[1],2,cents,list);
end function;
```

The function `RandomCheck` is a randomised algorithm that plays a role in determining the uniform spread of a group. The input is a group G, an element $s \in G$, a list $[x_1, \ldots, x_k]$

of elements in G and a nonnegative integer N. The claim to be tested is: for every list $[y_1, \ldots, y_k]$ with $y_i \in x_i^G$, there exists $z \in s^G$ such that $\langle y_1, z\rangle = \cdots = \langle y_k, z\rangle = G$. If the function returns `true`, then this claim is true, and if the function returns `false`, then the result is inconclusive. The claim is tested by random selections of elements in G, the number of which depends on the parameter N.

```
function RandomCheck( G, s, list, N )
  classtuples:=ClassRepTuples(G,list);
  for X in classtuples do
    found:=false;
    for i in [1..N] do
      h:=Random(G);
      found:=true;
      for x in X do
        H:=sub<G|[x,s^h]>;
        if not (Order(H) eq Order(G)) then
          found:=false;
          break;
        end if;
      end for;
      if (found) then
        break;
      end if;
    end for;
    if (not found) then
      return false;
    end if;
  end for;
  return true;
end function;
```

The function `ProbabilisticMethod` is our main computational tool for studying the uniform spread of a group. The input is a group G, an element $s \in G$ and nonnegative integers k and N. First, the function implements the probabilistic method described in Section 2.1 to determine whether $u(G) \geqslant k$ with respect to the class s^G. If successful, the function returns `true`; otherwise the second phase commences. Here `RandomCheck` is employed to verify that for all $(y_1, \ldots, y_k)$ with $y_i \in x_i^G$ there exists $z \in s^G$ such that $\langle y_1, z\rangle = \cdots = \langle y_k, z\rangle$, for all k-tuples $(x_1^G, \ldots, x_k^G)$ of conjugacy classes for which this was not proved in the first phase. If successful, the function returns `true`. If `false` is returned, then the result is inconclusive. A variety of helpful data from the computation is printed to the standard output.

```
function ProbabilisticMethod( G, s, k, N )
  maxandmult:=MaximalOvergroups(G,s);
  max:=maxandmult[1];
  mult:=maxandmult[2];

  print "-------------- \nMAXIMALSUBGROUPS \n-------------- \n ";
  for i in [1..#max] do
    print [Order(max[i]), mult[i]];
  end for;
  print " ";

  classes:=Classes(G);
  primeclasses:=[];
  sums:=[];

  print "-------------- \nCONJUGACY CLASSES \n-------------- \n ";
  for class in classes do
    if (IsPrime(class[1])) then
      primeclasses:=Append(primeclasses,class[3]);
      ratios:=[];
      for H in max do
        ratios:=Append(ratios,FixedPointRatio(G,H,class[3]));
      end for;
      sum:=0;
      for i in [1..#max] do
        sum:=sum+ratios[i]*mult[i];
      end for;
      sums:=Append(sums,sum);
      print "Order:", class[1];
      print "Size:", class[2];
      print "Fixed Point Ratios:", ratios;
      print "Sum of FPRs:", sum;
      print " \n--------------\n ";
    end if;
  end for;

  print "-------------- \nBAD TUPLES \n-------------- \n ";

  tuples:=[];
  if exists{sum: sum in sums | sum ge 1/k} then
    markers:=[1 .. #sums];
```

```
  ind:=[[]];
  for i in [1 .. k] do
    newind:=[];
    for y in ind do
      for x in markers do
        if (i eq 1) or (x ge y[i-1]) then
          z:=Append(y,x);
          newind:=Append(newind,z);
        end if;
      end for;
    end for;
    ind:=newind;
  end for;
  seq:=[];
  for I in ind do
    elt:=[];
    for i in I do
      elt:=Append(elt,sums[i]);
    end for;
    seq:=Append(seq,elt);
  end for;
  for i in [1 .. #seq] do
    tot:=0;
    for x in seq[i] do
      tot:=tot+x;
    end for;
    if tot ge 1 then
      tuples:=Append(tuples,ind[i]);
    end if;
  end for;
end if;

print "Bad Tuples:", tuples;
print " ";
if N gt 0 then
  badtuples:=[];
  for tuple in tuples do
    list:=[];
    for t in tuple do
      list:=Append(list, primeclasses[t]);
    end for;
```

```
      if not RandomCheck(G,s,list,N) then
        badtuples:=Append(badtuples,tuple);
      end if;
    end for;
    print "Bad tuples remaining after", N, "random checks:", badtuples;
    print " ";
  else
    badtuples:=tuples;
  end if;

  return (badtuples eq []);
end function;
```

We sometimes want to work with groups that cannot be handled with `MaximalSubgroups`. In this case, we use the function `ClassicalMaximals`. For example, to obtain the maximal subgroups of $O^+_{12}(2)$ we use

```
ClassicalMaximals("O+", 12, 2 : general:=true);
```

MAGMA handles permutation groups more efficiently than matrix groups. Therefore, when working with $O^+_{12}(2)$ it would be advantageous to do the following, which uses `ClassicalMaximals` to obtain the maximal subgroups of $O^+_{12}(2)$ in its permutation group representation.

```
X:=GOPlus(12,2);
f, G, K:=PermutationRepresentation(X : ModScalars:=true);
mX:=ClassicalMaximals("O+", 12, 2 : general:=true);
mG:={f(H) : H in mX};
```

We manually change the relevant line in `MaximalOvergroups` to use `ClassicalMaximals` instead of `MaximalSubgroups` when we need to.

References

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

[2] M. Aschbacher, *Finite Group Theory*, Cambridge Studies in Advanced Mathematics, vol. 10, 2nd ed., Cambridge University Press, 2000.

[3] M. Aschbacher and G. M. Seitz, *Involutions in Chevalley groups over fields of even order*, Nagoya Math. J. **63** (1976), 1–91.

[4] J. Bamberg and T. Penttila, *Overgroups of cyclic Sylow subgroups of linear groups*, Comm. Algebra **36** (2008), 2503–2543.

[5] W. Bosma, J. Cannon and C. Playoust, *The* MAGMA *algebra system I: The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[6] J. N. Bray, D. F. Holt and C. M. Roney-Dougal, *Certain classical groups are not well-defined*, J. Group Theory **12** (2009), 171–180.

[7] 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 Notes Series, vol. 407, Cambridge University Press, 2013.

[8] J. L. Brenner and J. Wiegold, *Two generator groups, I*, Michigan Math. J. **22** (1975), 53–64.

[9] T. Breuer, *GAP computations concerning probabilistic generation of finite simple groups*, arXiv:0710.3267, 2007.

[10] T. Breuer, R. M. Guralnick and W. M. Kantor, *Probabilistic generation of finite simple groups, II*, J. Algebra **320** (2008), 443–494.

[11] T. Breuer, R. M. Guralnick, A. Lucchini, A. Maróti and G. P. Nagy, *Hamiltonian cycles in the generating graphs of finite groups*, Bull. Lond. Math. Soc. **42** (2010), 621–633.

[12] T. C. Burness, *Fixed point ratios in actions of finite classical groups, I*, J. Algebra **309** (2007), 69–79.

[13] T. C. Burness, *Fixed point ratios in actions of finite classical groups, II*, J. Algebra **309** (2007), 80–138.

[14] T. C. Burness, *Fixed point ratios in actions of finite classical groups, IV*, J. Algebra **314** (2007), 749–788.

[15] T. C. Burness, *Simple groups, fixed point ratios and applications*, in *Local Representation Theory and Simple Groups*, EMS Series of Lectures in Mathematics, European Mathematical Society, 2018, 267–322.

[16] T. C. Burness, *Simple groups, generation and probabilistic methods*, in *Proceedings of Groups St Andrews 2017*, London Math. Soc. Lecture Note Series, vol. 455, Cambridge University Press, 2019, 200–229.

[17] T. C. Burness and M. Giudici, *Classical Groups, Derangements and Primes*, Aust. Math. Soc. Lecture Note Series, vol. 25, Cambridge University Press, 2016.

[18] T. C. Burness and S. Guest, *On the uniform spread of almost simple linear groups*, Nagoya Math. J. **209** (2013), 35–109.

[19] T. C. Burness and S. Harper, *Computations concerning the uniform domination number of a finite simple group* at `http://seis.bristol.ac.uk/~tb13602/udncomp.pdf`.

[20] T. C. Burness and S. Harper, *On the uniform domination number of a finite simple group*, Trans. Amer. Math. Soc., to appear.

[21] T. C. Burness and S. Harper, *Finite groups,* 2*-generation and the uniform domination number*, arXiv:`1810.12076`, 2018.

[22] A. A. Buturlakin and M. A. Grechkoseeva, *The cyclic structure of maximal tori of the finite classical groups*, Algebra Logic **46** (2007), 73–89.

[23] R. W. Carter, *Simple Groups of Lie Type*, John Wiley and Sons, 1972.

[24] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, $\mathbb{ATLAS}$ *of Finite Groups*, Clarendon Press, 1985.

[25] L. E. Dickson, *Linear groups with an exposition of the Galois field theory*, Teubner, 1901.

[26] J. D. Dixon, *The probability of generating the symmetric group*, Math. Z. **110** (1969), 199–205.

[27] R. H. Dye, *Interrelations of symplectic and orthogonal groups in characteristic two*, J. Algebra **59** (1979), 202–221.

[28] F. Erdem, *On the generating graphs of symmetric groups*, J. Group Theory **21** (2018), 629–649.

[29] D. Frohardt and K. Magaard, *Grassmannian fixed point ratios*, Geom. Dedicata **82** (2000), 21–104.

[30] D. Frohardt and K. Magaard, *Composition factors of monodromy groups*, Ann. of Math. **154** (2001), 327–345.

[31] D. Gorenstein, R. Lyons and R. Solomon, *The Classification of the Finite Simple Groups, Number 3*, Mathematical Surveys and Monographs, vol. 40, Amer. Math. Soc., 1998.

[32] R. M. Guralnick, *The spread of finite groups*, preprint.

[33] R. M. Guralnick and W. M. Kantor, *Probabilistic generation of finite simple groups*, J. Algebra **234** (2000), 743–792.

[34] R. M. Guralnick and G. Malle, *Products of conjugacy classes and fixed point spaces*, J. Amer. Math. Soc. **25** (2012), 77–121.

[35] R. M. Guralnick, T. Penttila, C. E. Praeger and J. Saxl, *Linear groups with orders having certain large prime divisors*, Proc. Lond. Math. Soc. **78** (1997), 167–214.

[36] R. M. Guralnick and J. Saxl, *Generation of finite almost simple groups by conjugates*, J. Algebra **268** (2003), 519–571.

[37] R. M. Guralnick and A. Shalev, *On the spread of finite simple groups*, Combinatorica **23** (2003), 73–87.

[38] S. Harper, *On the uniform spread of almost simple symplectic and orthogonal groups*, J. Algebra **490** (2017), 330–371.

[39] B. Hartley and T. O. Hawkes, *Rings, Modules and Linear Algebra*, Chapman and Hall, 1970.

[40] W. M. Kantor and A. Lubotzky, *The probability of generating a finite classical group*, Geom. Dedicata **36** (1990), 67–87.

[41] N. Kawanaka, *On the irreducible characters of the finite unitary groups*, J. Math. Soc. Japan **29** (1977), 425–450.

[42] P. B. Kleidman, *The maximal subgroups of the finite 8-dimensional orthogonal groups* $\mathrm{P}\Omega_8^+(q)$ *and of their automorphism groups*, J. Algebra **110** (1987), 173–242.

[43] 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.

[44] S. Lang, *Algebra*, Graduate Texts in Mathematics, vol. 211, 3rd ed., Springer-Verlag, 2002.

[45] 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), 393–463.

[46] M. W. Liebeck, *Subgroups of simple algebraic groups and of related finite and locally finite groups of Lie type*, in *Finite and Locally Finite Groups*, NATO ASI Series, vol. 471, Springer, 1995.

[47] M. W. Liebeck, *Probabilistic and asymptotic aspects of finite simple groups*, in *Probabilistic Group Theory, Combinatorics, and Computing*, Lecture Notes in Math., vol. 2070, Springer, 2013, 1–34.

[48] 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.

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

[50] M. W. Liebeck and G. M. Seitz, *Unipotent and Nilpotent Classes in Simple Algebraic Groups and Lie Algebras*, Mathematical Surveys and Monographs, vol. 180, American Mathematical Society, 2012.

[51] M. W. Liebeck and A. Shalev, *The probability of generating a finite simple group*, Geom. Dedicata **56** (1995), 103–113.

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

[53] G. Malle and D. Testerman, *Linear Algebraic Groups and Finite Groups of Lie Type*, Graduate Studies in Advanced Mathematics, vol. 133, Cambridge University Press, 2011.

[54] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's Conjecture*, J. Reine Angew. Math. **572** (2003), 167–195.

[55] E. Netto, *Substitutionentheorie und ihre Anwendungen auf die Algebra*, Teubner, 1882, English translation: 1892, 2nd ed.

[56] S. Piccard, *Sur les bases du groupe symétrique et du groupe alternant*, Math. Ann. **116** (1939), 752–767.

[57] A. Shalev, *Probabilistic group theory and Fuchsian groups*, in *Infinite Groups: Geometric, Combinatorial and Dynamical Aspects*, Progr. Math., vol. 248, Birkhäuser, 2005, 363–388.

[58] T. Shintani, *Two remarks on irreducible characters of finite general linear groups*, J. Math. Soc. Japan **28** (1976), 396–414.

[59] R. Steinberg, *Endomorphisms of linear algebraic groups* Mem. Amer. Math. Soc. **80** (1968).

[60] R. Steinberg, *Generators for simple groups*, Canadian J. Math. **14** (1962), 277–283.

[61] M. Suzuki, *On a class of doubly transitive groups*, Ann. of Math. **75** (1962), 105–145.

[62] G. E. Wall, *On the conjugacy classes in the unitary, symplectic and orthogonal groups*, J. Aust. Math. Soc. **3** (1963), 1–62.

[63] R. A. Wilson, *The Finite Simple Groups*, Graduate Texts in Mathematics, vol. 251, Springer-Verlag, 2009.

[64] A. J. Woldar, $\frac{3}{2}$*-generation of the sporadic simple groups*, Comm. Algebra **22** (1994), 675–685.

[65] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monat Math. Physik **3** (1892), 265–284.

This thesis was typeset in LaTeX, a system created by Lamport extending Knuth's TeX. The body text is set at 11/16.5pt on a 35pc measure with Palatino, designed by Zapf.