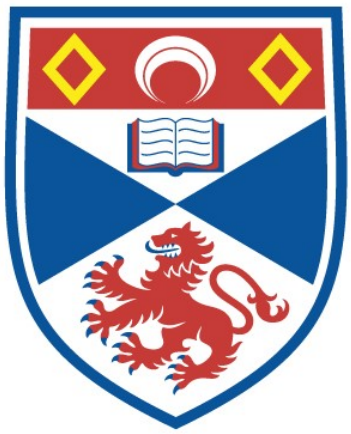
# DIAMETERS OF GRAPHS RELATED TO GROUPS AND BASE SIZES OF PRIMITIVE GROUPS

Saul D. Freedman

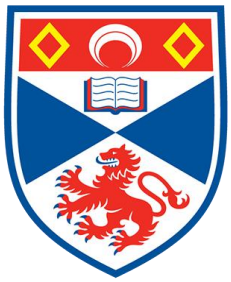
A Thesis Submitted for the Degree of PhD
at the
University of St Andrews



2022

# Diameters of graphs related to groups and base sizes of primitive groups

Saul D. Freedman



University of
St Andrews

This thesis is submitted in partial fulfilment for the degree of

Doctor of Philosophy (PhD)

at the University of St Andrews

May 2022

**Abstract**

In this thesis, we study three problems. First, we determine new bounds for base sizes $b(G, \Omega)$ of primitive subspace actions of finite almost simple classical groups $G$. Such base sizes are useful statistics in computational group theory. We show that if the underlying set $\Omega$ consists of $k$-dimensional subspaces of the natural module $V = \mathbb{F}_q^n$ for $G$, then $b(G, \Omega) \geqslant \lceil n/k \rceil + c$, where $c \in \{-2, -1, 0, 1\}$ depends on $n$, $q$, $k$ and the type of $G$. If instead $\Omega$ consists of pairs $\{X, Y\}$ of subspaces of $V$ with $k := \dim(X) < \dim(Y)$, and $G$ is generated by $\mathrm{PGL}(n, q)$ and the graph automorphism of $\mathrm{PSL}(n, q)$, then $b(G, \Omega) \leqslant \max\{\lceil n/k \rceil, 4\}$.

The second part of the thesis concerns the intersection graph $\Delta_G$ of a finite simple group $G$. This graph has vertices the nontrivial proper subgroups of $G$, and its edges are the pairs of subgroups that intersect nontrivially. We prove that $\Delta_G$ has diameter at most 5, and that a diameter of 5 is achieved only by the graphs of the baby monster group and certain unitary groups of odd prime dimension. This answers a question posed by Shen [126].

Finally, we study the non-commuting, non-generating graph $\Xi(G)$ of a group $G$, where $G/Z(G)$ is either finite or non-simple. This graph is closely related to the hierarchy of graphs introduced by Cameron [34, §2.6]. The graph's vertices are the non-central elements of $G$, and its edges are the pairs $\{x, y\}$ such that $\langle x, y \rangle \neq G$ and $xy \neq yx$. We show that if $\Xi(G)$ has an edge, then either the graph is connected with diameter at most 5; the graph has exactly two connected components, each of diameter 2; or the graph consists of isolated vertices and a component of diameter at most 4. In this last case, either the nontrivial component has diameter 2, or $G/Z(G)$ is a non-simple insoluble primitive group with every proper quotient cyclic.

## Candidate's declaration

I, Saul Daniel Freedman, do hereby certify that this thesis, submitted for the degree of PhD, which is approximately 80,000 words in length, has been written by me, and that it is the record of work carried out by me, or principally by myself in collaboration with others as acknowledged, and that it has not been submitted in any previous application for any degree. I confirm that any appendices included in my thesis contain only material permitted by the 'Assessment of Postgraduate Research Students' policy.

I was admitted as a research student at the University of St Andrews in January 2019.

I received funding from an organisation or institution and have acknowledged the funder(s) in the full text of my thesis.

Date 28/04/2022 Signature of candidate

## Supervisor's declaration

I hereby certify that the candidate has fulfilled the conditions of the Resolution and Regulations appropriate for the degree of PhD in the University of St Andrews and that the candidate is qualified to submit this thesis in application for that degree. I confirm that any appendices included in the thesis contain only material permitted by the 'Assessment of Postgraduate Research Students' policy.

Date 28/4/22 Signature of supervisor

## Permission for publication

In submitting this thesis to the University of St Andrews we understand that we are giving permission for it to be made available for use in accordance with the regulations of the University Library for the time being in force, subject to any copyright vested in the work not being affected thereby. We also understand, unless exempt by an award of an embargo as requested below, that the title and the abstract will be published, and that a copy of the work may be made and supplied to any bona fide library or research worker, that this thesis will be electronically accessible for personal or research use and that the library has the right to migrate this thesis into new electronic forms as required to ensure continued access to the thesis.

I, Saul Daniel Freedman, confirm that my thesis does not contain any third-party material that requires copyright clearance.

The following is an agreed request by candidate and supervisor regarding the publication of this thesis:

**Printed copy**

No embargo on print copy.

**Electronic copy**

No embargo on electronic copy.

Date 28/04/2022 Signature of candidate

Date 28/04/2022 Signature of supervisor

**Underpinning Research Data or Digital Outputs**

**Candidate's declaration**

I, Saul Daniel Freedman, understand that by declaring that I have original research data or digital outputs, I should make every effort in meeting the University's and research funders' requirements on the deposit and sharing of research data or research digital outputs.

Date 28/04/2022 Signature of candidate

**Permission for publication of underpinning research data or digital outputs**

We understand that for any original research data or digital outputs which are deposited, we are giving permission for them to be made available for use in accordance with the requirements of the University and research funders, for the time being in force.

We also understand that the title and the description will be published, and that the underpinning research data or digital outputs will be electronically accessible for use in accordance with the license specified at the point of deposit, unless exempt by award of an embargo as requested below.

The following is an agreed request by candidate and supervisor regarding the publication of underpinning research data or digital outputs:

No embargo on underpinning research data or digital outputs.

Date 28/04/2022 Signature of candidate

Date 28/04/2022 Signature of supervisor

## Acknowledgements

I am immensely grateful to my supervisors, Professor Colva Roney-Dougal and Professor Peter Cameron, for their invaluable academic and personal support throughout my entire PhD. I owe the quality of this thesis, and my fruitful and enjoyable PhD experience, to their wisdom, kindness, patience and dedication.

I would also like to thank Dr Gareth Tracey for very helpful discussions regarding elements of groups that lie in a unique maximal subgroup, and my thesis examiners, Dr Martyn Quick and Professor Donna Testerman, for their insightful comments. Additionally, I am grateful to the Isaac Newton Institute for Mathematical Sciences, Cambridge, for support and hospitality during the programme "Groups, representations and applications: new perspectives", where work on this thesis was undertaken.

Finally, I give my deepest thanks to my mother, my brother, and all of my friends, for their constant love and support. It means the world to me.

## Funding

This work was supported by the University of St Andrews (School of Mathematics and Statistics and St Leonard's Postgraduate College).
This work was supported by EPSRC grant number EP/R014604/1.

## Digital outputs access statement

Digital outputs underpinning this thesis are available at
`https://doi.org/10.17630/56ceed97-0a86-4684-b0a9-e454c1a7440b`

# Contents

# Chapter 1

# Introduction

In this thesis, we explore the connectedness and diameter of two graphs related to groups: the intersection graph of a non-abelian finite simple group, and the non-commuting, non-generating graph of a group. In order to do so, we first determine bounds for the base sizes of primitive subspace actions of finite almost simple classical groups. These bounds are useful when considering the aforementioned graphs related to the finite simple unitary groups, and, as we explain below, they are also of general interest, and may have applications in computational group theory.

Before introducing in more detail the problems discussed in this thesis, we point out that (with one specified exception in this introduction) all graphs that we consider are undirected, and do not contain loops or multiple edges. Additionally, we often use Atlas notation [42, Ch. 5] to describe the structures of groups. For completeness, some of the basic group theoretic and graph theoretic terms used in this introduction will be defined in Chapters 2 and 4, respectively. Note also that several of the proofs and remarks in this thesis involve computations performed using GAP [56] and Magma [15]. Appendix A provides brief summaries of the files [54] containing the relevant code, and where in the thesis they are used (see the comments in the files themselves for more information).

### 1.0.1 Base sizes of primitive groups

The *base size* $b(G)$ of a transitive permutation group $G$ acting on a set $\Omega$ is the smallest size of a subset of $\Omega$ whose pointwise stabiliser in $G$ is trivial. Since the action of $G$ is completely determined by its action on the points of any such subset, $b(G)$ is a useful measure of the computational resources required to store elements of $G$ and perform associated calculations [33, p. 120]. The base size of $G$ is also closely related to other important permutation group statistics, including the maximum size of an *irredundant base* for $G$, the *height* of $G$, and the *relational complexity* of $G$ (see, for example, [57, §1.1]).

Due to the wide importance of almost simple primitive groups, information about

their base sizes is of particular interest. One of the most famous results in this area is the Cameron-Kantor conjecture (see [32, Conjecture 3.4] and [36, p. 260]), which was proved by Liebeck and Shalev [99, Theorem 1.3] in 1999. This result states that there exists an absolute constant $c$ such that, if $G$ is a finite almost simple primitive group (acting faithfully) and $b(G) > c$, then $G$ lies in a known collection of groups with large base sizes, which are said to have *standard actions*. More specifically, these are the actions of the alternating and symmetric groups of degree $k$ on subsets or partitions of $\{1, \ldots, k\}$, and the *subspace actions* of the classical groups. For the most part, a subspace action is an action of a classical group on subspaces or unordered pairs of subspaces of the natural module for the group.

The non-standard actions of finite almost simple groups have been a large focus of base size-related research. For example, shortly after Liebeck and Shalev proved the Cameron-Kantor conjecture, Cameron [33, p. 122] further conjectured that 7 is the best possible value for the constant $c$. This was finally proved in 2011, with the combined results of [23, 26, 28, 30]. There have also been recent developments in the study of standard actions. Indeed, in 2021, Morris and Spiga [112] determined the base sizes of the aforementioned actions of alternating and symmetric groups on partitions. For the actions of these groups on subsets, Halasi [71] (in 2011) and Cáceres et al. [31, p. 2, §2] (in 2013) calculated the base size in certain cases, and proved general asymptotic results.

It remains to discuss the base sizes of primitive subspace actions. In 2019, Halasi, Liebeck and Maróti [72, §3] determined upper bounds for most families of these actions. Moscatiello and Roney-Dougal [113] built on this work by improving these bounds for certain actions on low-dimensional subspaces, and determining the exact base size for one family of groups. However, no reasonable lower bounds are known for the base sizes of most families of primitive subspace actions.

In Chapter 3, we narrow this knowledge gap by proving lower bounds for the base size of a finite almost simple classical group acting primitively on a set of subspaces of its natural module. We achieve bounds similar to those for the base sizes of subspace actions of (infinite) simple classical algebraic groups given by Burness, Guralnick and Saxl [27, §4] in 2017, and our proofs use similar ideas. In addition, we prove an upper bound for $b(G)$ when $G$ is an almost simple linear group acting primitively on an unordered pair of subspaces of the natural module. Our upper bound is significantly tighter than the corresponding bound proved in [72]. By explicitly computing the base sizes of certain small permutation groups, we observe that all of our bounds are, in general, tight. As detailed in §3.1.3, these bounds have found application in [55], in the context of the *closure number* of a finite simple classical group.

### 1.0.2 Diameters of graphs related to groups

Given a binary relation defined on the elements or subgroups of a group $G$, it is natural to study the properties of the graph that encodes this relation, and the relationships between the structures of the graph and the group. This provides new and interesting ways of understanding and distinguishing between individual groups and families of groups, and can lead to applications in other areas of group theory (see the example of the commuting graph below).

Let us first consider graphs defined on subgroups of $G$. The most natural of these graphs is perhaps the *intersection graph* $\Delta_G$ of $G$, introduced by Csákány and Pollák [48] in 1969. The vertices of this graph are the nontrivial proper subgroups of $G$, with two vertices $H$ and $K$ adjacent if and only if $H \cap K \neq 1$. Csákány and Pollák classified the finite non-simple groups $G$ for which $\Delta_G$ is connected, and proved that the diameter of $\Delta_G$ is at most 4 for every such group.

To complement the results of Csákány and Pollák, we prove in Chapter 4 that the intersection graph of a non-abelian finite simple group is connected with diameter at most 5. Furthermore, we show that a diameter of 5 is achieved only by the sporadic baby monster group and certain unitary groups of odd prime dimension. This resolves a question from 2010 posed by Shen [126], who first proved the connectedness of the graph for simple groups. Our result also improves the previous upper bounds for the graph's diameter proved by Herzog, Longobardi and Maj [77] in 2010 and by Ma [106] in 2016.

Now, there is an extremely prolific body of research related to graphs defined on the elements of the group $G$. For a rather comprehensive introduction to this topic, see [34] and the references therein. These graphs of course include the Cayley graphs, but our focus here will be on graphs that are necessarily preserved by automorphisms of $G$, and that (up to isomorphism) depend only on the isomorphism type of $G$.

The earliest of these graphs to be studied was the *commuting graph*, implicitly introduced by Brauer and Fowler [16] in 1955. This graph encodes the binary relation "$x \sim y$ if and only if $x$ and $y$ commute" for $x, y \in G$. Notice that this graph is always connected with diameter at most 2, as each central element is adjacent to each other element. However, the question of the graph's diameter becomes more interesting when all central vertices are deleted. Indeed, in 2013, Morgan and Parker [111] proved that if $G$ is a finite group with trivial centre, then each connected component of this new graph has diameter at most 10. On the other hand, in the same year, Giudici and Parker [60] proved that, for finite groups in general, the associated graphs can be connected with arbitrarily large diameter. We also note that the version of the graph with central elements included, and with a loop at

every vertex, has a useful computational application: random walks on this graph can be used to find representatives of small conjugacy classes of $G$ [34, p. 57].

The commuting graph of $G$ is one of the graphs in a certain hierarchy of graphs defined on the elements of $G$, formally introduced by Cameron in [34, §2.6] (and mentioned earlier in [35, p. 2]). The final three graphs in this hierarchy are the commuting graph of $G$; the *non-generating graph* of $G$, where two vertices are adjacent if and only if they do not generate $G$; and the complete graph on $G$. If $G$ is non-abelian or not 2-generated, then the commuting graph is a spanning subgraph of the non-generating graph, which is of course a spanning subgraph of the complete graph.

While these graphs (and the remaining graphs in Cameron's hierarchy) are interesting in their own right, it is also interesting to consider the differences between subsequent graphs in the hierarchy (with certain vertices deleted in each case). For example[1], the difference between the complete graph and the non-generating graph (with the identity vertex deleted) is the *generating graph* $\Gamma(G)$, which was introduced by Liebeck and Shalev [98, p. 55] in 1996, and which has since been very well studied. One of the most well-known results about this graph was proved by Breuer, Guralnick and Kantor [19, Theorem 1.2] in 2008: if $G$ is a non-abelian finite simple group, then $\Gamma(G)$ is always connected with diameter 2 (in fact, their result is stronger than this statement). In 2021, Burness, Guralnick and Harper [22, Corollary 6] generalised this result, and showed that if $G$ is any finite group, then $\Gamma(G)$ either has an isolated vertex or is connected with diameter at most 2. The structure of $\Gamma(G)$ has also been studied in the case where the graph does have an isolated vertex, for example, in [47, 102].

In this thesis, we study the connectedness and diameter of the next difference in the hierarchy, i.e., the *non-commuting, non-generating graph* of $G$, which we denote by $\Xi(G)$. Here, two vertices are adjacent if and only if they do not commute and do not generate $G$. We delete the vertices of the graph corresponding to $Z(G)$, as they would otherwise always be isolated. For easy reference, we note here that $\Xi^+(G)$ denotes the subgraph of $\Xi(G)$ induced by its non-isolated vertices. In Chapter 5, we prove general results about $\Xi(G)$, and we explore its structure when $G$ is a (finite or infinite) group that is not a central extension of a non-abelian simple group. We then consider the case where $G$ is a (central extension of a) non-abelian finite simple group in Chapter 6.

Our results here include detailed structural classification theorems, especially for finite nilpotent groups and for finite groups where $\Xi(G)$ has more than one nontrivial

[1] See also [34, §3] for a discussion of differences involving graphs in the hierarchy that we have not defined here.

connected component. In particular, we show that, as in the case of the generating graph, the diameter of $\Xi(G)$ is often very small. We also prove that if $G$ is a non-abelian finite simple group, then $\Xi(G)$ is connected with diameter at most 5, with smaller bounds for certain families of groups. For the baby monster group and the unitary group $\mathrm{PSU}(7,2)$, we utilise a relationship between $\Xi(G)$ and $\Delta_G$, which is related to the concept of *dual pairs* described in [34, §12].

# Chapter 2

# Preliminaries

## 2.1 Group theory preliminaries

In this chapter, we discuss several preliminary concepts and results that will be necessary later in the thesis. After focusing on abstract group theory, we will discuss the finite classical geometric spaces and use these to define the finite classical groups. This will be followed by a brief discussion of the finite simple groups. We will then conclude this chapter by considering matrices and cyclic subgroups of general linear groups. Note that the basic graph theoretic definitions and notation used in Chapters 4–6 will be summarised at the beginning of Chapter 4.

Throughout this section, $G$ denotes an arbitrary group, except where specified otherwise. We begin with a few elementary results involving subgroups, quotients and commutators of $G$.

**Lemma 2.1.1** (Dedekind's Identity [144, Lemma 1.2.3])**.** *Let $H$, $J$ and $K$ be subgroups of $G$, with $H \leqslant K$. Then $H(J \cap K) = HJ \cap K$.*

Recall that if $N$ is a normal subgroup of $G$, then $N$ is maximal in $G$ if and only if $G/N$ is cyclic of prime order. This follows from the Correspondence Theorem and the fact that the cyclic groups of prime order are precisely the nontrivial groups with no nontrivial proper subgroups. The related proposition below is a collection of well-known results; for example, see [82, Proposition 10.21].

**Proposition 2.1.2.** *Let $H$ be a group such that $H/Z(H)$ is cyclic. Then $H$ is abelian. Hence $Z(G)$ is not maximal in $G$, for any group $G$. Additionally, if $N$ and $K$ are normal subgroups of $G$, with $N$ non-abelian and $K \leqslant Z(N)$, then $G/K$ is not cyclic. In particular, $G/Z(N)$ is not cyclic.*

*Proof.* As $H/Z(H)$ is cyclic, there exists $h \in H$ such that $H/Z(H) = \langle Z(H)h \rangle$. Hence $H$ is equal to its abelian subgroup $\langle Z(H), h \rangle$. It follows that, for any group $G$, the quotient $G/Z(G)$ is not cyclic of prime order, i.e., $Z(G)$ is not maximal in $G$.

Finally, suppose that $N$ and $K$ are normal subgroups of $G$, with $N$ non-abelian and $K \leqslant Z(N)$. Then $N/Z(N)$ is not cyclic, and so neither is $G/K$. The fact that $Z(N)$ is characteristic in $N$ yields the final statement of the proposition. □

Now, in this thesis, for $x, y \in G$, we use the convention $x^y := y^{-1}xy$. Additionally, the commutator $[x, y]$ denotes $x^{-1}y^{-1}xy$. The following commutator identities can be derived directly from this definition of a commutator, and are well known (for example, see [142, p. 11]).

**Proposition 2.1.3.** *Let $x, y, z \in G$. Then:*

(i) $[y, x] = [x, y]^{-1}$;

(ii) $[x, yz] = [x, z][x, y]^z$; *and*

(iii) $[xy, z] = [x, z]^y[y, z]$.

Additionally, throughout this thesis, for a subset $S := \{g_1, g_2, \ldots\}$ of $G$, we write $\langle S\rangle^G = \langle g_1, g_2, \ldots\rangle^G$ to denote the normal closure of $S$ in $G$.

**Proposition 2.1.4.** *Let $H$ be a subgroup of $G$, and let $g \in H$.*

(i) *If $G = C_G(g)H$, then $\langle g\rangle^G \leqslant H$.*

(ii) *Suppose that $\langle g\rangle^G \leqslant H$. If $G/\langle g\rangle^G$ is abelian, then $H \trianglelefteqslant G$.*

*Proof.*

(i) Observe that $\langle g\rangle^G = \langle g^x \mid x \in G\rangle$. For each $x \in G$, we can write $x = ch$ for some $c \in C_G(g)$ and some $h \in H$. Then $g^x = g^{ch} = g^h$, and hence $\langle g\rangle^G = \langle g^h \mid h \in H\rangle$. This is equal to the subgroup $\langle g\rangle^H$ of $H$.

(ii) As $G/\langle g\rangle^G$ is abelian, it normalises its subgroup $H/\langle g\rangle^G$. Thus the Correspondence Theorem yields $H \trianglelefteqslant G$. □

### 2.1.1 Maximal subgroups

The focus of this subsection is on results related to maximal subgroups of $G$. Our first proposition here relies on Zorn's Lemma in the case where $G$ is infinite.

**Proposition 2.1.5** ([41, Proposition 2.1.1])**.** *Suppose that $G$ is finitely generated, and let $H$ be a proper subgroup of $G$. Then $H$ is contained in a maximal subgroup of $G$.*

The next few results relate to the centre of $G$, or of a maximal subgroup of $G$.

**Proposition 2.1.6.** *Let $M$ be a maximal subgroup of $G$. If $M \not\trianglelefteq G$, then $Z(G) < M$.*

*Proof.* Observe that $N_G(M) = M$. Since $Z(G) \leqslant N_G(M)$, and since $Z(G)$ is not maximal in $G$ by Proposition 2.1.2, the result follows. □

**Proposition 2.1.7.** *Let $M$ be a maximal subgroup of $G$, such that there exists $x \in Z(M) \setminus Z(G)$. Then $C_G(x) = M$, and $Z(G) < Z(M)$. Hence each element of $G \setminus Z(G)$ is central in at most one maximal subgroup of $G$.*

*Proof.* Clearly, $M \leqslant C_G(x) < G$. The maximality of $M$ therefore yields $C_G(x) = M$. Thus $Z(G) \leqslant M$, and since $x \in Z(M) \setminus Z(G)$, we conclude that $Z(G) < Z(M)$. □

**Corollary 2.1.8.** *Let $(X, Y)$ be an ordered pair of proper subgroups of $G$, with $X$ maximal and $Y \not\leqslant X$. If $Z(X) \cap Y \not\leqslant Z(G)$, then $Z(Y) \leqslant X \cap Y$. If, in addition, $X$ is abelian, then $Z(Y) \leqslant Z(G)$.*

*Proof.* Let $z$ be an element of $Z(X) \cap Y$ that does not lie in $Z(G)$. Then $X = C_G(z)$ by Proposition 2.1.7, and hence $Z(Y) \leqslant C_Y(z) = X \cap Y$. If $X$ is abelian, then each element of $Z(Y)$ is centralised by $\langle X, Y \rangle = G$, and hence $Z(Y) \leqslant Z(G)$. □

Next, we consider maximal subgroups that are normal.

**Proposition 2.1.9.** *Let $M$ be a normal maximal subgroup of $G$, and let $H$ be a subgroup of $G$ that does not lie in $M$. Then $M \cap H$ is a maximal subgroup of $H$.*

*Proof.* As $M \trianglelefteq G$ and $\langle M, H \rangle = G$, it follows that $G/M = MH/M$, which is isomorphic to $H/(M \cap H)$ by the Second Isomorphism Theorem. Since $G/M$ is cyclic of prime order, so is $H/(M \cap H)$, and the result follows. □

**Proposition 2.1.10.** *Let $(W, X, Y)$ be an ordered triple of distinct proper subgroups of $G$, with $W \cap X$ and $X$ normal in $G$, $W \cap X \not\leqslant Y$, and $Y$ maximal in $G$. If $X$ is maximal in $G$, then $X \cap Y \not\leqslant W$, while if $X \cap Y \leqslant W$, then $G/(W \cap X) \cong G/X$.*

*Proof.* Assume that $X \cap Y \leqslant W$, and observe that $(W \cap X)Y = G = XY$ and $W \cap X \cap Y = X \cap Y$. The Second Isomorphism Theorem therefore gives

$$G/(W \cap X) = (W \cap X)Y/(W \cap X) \cong Y/(W \cap X \cap Y) = Y/(X \cap Y) \cong XY/X = G/X.$$

Suppose now, for a contradiction, that $X$ is maximal in $G$. Then $|G/X|$ is equal to a prime $p$, and hence $|G/(W \cap X)| = p$. Since $W \cap X \leqslant X$, the intersection $W \cap X$ is equal to $X$. However, this contradicts the assumption that $X$ is a maximal subgroup of $G$ distinct from the proper subgroup $W$. Hence if $X$ is maximal, then in fact $X \cap Y \not\leqslant W$. □

Note that the observation regarding the finiteness of $|G/X|$ in the above proof is important. Indeed, if $H$ and $J$ are normal subgroups of $G$ of infinite index with $H \leqslant J$, then $G/H \cong G/J$ does not imply that $H = J$. In particular, if $G$ is a *non-Hopfian group*, such as the *Baumslag-Solitar group* $\mathrm{BS}(2,3)$ with presentation $\langle a, b \mid a^{-1}b^2a = b^3\rangle$, then there exists a nontrivial normal subgroup $J$ of $G$ such that $G \cong G/J$ [73, p. 63].

It will sometimes be useful to apply Proposition 2.1.10 in the case where $X$ and $Y$ are both maximal in $G$, and $W = Z(X)$ (which is characteristic in the normal subgroup $X$ and therefore normal in $G$). Thus for convenience, we state the following corollary, which is precisely the proposition with these conditions assumed.

**Corollary 2.1.11.** *Let $(X, Y)$ be an ordered pair of distinct maximal subgroups of $G$, with $X$ normal in $G$ and $Z(X) \not\leqslant Y$. Then $X \cap Y \not\leqslant Z(X)$.*

To conclude this subsection, we explore the case where $G$ has a maximal subgroup that is abelian.

**Lemma 2.1.12.** *Suppose that $G$ contains an abelian maximal subgroup. If $G$ also contains a normal, non-abelian subgroup $H$, with $Z(H) \not\leqslant Z(G)$, then $|G : H|$ is infinite. Hence every normal, non-abelian maximal subgroup $M$ of $G$ satisfies $Z(M) \leqslant Z(G)$.*

*Proof.* Let $L$ be an abelian maximal subgroup of $G$, and $H$ a normal, non-abelian subgroup of $G$ with $Z(H) \not\leqslant Z(G)$. As $L$ is abelian, the contrapositive of Corollary 2.1.8, applied to the pair $(L, H)$, yields $L \cap H = Z(L) \cap H \leqslant Z(G)$. Thus $Z(H) \not\leqslant L$ and $L \cap H \leqslant Z(H)$. Since the characteristic subgroup $Z(H)$ of $H$ is normal in $G$, applying Proposition 2.1.10 to the triple $(Z(H), H, L)$ shows that $G/Z(H) \cong G/H$. Thus $|G : H|$ is infinite, and so $H$ is not maximal in $G$. □

For the following result, note that the centraliser in $G$ of a normal subgroup $N$ is normal in $N_G(N) = G$. We write $G'$ to denote the derived subgroup $[G, G]$ of $G$.

**Proposition 2.1.13.** *Let $N$ be a normal, non-central subgroup of $G$, and let $C := C_G(N)$. Suppose also that $G/C$ is finite, and that $G$ contains an abelian maximal subgroup. Then $C$ is abelian. Furthermore, if $N$ is non-abelian and $G/C_G(C)$ is finite, then $C = Z(G)$.*

*Proof.* Notice that $N \cap C \leqslant Z(C)$. Since $G/C$ is finite, Lemma 2.1.12 shows that either $C$ is abelian or $Z(C) = Z(G)$. If $N$ is abelian, then $N \leqslant C$, and so $Z(C) \not\leqslant Z(G)$. Hence, in this case, $C$ is abelian.

Assume therefore that $N$ is non-abelian, and suppose for a contradiction that $C$ is also non-abelian, so that $Z(C) = Z(G)$. In addition, let $L$ be an abelian maximal subgroup of $G$. Then $G = LN$, and the Second Isomorphism Theorem shows that $G/N$ is isomorphic to the abelian group $L/(L \cap N)$. Similarly, $G/C$ is abelian. We deduce that $G' \leqslant N \cap C \leqslant Z(C) = Z(G)$, and so $G/Z(G)$ is also abelian. Therefore, $G$ is nilpotent of class 2, and hence $L \trianglelefteqslant G$.

Proposition 2.1.9 now shows that $L \cap N$ is a maximal subgroup of $N$. Thus $L \cap N \neq Z(N)$ by Proposition 2.1.2, i.e., $L \cap N$ contains an element $n \notin Z(N)$. In particular, $n \notin Z(G)$, and so Proposition 2.1.7 yields $C_G(n) = L$. As $C \leqslant C_G(n)$, we conclude that $C$ is abelian.

Finally, suppose that $G/C_G(C)$ is finite (with $N$ non-abelian), and assume for a contradiction that the abelian group $C$ is not equal to $Z(G)$. Then repeating the argument in the first paragraph of this proof, with $C$ and $C_G(C)$ replacing $N$ and $C$, respectively, shows that $C_G(C)$ is abelian. This contradicts the fact that $C_G(C)$ contains the non-abelian group $N$, and so $C = Z(G)$. □

### 2.1.2 Finite soluble groups

We now briefly consider finite soluble groups, including finite nilpotent groups. In this thesis, we write $\Phi(G)$ to denote the *Frattini subgroup* of $G$, i.e., the intersection of all maximal subgroups of $G$. The first result here provides important information about the quotient of a $p$-group by its Frattini subgroup.

**Theorem 2.1.14** (Burnside's Basis Theorem [124, Theorem 11.12])**.** *Let $P$ be a nontrivial $p$-group, and let $d$ be the smallest size of a generating set for $P$. Then $P/\Phi(P)$ is elementary abelian of order $p^d$. Moreover, a subset $\{x_1, \ldots, x_d\}$ of $P$ is a generating set for $P$ if and only if $\{\Phi(P)x_1, \ldots, \Phi(P)x_d\}$ is a basis for $P/\Phi(P)$, considered as a vector space over $\mathbb{F}_p$.*

**Theorem 2.1.15** ([124, Theorem 11.3])**.** *A finite group is nilpotent if and only if it is a direct product of groups of prime power order. In particular, a finite nilpotent group is the direct product of its Sylow subgroups, each of which is a normal subgroup.*

Our next theorem describes an important property of finite groups, and is in fact very useful when studying finite insoluble groups.

**Theorem 2.1.16** ([76])**.** *Suppose that $G$ is finite and contains an abelian maximal subgroup. Then $G$ is soluble.*

This theorem does not hold when $G$ is infinite. For example, the *Tarski monster groups* are infinite simple (and therefore insoluble) groups where every nontrivial

proper subgroup is cyclic of fixed prime order $p$. Ol'shanskiĭ [116] proved in 1982 that a Tarski monster group exists for each prime $p > 10^{75}$.

We recall that if $H \leqslant G$, then the *core* of $H$ in $G$ is $\mathrm{Core}_G(H) := \bigcap_{g \in G} H^g$. Observe that this is the largest normal subgroup of $G$ that lies in $H$. If $\mathrm{Core}_G(H) = 1$, then we say that $H$ is a *core-free* subgroup of $G$.

**Theorem 2.1.17** ([117, Theorem I.4, Theorem IV.11, Theorem IV.14])**.** *Suppose that $G$ is finite and soluble, and let $L$ and $M$ be distinct maximal subgroups of $G$. Then the following are equivalent:*

(i) *$L$ and $M$ are conjugate in $G$;*

(ii) *$\mathrm{Core}_G(L) = \mathrm{Core}_G(M)$; and*

(iii) *$LM \neq G$.*

### 2.1.3 Frobenius groups

In this subsection, we consider (abstract) Frobenius groups. Certain finite simple groups have maximal subgroups that are Frobenius groups, and so the results here will be useful when studying those simple groups.

**Definition 2.1.18** ([84, p. 177, p. 182])**.** A finite semidirect product $G := N{:}H$ (with $N$ and $H$ nontrivial) is a *Frobenius group* if $n^h \neq n$ for all $n \in N \setminus \{1\}$ and $h \in H \setminus \{1\}$.

This definition is closely related to that of a Frobenius permutation group; see [84, p. 183]. The next two results summarise useful properties of Frobenius groups.

**Theorem 2.1.19** ([84, Theorem 6.4])**.** *Suppose that $G$ is a finite semidirect product $N{:}H$. Then the following are equivalent.*

(i) *$G$ is a Frobenius group.*

(ii) *$H \cap H^g = 1$ for all $g \in G \setminus H$.*

(iii) *$C_G(h) \leqslant H$ for all $h \in H \setminus \{1\}$.*

(iv) *$C_G(n) \leqslant N$ for all $n \in N \setminus \{1\}$.*

**Proposition 2.1.20** ([84, Corollary 6.6])**.** *Suppose that $G$ is a Frobenius group $N{:}H$. Then each element of $G$ lies in $N$ or in a conjugate of $H$.*

### 2.1.4 Primitive groups

We now state several well-known results about primitive groups. Ballester-Bolinches and Ezquerro [6, p. 2] state the following theorem in the context of finite groups, but their proof also applies to infinite groups.

**Theorem 2.1.21.** *The group $G$ acts faithfully and primitively on some set if and only if $G$ contains a core-free maximal subgroup. In particular, a subgroup $H$ of $G$ is a point stabiliser for some faithful, primitive action of $G$ if and only if $H$ is core-free and maximal in $G$. In this case, any such action is equivalent to the usual action of $G$ on the right cosets of $H$.*

We can therefore define primitivity as a property of an abstract group, as follows.

**Definition 2.1.22.** We say that $G$ is *primitive* as an abstract group if it contains a core-free maximal subgroup. In this case, a *point stabiliser* of $G$ is any core-free maximal subgroup of $G$.

Note that in Chapter 3, we will consider primitivity as a property of permutation groups. However, in Chapter 5, as well as throughout the remainder of this subsection, we consider primitivity as a property of abstract groups.

**Proposition 2.1.23.** *Suppose that $G$ is primitive and not cyclic of prime order. Then $Z(G) = 1$.*

*Proof.* Since $G$ is primitive, it contains a core-free maximal subgroup $M$. As $G$ is not cyclic of prime order, it follows that $M \not\trianglelefteq G$. Proposition 2.1.6 therefore implies that the normal subgroup $Z(G)$ of $G$ lies in $M$, which is core-free. Thus $Z(G) = 1$. □

In the following theorem, we summarise a well-known classification of certain primitive groups according to the properties of their *minimal normal subgroups*, i.e., their nontrivial normal subgroups that are minimal by inclusion. The final part of this result follows from the fact that the penultimate subgroup in the derived series of a soluble group is normal and abelian.

**Theorem 2.1.24** ([5, pp. 119–120])**.** *Let $G$ be a primitive group with point stabiliser $M$, and suppose that $G$ contains a minimal normal subgroup $N$. Then $G = NM$, and one of the following holds.*

(i) *$N$ is the unique minimal normal subgroup of $G$, $C_G(N) = N$, and $G = N{:}M$.*

(ii) *$N$ is the unique minimal normal subgroup of $G$, and $C_G(N) = 1$.*

(iii) *There is exactly one minimal normal subgroup $K$ of $G$ distinct from $N$, the subgroups $K$ and $N$ are isomorphic, $K \cap N = 1$, $C_G(K) = N$, $C_G(N) = K$, and $G = N{:}M = K{:}M$.*

*Hence $N$ is abelian if and only if (i) holds. In particular, (i) holds if $G$ is soluble.*

It is clear that any finite primitive group contains a minimal normal subgroup. However, there exist infinite primitive groups with no minimal normal subgroups, for example the free group on two generators [59, p. 148].

## 2.2 Classical forms and geometric spaces

In this section, we describe some of the basic properties of finite classical geometric spaces. Much of this discussion is standard, and we follow the approaches of [89, §2.1] and [17, §1.5, §1.6.1].

Let $n$ be a positive integer and $q$ a prime power, and let $V$ be the vector space $\mathbb{F}_q^n$. We begin by defining standard forms on $V$.

A bilinear form $\beta : V \times V \to \mathbb{F}_q$ is called *symplectic* if $\beta(v, v) = 0$ for all $v \in V$. Note that this implies that $\beta(u, v) = -\beta(v, u)$ for all $u, v \in V$.

If $q$ is a square, then a form $\beta : V \times V \to \mathbb{F}_q$ is called *unitary* if $\beta$ is linear in the first coordinate and $\beta(v, u) = \beta(u, v)^\sigma$ for all $u, v \in V$, where $\sigma$ is the unique involution of $\mathrm{Aut}(\mathbb{F}_q)$. This implies that $\beta(\alpha u, \gamma v) = \alpha\gamma^\sigma\beta(u, v)$ for all $\alpha, \gamma \in \mathbb{F}_q$ and $u, v \in V$.

Finally, let $Q : V \to \mathbb{F}_q$ be a map such that $Q(\alpha v) = \alpha^2 Q(v)$ for all $\alpha \in \mathbb{F}_q$ and $v \in V$, and let $\beta_Q : V \times V \to \mathbb{F}_q$ be the associated map satisfying $\beta_Q(u, v) = Q(u + v) - Q(u) - Q(v)$ for all $u, v \in V$. If $\beta_Q$ is a bilinear form with $\beta_Q(u, v) = \beta_Q(v, u)$ for all $u, v \in V$, then we say that $Q$ is a *quadratic form* with *polar form* $\beta_Q$. Observe that $\beta_Q(u, u) = 2Q(u)$, and in particular, $\beta_Q$ is symplectic if $q$ is even.

Now, let $\kappa$ be a *classical form* on $V$, i.e., the zero bilinear form on $V$ or a symplectic, unitary or quadratic form on $V$. Then $(V, \kappa)$ is called a *classical geometry*. We also call $(V, \kappa)$ a *symplectic space*, a *unitary space* or a *quadratic space* if $\kappa$ is symplectic, unitary or quadratic, respectively. If $\kappa$ is quadratic, then let $\beta := \beta_\kappa$, and otherwise let $\beta := \kappa$. We will often write $(u, v) := \beta(u, v)$ for $u, v \in V$, and similarly for other bilinear and unitary forms throughout this thesis.

Fixing a basis $\{e_1, e_2, \ldots, e_n\}$ for $V$, we can define a matrix $M_\kappa = (m_{ij})_{n\times n}$ over

$\mathbb{F}_q$, associated with $\kappa$. If $\kappa$ is quadratic, then

$$m_{ij} = \begin{cases} (e_i, e_j), & \text{if } i < j; \\ \kappa(e_i), & \text{if } i = j; \\ 0, & \text{if } i > j. \end{cases}$$

Otherwise, $M_\kappa$ is the *Gram matrix* associated with $\kappa$, so that $m_{ij} = (e_i, e_j)$ for all $i$ and $j$. In each case, we can define the Gram matrix $M_\beta$. In particular, if $\kappa$ is quadratic, then $M_\beta = M_\kappa + M_\kappa^T$.

The matrices $M_\kappa$ and $M_\beta$ encode the images of vectors or pairs of vectors under the relevant forms, as follows. Let $u, v \in V$, and let $\sigma$ be the unique involution of $\mathrm{Aut}(\mathbb{F}_q)$ if $\kappa$ is unitary, or the identity of $\mathrm{Aut}(\mathbb{F}_q)$ otherwise. Additionally, write $v^{\sigma T}$ to denote the transpose of the vector obtained by applying $\sigma$ to each entry in $v$. Then $(u, v)$ is the unique entry of the matrix $uM_\beta v^{\sigma T}$, and if $\kappa$ is quadratic, then $\kappa(u)$ is the unique entry of $uM_\kappa u^T$. We also note that if $\kappa$ is quadratic and $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$, then

$$\kappa(\sum_{i=1}^{n} \alpha_i e_i) = \sum_{i=1}^{n} \alpha_i^2 \kappa(e_i) + \sum_{\substack{i,j=1 \\ i<j}}^{n} \alpha_i \alpha_j (e_i, e_j). \tag{2.2.1}$$

In addition, we will see shortly that the matrices $M_\kappa$ and $M_\beta$ provide useful information about the forms themselves, and about elements of $\mathrm{GL}(n, q)$ that (in a certain sense) preserve the space $(V, \kappa)$.

We now turn our attention to the subspaces of $(V, \kappa)$.

**Definition 2.2.1** ([89, p. 17])**.** Let $W$ be a subspace of $(V, \kappa)$. Then the *perpendicular space* of $W$ (with respect to $(V, \kappa)$) is the subspace

$$W^\perp := \{v \in V \mid (v, w) = 0 \text{ for all } w \in W\}$$

of $V$. Additionally, the *radical* of $W$ (with respect to the restriction $\kappa|_W$) is the subspace $W \cap W^\perp$.

Note that the term "perpendicular space" is from [148, p. 55]. Additionally, for each $v, w \in V$, the equality $(v, w) = 0$ holds if and only if $(w, v) = 0$.

Now, we say that $\kappa$ is *non-degenerate* if $V^\perp = \{0\}$, and *degenerate* otherwise. In fact, $\kappa$ is non-degenerate if and only if $\det(M_\beta) \neq 0$, so that $M_\beta \in \mathrm{GL}(n, q)$. Similarly, a subspace $W$ of $(V, \kappa)$ is called *non-degenerate* if the restriction $\kappa|_W$ is non-degenerate, i.e., if the radical of $W$ is zero, and *degenerate* otherwise. If instead $\kappa|_W$ is the zero form, then we say that $W$ is *totally singular*. Finally, if $\beta|_W$ is the zero form, so that $W$ is its own radical, then we call $W$ *totally isotropic*.

By definition, if $\beta = \kappa$, then a subspace of $V$ is totally isotropic if and only if it is totally singular. Moreover, if $\kappa$ is quadratic, then it follows from the definition of $\beta_\kappa$ that each totally singular subspace is totally isotropic, and the converse holds when $q$ is odd. However, this is not the case when $q$ is even. For example, when $\kappa$ is quadratic and $q$ is even, $\beta$ is symplectic and so every one-dimensional subspace of $V$ is totally singular. However, if $v \in V$ satisfies $Q(v) \neq 0$, then the subspace $\langle v \rangle$ is not totally isotropic. We call such a one-dimensional subspace *nonsingular*.

The following lemma highlights important properties of subspaces of $(V, \kappa)$ when $\kappa$ is non-degenerate.

**Lemma 2.2.2** ([89, Lemma 2.1.5])**.** *Suppose that $\kappa$ is non-degenerate, and let $W$ be a subspace of $(V, \kappa)$. Then:*

(i) $\dim(W^\perp) = \dim(V) - \dim(W)$;

(ii) $(W^\perp)^\perp = W$;

(iii) *$W$ is totally isotropic if and only if $W \subseteq W^\perp$; and*

(iv) *$W$ is non-degenerate if and only if $V = W \oplus W^\perp$.*

In particular, $W^\perp$ is non-degenerate if and only if $W$ is non-degenerate.

The following proposition is elementary.

**Proposition 2.2.3.** *Suppose that $\kappa$ is non-degenerate, and let $U$ and $W$ be subspaces of $(V, \kappa)$. Then $U \subseteq W$ if and only if $W^\perp \subseteq U^\perp$.*

*Proof.* Suppose first that $U \subseteq W$. Then any vector $v \in W^\perp$ satisfies $(v, u) = 0$ for all $u \in U$, and so $v \in U^\perp$. Thus $W^\perp \subseteq U^\perp$. Since $(W^\perp)^\perp = W$ and $(U^\perp)^\perp = U$ by Lemma 2.2.2, the same argument proves the converse. □

Let $V'$ be another vector space of dimension $n$ over $\mathbb{F}_q$, and let $\kappa'$ be a classical form on $V'$, with $\kappa'$ quadratic if and only if $\kappa$ is quadratic. If $\kappa$ is quadratic, then let $r \in V$, and otherwise let $r$ be an ordered pair of vectors in $V$. An invertible linear map $g$ from $(V, \kappa)$ to $(V', \kappa')$ is called a *similarity* if there exists $\alpha \in \mathbb{F}_q^\times$ (independent from $r$) such that $\kappa'(r^g) = \alpha\kappa(r)$ for all choices of $r$. If such a similarity exists, then we say that $(V, \kappa)$ and $(V', \kappa')$ are *similar*. A similarity with $\alpha = 1$ is called an *isometry*, and if there exists an isometry from $(V, \kappa)$ to $(V', \kappa')$, then we say that $(V, \kappa)$ and $(V', \kappa')$ are *isometric*.

Observe that if $\kappa$ and $\kappa'$ are quadratic forms such that $(V, \kappa)$ and $(V', \kappa')$ are similar or isometric, then $(V, \beta_\kappa)$ and $(V', \beta_{\kappa'})$ are also similar or isometric, respectively.

The following is an incredibly important result about isometric vector spaces.

**Lemma 2.2.4** (Witt's Lemma [89, Proposition 2.1.6]). *Suppose that the vector spaces $(V, \kappa)$ and $(V', \kappa')$ are isometric. Additionally, let $W$ and $W'$ be subspaces of $V$ and $V'$, respectively. If there exists an isometry $\theta : (W, \kappa|_W) \to (W', \kappa'|_{W'})$, then $\theta$ extends to an isometry from $(V, \kappa)$ to $(V', \kappa')$.*

We will now focus on the case $(V', \kappa') = (V, \kappa)$, where Witt's Lemma is particularly useful. For example, the following result about maximal (with respect to inclusion) totally singular subspaces is a consequence of the lemma.

**Corollary 2.2.5** ([89, Corollary 2.1.7]). *All maximal totally singular subspaces of $(V, \kappa)$ are equidimensional.*

Now, a *similarity* of $\kappa$ is a similarity from $(V, \kappa)$ to itself, and an *isometry* of $\kappa$ is an isometry from $(V, \kappa)$ to itself. It is clear that the set of similarities of $\kappa$ and the set of isometries of $\kappa$ are subgroups of $\mathrm{GL}(n, q)$, and we call these the *similarity group* of $\kappa$ and the *isometry group* of $\kappa$, respectively.

We can also define transformations of $(V, \kappa)$ that are more general than similarities. For an automorphism $\theta$ of $\mathbb{F}_q$, a transformation $g : V \to V$ is called *$\theta$-semilinear* if $(u+v)^g = u^g + v^g$ and $(\lambda u)^g = \lambda^\theta u^g$ for all $u, v \in V$ and $\lambda \in \mathbb{F}_q$. The *general semilinear group* $\Gamma\mathrm{L}(n, q)$ is the group (under composition) of all invertible $\theta$-semilinear transformations of $V$, for all $\theta \in \mathrm{Aut}(\mathbb{F}_q)$. With $r$ as above, a $\theta$-semilinear transformation $g \in \Gamma\mathrm{L}(n, q)$ is a *semisimilarity* of $\kappa$ if there exists a fixed scalar $\alpha \in \mathbb{F}_q^\times$ such that $\kappa(r^g) = \alpha\kappa(r)^\theta$ for all choices of $r$. The set of these semisimilarities forms the *semisimilarity group* of $\kappa$.

Note also that $\Gamma\mathrm{L}(n, q)$ may be defined as the semidirect product of $\mathrm{GL}(n, q)$ and its group of *field automorphisms*, which corresponds to the group of field automorphisms of $\mathbb{F}_q$. Namely, if $\phi$ is a field automorphism of $\mathbb{F}_q$, then (with a slight abuse of notation) we can consider $\phi$ as the automorphism of $\mathrm{GL}(n, q)$ that maps a matrix $A \in \mathrm{GL}(n, q)$ to the matrix $A^\phi$, obtained by applying $\phi$ to each entry of $A$.

The following lemma provides a useful description of the isometry group of $\kappa$, in terms of the matrices $M_\beta$ and $M_\kappa$.

**Lemma 2.2.6** ([17, Lemma 1.5.21]). *If $\kappa$ is unitary, then let $\sigma$ be the unique involution of $\mathrm{Aut}(\mathbb{F}_q)$, and otherwise let $\sigma := 1$. Additionally, let $A \in \mathrm{GL}(n, q)$. If $\kappa$ is quadratic, then $A$ is an isometry of $\kappa$ if and only if $AM_\beta A^T = M_\beta$, and each diagonal entry of $M_\kappa$ is equal to the corresponding diagonal entry of $AM_\kappa A^T$. Otherwise, $A$ is an isometry of $\kappa$ if and only if $AM_\kappa A^{\sigma T} = M_\kappa$.*

Our next result, which is elementary, will be useful when proving lower bounds for base sizes of certain primitive subspace actions.

**Lemma 2.2.7.** *Let $g$ be an isometry of $\kappa$, and $U$ a subspace of $V$. Then $(U^\perp)^g = (U^g)^\perp$. Hence if a subgroup $G$ of the isometry group of $\kappa$ acts transitively on a set $\mathcal{U}$ of subspaces of $V$, then $G$ also acts transitively on $\{U^\perp \mid U \in \mathcal{U}\}$.*

*Proof.* Observe from the definition of $U^\perp$ that

$$(U^\perp)^g = \{v^g \mid v \in V \text{ and } (v,u) = 0 \text{ for all } u \in U\}.$$

As $g$ is an isometry of $\kappa$, this is equal to $\{v^g \mid v \in V \text{ and } (v^g, u^g) = 0 \text{ for all } u \in U\}$, which is in turn equal to $(U^g)^\perp$. □

The above lemma immediately yields the following corollary, which is well known (see, for example, [25, p. 39]).

**Corollary 2.2.8.** *Let $g$ be an isometry of $\kappa$, and let $U$ be a subspace of $V$. If $g$ stabilises $U$, then $g$ also stabilises $U^\perp$.*

### 2.2.1 Non-degenerate finite classical forms

In this subsection, we explicitly describe the non-degenerate classical forms $\kappa$ on $V = \mathbb{F}_q^n$. As we will see in §2.3, any finite classical group can be defined in relation to the isometry group of such a form, or of a zero bilinear form.

**Lemma 2.2.9** ([89, Propositions 2.3.1, 2.4.1, 2.5.1 and 2.5.4])**.**

(i) *Up to isometry, there is a unique non-degenerate unitary form on $V$ (assuming that $q$ is a square).*

(ii) *If $n$ is even, then, up to isometry, there is a unique non-degenerate symplectic form on $V$. If instead $n$ is odd, then there is no non-degenerate symplectic form on $V$.*

(iii) *If $n$ is even or $q$ is odd, then, up to isometry, there are exactly two distinct non-degenerate quadratic forms on $V$, and these two forms are similar if and only if $n$ is odd. If instead $n$ is odd and $q$ is even, then there is no non-degenerate quadratic form on $V$.*

It can be shown that if $\kappa$ and $\kappa'$ are similar non-degenerate quadratic forms on $V$, then their isometry groups are conjugate subgroups of $\mathrm{GL}(n,q)$. Hence, for our purposes, we do not usually need to distinguish between the two isometry classes of

non-degenerate quadratic forms when $n$ is odd, and we say that any such form is of type $\circ$. However, it is important to distinguish between the two isometry classes when $n$ is even. As such, when $n$ is even, we refer to non-degenerate quadratic forms of *plus type* and *minus type*; we will distinguish between these shortly. It is sometimes convenient to use the symbols $+$ and $-$ in these respective cases.

We conclude this section by fixing the standard non-degenerate forms that we will use in this thesis, by defining the corresponding matrices $M_\kappa$ and $M_\beta$. In particular, any non-degenerate unitary, symplectic or quadratic form corresponds to one such set of matrices, up to similarity if $\kappa$ is quadratic and $n$ is odd, or up to isometry otherwise. Conversely, any unitary, symplectic or quadratic form with matrices equal to those below (with $q$ and $n$ as appropriate) is a non-degenerate form of the corresponding type.

Here, for a positive integer $k$, we write $A_k$ to denote the $k \times k$ antidiagonal matrix with each antidiagonal entry equal to 1, and $Z_k$ to denote the $k \times k$ zero matrix.

**Proposition 2.2.10** ([17, p. 20])**.** *Suppose that $q$ is a square. Then there exists a non-degenerate unitary form $\kappa$ on $V$, such that $M_\kappa = M_\beta$ is the $n \times n$ identity matrix over $\mathbb{F}_q$.*

**Proposition 2.2.11** ([17, p. 19])**.** *Suppose that $n$ is even. Then there exists a non-degenerate symplectic form $\kappa$ on $V$, such that $M_\kappa = M_\beta$ is the (antidiagonal) block matrix* $\mathrm{antidiag}(A_{n/2}, -A_{n/2})$.

**Proposition 2.2.12** ([89, pp. 26–27])**.**

(i) *Suppose that $n$ and $q$ are odd. Then there exists a non-degenerate quadratic form $\kappa$ on $V$, such that $M_\kappa$ is the block matrix* $\mathrm{antidiag}(A_{(n+1)/2}, Z_{(n-1)/2})$.

(ii) *Suppose that $n$ is even. Then there exists a non-degenerate quadratic form $\kappa$ of plus type on $V$, such that $M_\kappa$ is the block matrix* $\mathrm{antidiag}(A_{n/2}, Z_{n/2})$.

(iii) *Suppose that $n$ is even. Then there exists a non-degenerate quadratic form $\kappa$ of minus type on $V$ and an element $\zeta \in \mathbb{F}_q^\times$, such that $M_\kappa$ is the block matrix* $\mathrm{antidiag}(A_{n/2-1}, \begin{pmatrix} 1 & 1 \\ 0 & \zeta \end{pmatrix}, Z_{n/2-1})$ *and the polynomial $x^2 + x + \zeta$ is irreducible over $\mathbb{F}_q$.*

*In each case, $M_\beta = M_\kappa + M_\kappa^T$.*

## 2.3 The finite classical groups

Each non-degenerate finite classical form described in §2.2.1, as well as each zero classical form on a finite vector space, is associated with a family of *classical groups*. In this section, we define the groups in each of these families, following the approaches of [89, Ch. 2] and [17, §1.6–1.7].

Let $V$ be a vector space of finite dimension $n \geqslant 2$ over a finite field $\mathbb{F}$, equipped with a non-degenerate or zero classical form $\kappa$. Recall that $|\mathbb{F}|$ must be a square in order for $\kappa$ to be unitary. We therefore assume that $\mathbb{F} = \mathbb{F}_{q^u}$ for some prime power $q$, where $u = 2$ if $\kappa$ is unitary, and $u = 1$ otherwise.

We define a chain

$$\Omega(\kappa) \leqslant S(\kappa) \leqslant I(\kappa) \leqslant \Delta(\kappa) \leqslant \Gamma(\kappa) \leqslant A(\kappa) \tag{2.3.1}$$

of subgroups related to $\kappa$, and their projective versions

$$\mathrm{P}\Omega(\kappa) \leqslant \mathrm{P}S(\kappa) \leqslant \mathrm{P}I(\kappa) \leqslant \mathrm{P}\Delta(\kappa) \leqslant \mathrm{P}\Gamma(\kappa) \leqslant \mathrm{P}A(\kappa), \tag{2.3.2}$$

as follows.

**Definition 2.3.1.** The groups $I(\kappa)$, $\Delta(\kappa)$ and $\Gamma(\kappa)$ are the isometry group of $\kappa$, the similarity group of $\kappa$, and the semisimilarity group of $\kappa$, respectively, as defined in §2.2. Additionally, $S(\kappa) := I(\kappa) \cap \mathrm{SL}(n, q^u)$. If $\kappa$ is nonzero, then $A(\kappa) := \Gamma(\kappa)$, and if $\kappa$ is not quadratic, then $\Omega(\kappa) := S(\kappa)$. For each group $X$ in (2.3.1), the corresponding group $\mathrm{P}X$ in (2.3.2) is equal to $X/(Z(\mathrm{GL}(n, q^u)) \cap X)$, the quotient of $X$ by its subgroup of scalar matrices.

We will define $A(\kappa)$ in the case $\kappa = 0$, and $\Omega(\kappa)$ in the quadratic case, in the corresponding subsections below.

For the most part, a *finite classical group* related to $\kappa$ is any subgroup $H$ satisfying $\Omega(\kappa) \leqslant H \leqslant A(\kappa)$, or its projective version $\mathrm{P}H$. In most cases, $\mathrm{P}A(\kappa) = \mathrm{Aut}(\mathrm{P}\Omega(\kappa))$, but we will see in the subsections below that there are certain families of exceptions. In these exceptional cases, with $n = 8$ if $\kappa$ is quadratic, we also consider a group $K$ satisfying $\mathrm{P}\Omega(\kappa)' \leqslant K \leqslant \mathrm{Aut}(\mathrm{P}\Omega(\kappa))$ as a finite classical group related to $\kappa$. Among these exceptions, if $\mathrm{P}\Omega(\kappa)' \neq \mathrm{P}\Omega(\kappa)$, then $\kappa$ is symplectic and $V = \mathbb{F}_2^4$. We will see in §2.4 why this derived subgroup is included here.

Note that each subgroup in (2.3.1) is normal in $A(\kappa)$, and similarly, each subgroup in (2.3.2) is normal in $\mathrm{P}A(\kappa)$. Additionally, $\mathrm{P}\Delta(\kappa) \leqslant \mathrm{PGL}(n, q^u)$, as each similarity of $\kappa$ is an invertible linear transformation of $V$.

The following result is well known.

**Proposition 2.3.2.** *Let $G$ be a subgroup of $\mathrm{GL}(n, q^u)$ that contains $\Omega(\kappa)$, and suppose that $n \geqslant 3$ if $\kappa$ is quadratic. Then $Z(G) = G \cap Z(\mathrm{GL}(n, q^u))$.*

*Proof.* By [17, Proposition 1.12.2] (see also [17, Table 1.2] or the more detailed descriptions of the groups $\Omega(\kappa)$ in the subsections below), $\Omega(\kappa)$ acts absolutely irreducibly on the vector space $\mathbb{F}_{q^u}^n$. Therefore, $G$ also acts absolutely irreducibly on this vector space. We now deduce from Schur's Lemma (see [17, p. 38]) that the centraliser of $G$ in $\mathrm{GL}(n, q^u)$ is equal to $Z(\mathrm{GL}(n, q^u))$, and the result follows. □

For convenience, we define the following.

**Definition 2.3.3.** Let $G$ be a classical subgroup related to $\kappa$. The *natural module* for $G$ is the geometric space $(V, \kappa)$.

Note that the action of a given subgroup of $\Gamma(\kappa)$ on the set of subspaces of $(V, \kappa)$ induces on this set an action of the corresponding subgroup of $\mathrm{P}\Gamma(\kappa)$. In fact, we will see below that any subgroup of $\mathrm{P}A(\kappa)$ has a natural action on this set.

We now briefly discuss, in more detail, the classical groups corresponding to each type of the form $\kappa$. In particular, we specify each subgroup in (2.3.1) using the notation of [17, §1.6.2], and describe each subgroup in (2.3.2) as a group of automorphisms of $\mathrm{P}\Omega(\kappa)$. Any such automorphism is a product of inner, *field*, *diagonal* and *graph* automorphisms [17, Proposition 5.1.1], and $\mathrm{P}\Omega(\kappa)$ has no nontrivial field automorphisms if and only if $q^u$ is prime.

Note also that [17, §1.6.4] yields $|K|$ for each group $K$ in (2.3.1) or (2.3.2). We can also use [17, §1.6.4] together with Proposition 2.3.2 to determine $|Z(K)|$ for the groups $K$ in (2.3.1) that lie in $\mathrm{GL}(n, q^u)$, assuming that $\kappa$ is not quadratic if $n = 2$.

### 2.3.1 Linear classical groups

Assume that $\kappa$ is the zero form. Then we say that each classical group associated with $\kappa$ is *linear*. In particular, $\Omega(\kappa) = S(\kappa) = \mathrm{SL}(n, q)$; $I(\kappa) = \Delta(\kappa) = \mathrm{GL}(n, q)$; and $\Gamma(\kappa) = \Gamma\mathrm{L}(n, q)$. We will now define $A(\kappa)$ in the linear case.

**Definition 2.3.4.** If $n = 2$, then $A(\kappa) := \Gamma(\kappa)$. Otherwise $A(\kappa) := \Gamma\mathrm{L}(n, q) : \langle\gamma\rangle$, where $\gamma$ is the *duality automorphism* of $\mathrm{SL}(n, q)$, i.e., the automorphism that maps each matrix to its inverse transpose.

The group $\mathrm{PGL}(n, q)$ consists of the inner and diagonal automorphisms of the group $\mathrm{PSL}(n, q)$, while $\mathrm{P}\Gamma\mathrm{L}(n, q)$ consists of the inner, diagonal and field automorphisms of $\mathrm{PSL}(n, q)$. If $n \geqslant 3$, then $\mathrm{P}A(\kappa)$ is generated by $\mathrm{P}\Gamma\mathrm{L}(n, q)$ and the

graph automorphism of $\mathrm{PSL}(n,q)$, which is induced by the duality automorphism of $\mathrm{SL}(n,q)$. In each case, $\mathrm{P}A(\kappa) = \mathrm{Aut}(\mathrm{PSL}(n,q))$.

The following proposition yields information about the aforementioned natural action of $\mathrm{P}A(\kappa)$ on the set of subspaces of $(V,\kappa)$. As above, the action of the subgroup $\mathrm{P\Gamma L}(n,q)$ of $\mathrm{P}A(\kappa)$ is induced by the action of $\Gamma\mathrm{L}(n,q)$.

**Proposition 2.3.5.** *Suppose that $n \geqslant 3$, let $V$ be the natural module for $\mathrm{PSL}(n,q)$, and let $\mathcal{U}$ be the set of subspaces of $V$. Additionally, let $\mathcal{A}$ be the group of bijections $\alpha : \mathcal{U} \to \mathcal{U}$ such that $U \subseteq W$ if and only if $U^\alpha \subseteq W^\alpha$, for all $U, W \in \mathcal{U}$, and $\mathcal{B}$ the set of bijections $\gamma : \mathcal{U} \to \mathcal{U}$ such that $U \subseteq W$ if and only if $W^\gamma \subseteq U^\gamma$. Then:*

(i) *$\mathcal{A} = \mathrm{P\Gamma L}(n,q)$, and $\mathcal{B} = \mathrm{Aut}(\mathrm{PSL}(n,q)) \setminus \mathrm{P\Gamma L}(n,q)$; and*

(ii) *$\dim(U^\gamma) = n - \dim(U)$ for each $\gamma \in \mathcal{B}$.*

*Proof.* The claim (i) is from [137, p. 51, p. 66]. To prove (ii), note that the zero subspace of $V$ is the unique subspace contained in every subspace, while $V$ is the unique subspace containing every subspace. Similarly, the one-dimensional subspaces are the only subspaces that properly contain a single subspace (i.e., $\{0\}$), while the $(n-1)$-dimensional subspaces are the only subspaces properly contained in a single subspace (i.e., $V$). Proceeding by induction, and using the fact that $\gamma$ reverses inclusion of subspaces, we obtain (ii). □

### 2.3.2 Unitary classical groups

Suppose now that $\kappa$ is a non-degenerate unitary form. The associated classical groups are the *unitary groups*. Note that we write $\mathrm{SU}(n,q)$ to denote $\Omega(\kappa) = S(\kappa)$, even though this is a group of matrices defined over $\mathbb{F}_{q^2}$. Additionally, $\mathrm{GU}(n,q) := I(\kappa)$; $\mathrm{CGU}(n,q) := \Delta(\kappa)$; and $\mathrm{C\Gamma U}(n,q) := \Gamma(\kappa) = A(\kappa)$.

Now, $\mathrm{PGU}(n,q) = \mathrm{PCGU}(n,q)$ consists of the inner and diagonal automorphisms of $\mathrm{PSU}(n,q)$, while $\mathrm{PC\Gamma U}(n,q)$ consists of the inner, diagonal, field and graph automorphisms of $\mathrm{PSU}(n,q)$. Furthermore, $\mathrm{PC\Gamma U}(n,q) = \mathrm{Aut}(\mathrm{PSU}(n,q))$.

### 2.3.3 Symplectic classical groups

We now assume that $\kappa$ is a non-degenerate symplectic form. The associated classical groups are the *symplectic groups*. Here, $\mathrm{Sp}(n,q) := \Omega(\kappa) = S(\kappa) = I(\kappa)$; $\mathrm{CSp}(n,q) := \Delta(\kappa)$; and $\mathrm{C\Gamma Sp}(n,q) := \Gamma(\kappa) = A(\kappa)$. We note that $|Z(\mathrm{Sp}(n,q)| = (2, q-1)$, and so $\mathrm{Sp}(n,q) \cong \mathrm{PSp}(n,q)$ if $q$ is even.

The group $\mathrm{PCSp}(n,q)$ consists of the inner and diagonal automorphisms of $\mathrm{PSp}(n,q)$, while $\mathrm{PC\Gamma Sp}(n,q)$ consists of the inner, diagonal and field automorphisms of $\mathrm{PSp}(n,q)$. The group $\mathrm{PC\Gamma Sp}(n,q)$ is equal to $\mathrm{Aut}(\mathrm{PSp}(n,q))$, unless $n=4$ and $q$ is even, in which case $\mathrm{Aut}(\mathrm{PSp}(n,q))$ contains the additional graph automorphisms of $\mathrm{PSp}(n,q)$.

### 2.3.4 Orthogonal classical groups

Finally, suppose that $\kappa$ is a non-degenerate orthogonal form of type $\varepsilon \in \{\circ,+,-\}$. The associated classical groups are the *orthogonal groups*. In this case, $\mathrm{SO}^\varepsilon(n,q) := S(\kappa)$; $\mathrm{GO}^\varepsilon(n,q) := I(\kappa)$; $\mathrm{CGO}^\varepsilon(n,q) := \Delta(\kappa)$; and $\mathrm{C\Gamma O}^\varepsilon(n,q) := \Gamma(\kappa) = A(\kappa)$. We now extend the definition of (2.3.1), and hence of (2.3.2).

**Definition 2.3.6.** If $(n,q,\varepsilon) \neq (4,2,+)$, then $\Omega^\varepsilon(n,q) := \Omega(\kappa)$ is the unique subgroup of $\mathrm{SO}^\varepsilon(n,q)$ of index two.

For alternative definitions of $\Omega^\varepsilon(n,q)$, including in the case $(n,q,\varepsilon) = (4,2,+)$ where this group is one of three subgroups of $\mathrm{SO}^+(4,2)$ of index two, see [89, pp. 29–31]. Note that when $\varepsilon = \circ$ (i.e., when $n$ is odd), we do not include $\circ$ in the notation for the orthogonal classical groups. For example, we write $\Omega(n,q)$ instead of $\Omega^\circ(n,q)$.

Observe from Proposition 2.3.2 that if $n$ is odd, then $Z(\mathrm{GO}(n,q))$ has order 2, while $\mathrm{SO}(n,q)$ and $\Omega(n,q)$ have trivial centres. For even $n \geqslant 4$, the centres of $\mathrm{GO}^\varepsilon(n,q)$ and $\mathrm{SO}^\varepsilon(n,q)$ each have order $(2,q-1)$. The same is true for $\Omega^\varepsilon(n,q)$, unless either $\varepsilon = +$ and $4 \mid (q^{n/2}+1)$, or $\varepsilon = -$ and $4 \mid (q^{n/2}-1)$, in which case the group has trivial centre. Thus $\Omega^\varepsilon(n,q) \cong \mathrm{P}\Omega^\varepsilon(n,q)$ in this last case, as well as when $n$ is odd or $q$ is even.

Recall Lemma 2.2.6, which gives a necessary and sufficient condition for a matrix in $\mathrm{GL}(n,q)$ to lie in $I(\kappa)$. The following result describes precisely when a matrix in $S(\kappa)$ lies in $\Omega(\kappa)$, in the case where $q$ is even and $(n,q,\varepsilon) \neq (4,2,+)$. Here, $I_n$ denotes the $n \times n$ identity matrix over $\mathbb{F}_q$.

**Proposition 2.3.7** ([17, Proposition 1.6.11(i), Definition 1.6.13])**.** *Suppose that $q$ is even and $(n,q,\varepsilon) \neq (4,2,+)$, and let $A \in \mathrm{SO}^\varepsilon(n,q)$. Then $A \in \Omega^\varepsilon(n,q)$ if and only if the matrix $I_n + A$ has even rank.*

See [17, Proposition 1.6.11(ii), Definition 1.6.13] for a corresponding result when $q$ is odd.

Finally, suppose that $n \geqslant 3$, with $\varepsilon = -$ if $n = 4$. Then $\mathrm{Aut}(\mathrm{P}\Omega^\varepsilon(n,q)) = \mathrm{P}A(\kappa)$, unless $(n,\varepsilon) = (8,+)$, in which case $\mathrm{Aut}(\mathrm{P}\Omega^+(8,q)) \setminus \mathrm{P}A(\kappa)$ contains the *triality* graph automorphisms of $\mathrm{P}\Omega^+(8,q)$ (see [89, Theorem 2.1.4, p. 38]). For a more

detailed discussion of the relationship between the subgroups in (2.3.2) and the automorphisms of $\mathrm{P}\Omega^{\varepsilon}(n,q)$, see [17, §1.7].

## 2.4 The finite simple groups

In this section, we summarise important and useful information about the finite simple groups. Except where stated otherwise, the information in this section is well known and can be found in, for example, [89, §5.1] and [17, Ch. 1.10].

We begin with a brief overview of the classification of finite simple groups. In what follows, $p$ denotes a prime, $q$ a prime power, $i$ an odd positive integer, $n$ an integer at least 2, and $\varepsilon \in \{\circ, +, -\}$. These integers can take arbitrary values, except where specified otherwise. Note that the following theorem describes a set of groups that properly contains the set of finite simple groups; the non-simple groups in this set are specified below.

**Theorem 2.4.1.** *Each finite simple group is isomorphic to one of the following:*

- *a cyclic group* $C_p$*;*
- *an alternating group* $A_n$ *(*$n \geqslant 5$*);*
- *a classical group of Lie type* $\mathrm{PSL}(n,q)$*,* $\mathrm{PSU}(n,q)$*,* $\mathrm{PSp}(n,q)$ *or* $\mathrm{P}\Omega^{\varepsilon}(n,q)$*;*
- *an exceptional group of Lie type* $\mathrm{Sz}(q) = {}^2B_2(q)$ *(*$q = 2^i$*),* ${}^2G_2(q)$ *(*$q = 3^i$*),* $G_2(q)$*,* ${}^3D_4(q)$*,* ${}^2F_4(q)$ *(*$q = 2^i$*),* $F_4(q)$*,* ${}^2E_6(q)$*,* $E_6(q)$*,* $E_7(q)$ *or* $E_8(q)$*;*
- *the Tits group* ${}^2F_4(2)'$*; or*
- *a sporadic group:*
  - *a Mathieu group* $\mathrm{M}_{11}$*,* $\mathrm{M}_{12}$*,* $\mathrm{M}_{22}$*,* $\mathrm{M}_{23}$ *or* $\mathrm{M}_{24}$*;*
  - *a Janko group* $\mathrm{J}_1$*,* $\mathrm{J}_2$*,* $\mathrm{J}_3$ *or* $\mathrm{J}_4$*;*
  - *a Conway group* $\mathrm{Co}_1$*,* $\mathrm{Co}_2$ *or* $\mathrm{Co}_3$*;*
  - *a Fischer group* $\mathrm{Fi}_{22}$*,* $\mathrm{Fi}_{23}$ *or* $\mathrm{Fi}'_{24}$*; or*
  - *the Higman-Sims group* HS*, the McLaughlin group* McL*, the Held group* He*, the Rudvalis group* Ru*, the Suzuki group* Suz*, the O'Nan group* O'N*, the Harada-Norton group* HN*, the Lyons group* Ly*, the Thompson group* Th*, the baby monster group* $\mathbb{B}$*, or the monster group* $\mathbb{M}$*.*

Similarly to the classical groups, each exceptional group of Lie type is defined with respect to a finite field $\mathbb{F}_q$. The *defining characteristic* of a classical or exceptional group of Lie type is the unique prime $p$ dividing $q$. For definitions of the exceptional and sporadic groups, see, for example, [148, Ch. 4–5]. In this thesis (specifically, in Chapter 6), we will consider the Tits group together with the sporadic groups.

Now, a given group in Theorem 2.4.1 is simple if and only if it is not isomorphic to one of $\mathrm{PSL}(2,2)$, $\mathrm{PSL}(2,3)$, $\mathrm{PSU}(3,2)$, $\mathrm{PSp}(4,2)$, $\mathrm{P\Omega}^{\pm}(2,q)$, $\mathrm{P\Omega}^{+}(4,q)$, $\mathrm{Sz}(2)$, $G_2(2)$, ${}^2G_2(3)$ or ${}^2F_4(2)$. We also note that, up to isomorphism, certain families of groups and individual groups appear more than once in Theorem 2.4.1:

$$\mathrm{P\Omega}(3,q) \cong \mathrm{PSU}(2,q) \cong \mathrm{PSp}(2,q) = \mathrm{PSL}(2,q); \quad \mathrm{P\Omega}^{-}(4,q) \cong \mathrm{PSL}(2,q^2);$$

$$\mathrm{P\Omega}(5,q) \cong \mathrm{PSp}(4,q); \quad \mathrm{P\Omega}^{+}(6,q) \cong \mathrm{PSL}(4,q); \quad \mathrm{P\Omega}^{-}(6,q) \cong \mathrm{PSU}(4,q);$$

$$\mathrm{PSL}(2,4) \cong \mathrm{PSL}(2,5) \cong A_5; \quad \mathrm{PSL}(2,7) \cong \mathrm{PSL}(3,2); \quad \mathrm{PSL}(2,9) \cong A_6;$$

$$\mathrm{PSL}(4,2) \cong A_8; \text{ and } \mathrm{PSp}(4,3) \cong \mathrm{PSU}(4,2).$$

All other pairs of groups in Theorem 2.4.1 are non-isomorphic (excluding pairs of isomorphic groups that follow from the above, e.g., $\mathrm{PSU}(4,2)$ and $\mathrm{P\Omega}(5,3)$).

Now, an *almost simple* group is a group $G$ such that $S \leqslant G \leqslant \mathrm{Aut}(S)$ for some non-abelian simple group $S$ (here, $S$ is identified with its group of inner automorphisms). Note that $S$ is the socle of $G$ in this case.

Although $\mathrm{PSp}(4,2) \cong \mathrm{Sp}(4,2)$ is not simple, it is an almost simple group isomorphic to $S_6$, and so $\mathrm{Sp}(4,2)' \cong A_6$ (hence the definition of finite classical groups in §2.3). Thus $\mathrm{Sp}(n,q)'$ is a simple group unless $n = 2$ and $q \leqslant 3$. The groups $G_2(2)$, ${}^2G_2(3)$ or ${}^2F_4(2)$ are also almost simple with simple derived subgroups (indeed, the derived subgroup of this last group is the Tits group). On the other hand, $\mathrm{P\Omega}^{+}(4,q)$ is not almost simple; it is isomorphic to $\mathrm{PSL}(2,q) \times \mathrm{PSL}(2,q)$. The remaining non-simple groups in Theorem 2.4.1 are soluble.

The orders of the above classical, exceptional and sporadic groups are listed in [89, Tables 5.1.A–5.1.C], and the Tits group has index 2 in ${}^2F_4(2)$.

We note here the well-known fact that if $n \geqslant 5$ and $n \neq 6$, then $\mathrm{Aut}(A_n) \cong S_n$. On the other hand, $A_6$ has index 4 in $\mathrm{Aut}(A_6) \cong \mathrm{P\Gamma L}(2,9)$. The almost simple groups with socle $A_6$ and index 2 in $\mathrm{Aut}(A_6)$ are $S_6$, $\mathrm{PGL}(2,9)$, and the Mathieu group $\mathrm{M}_{10}$.

Next, a group $G$ is called *quasisimple* if it is perfect and $G/Z(G)$ is non-abelian and simple. The following result describes an important property of (finite and infinite) quasisimple groups.

**Proposition 2.4.2** ([13, p. 350]). *The proper normal subgroups of a quasisimple group are precisely its central subgroups.*

Our next proposition yields useful information about the classical group $\Omega(\kappa)$, defined in §2.3, in the case where $\mathrm{P}\Omega(\kappa)$ is simple.

**Proposition 2.4.3** ([17, Proposition 1.10.3(iii)]). *Let $\kappa$ be a non-degenerate or zero classical form on a finite-dimensional vector space over a finite field. If $\mathrm{P}\Omega(\kappa)$ is simple, then $\Omega(\kappa)$ is quasisimple.*

We conclude this section with two important results about generators for finite almost simple groups. The first of these was proved by Steinberg [134] in 1962 for the classical and exceptional groups, and in generality by Aschbacher and Guralnick [3, Theorem B] in 1984 (using the classification of finite simple groups).

**Theorem 2.4.4.** *Each non-abelian finite simple group is 2-generated.*

More recently, much stronger results were proved about generation of non-abelian finite simple groups; we mentioned some of these in §1.0.2, in the context of the generating graph of such a group.

**Theorem 2.4.5** ([49, p. 195]). *A finite almost simple group $G$ is not 2-generated if and only if the elementary abelian group $C_2^3$ is a quotient of $G$. Moreover, if this is the case, then $G$ is 3-generated, and the socle of $G$ is isomorphic to $\mathrm{PSL}(2m, q)$ or $\mathrm{P}\Omega^+(2m, q)$, with $m$ an integer at least 2 and $q$ a prime power.*

## 2.5 Matrices and polynomials

We conclude this chapter by exploring matrices and cyclic subgroups of general linear groups. In order to do so, we will also discuss related polynomials. The results here will be useful in Chapters 3, 4 and 6.

Throughout this section, $\mathbb{F}$ denotes a field, $q$ a prime power, and $n$ a positive integer. For a positive integer $k$, we write $I_k$ to denote the $k \times k$ identity matrix over $\mathbb{F}$. Additionally, for a square matrix $A$, we write $\chi_A$ and $\mu_A$ to denote the characteristic polynomial and minimal polynomial of $A$, respectively.

### 2.5.1 Companion and hypercompanion matrices

We begin by considering companion and hypercompanion matrices of monic polynomials in the ring $\mathbb{F}[x]$.

**Definition 2.5.1** ([118, p. 148, pp. 161–162])**.** Let

$$f(x) := x^n - \beta_n x^{n-1} - \ldots - \beta_2 x - \beta_1$$

be a (monic) polynomial in $\mathbb{F}[x]$. Then the *companion matrix* of $f$ is the $n \times n$ matrix

$$C(f) := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ \beta_1 & \beta_2 & \beta_3 & \cdots & \beta_n \end{pmatrix},$$

with $C(f) = (\beta_1)$ when $n = 1$. Moreover, if $f$ is irreducible over $\mathbb{F}$, then for each positive integer $k$, the *hypercompanion matrix* of $f^k$ is the $kn \times kn$ matrix

$$C_k(f) := \begin{pmatrix} C(f) & E_{n,1} & 0 & \cdots & 0 \\ 0 & C(f) & E_{n,1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & E_{n,1} \\ 0 & 0 & 0 & \cdots & C(f) \end{pmatrix},$$

where $E_{n,1}$ is the $n \times n$ matrix whose $(n, 1)$ entry is equal to 1, with all other entries equal to 0.

Observe that $\det(C(f)) = (-1)^{n-1}\beta_1$. Additionally, as $C_k(f)$ is a block triangular matrix, it follows that $\det(C_k(f)) = \det(C(f))^k$.

For the following theorem, recall that the characteristic polynomial of any square matrix is monic (assuming the convention $\chi_A(x) := \det(xI_n - A)$).

**Theorem 2.5.2** ([118, pp. 157–158, p. 162])**.** *Let $A$ be a square matrix with entries in $\mathbb{F}$. There exists a multiset $X$ of powers of monic irreducible polynomials over $\mathbb{F}$, with $\prod_{f \in X} f = \chi_A$, such that $A$ is similar to the direct sum of the hypercompanion matrices of the polynomials in $X$.*

Specifically, $X$ is the multiset of *elementary divisors* of $A$ over $\mathbb{F}$, which are defined in [118, p. 157].

Our next result will allow us to prove that certain matrices that arise later in this thesis can only be scalar matrices.

**Proposition 2.5.3.** *Suppose that $n > 1$, and let $m$ be a positive integer strictly less than $n$. Additionally, let $S$ be the companion matrix of a monic polynomial*

*of degree $n$ over $\mathbb{F}$, and let $K$ be a block matrix* $\begin{pmatrix} A & 0 \\ C & B \end{pmatrix}$, *where* $A \in \mathrm{GL}(m, \mathbb{F})$, $B \in \mathrm{GL}(n-m, \mathbb{F})$ *and $C$ is an $(n-m) \times m$ matrix with entries in $\mathbb{F}$. If $[K, S] = 1$, then $K$ is a scalar matrix.*

*Proof.* Let $r := n - m$, and let $(a_{ij})_{m\times m} = A$, $(b_{ij})_{r\times r} = B$ and $(c_{ij})_{r\times m} = C$. Additionally, let $x^n - \beta_n x^{n-1} - \ldots - \beta_2 x - \beta_1$ be the monic polynomial in $\mathbb{F}[x]$ associated with $S$, where $\beta_i \in \mathbb{F}$ for each $i$. By Definition 2.5.1, $S$ is equal to the block matrix $\begin{pmatrix} S_1 & S_2 \\ S_3 & S_4 \end{pmatrix}$, where each block has the same dimensions as the corresponding block of $K$, namely, $m \times m$, $m \times r$, $r \times m$ and $r \times r$, respectively. In particular,

$$S_1 = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}, \; S_2 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \end{pmatrix},$$

$$S_3 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \\ \beta_1 & \beta_2 & \cdots & \beta_m \end{pmatrix}, \text{ and } S_4 = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ \beta_{m+1} & \beta_{m+2} & \beta_{m+3} & \cdots & \beta_n \end{pmatrix}.$$

To avoid ambiguity when $m = 1$ or $r = 1$, we note that $S_1$ always contains an entry equal to 0, $S_2$ always contains an entry equal to 1, $S_3$ always contains an entry equal to $\beta_1$, and $S_4$ always contains an entry equal to $\beta_n$.

Suppose now that $[K, S] = 1$. Then $KS = SK$, i.e.,

$$\begin{pmatrix} AS_1 & AS_2 \\ CS_1 + BS_3 & CS_2 + BS_4 \end{pmatrix} = \begin{pmatrix} S_1A + S_2C & S_2B \\ S_3A + S_4C & S_4B \end{pmatrix}.$$

The equality $AS_2 = S_2B$ yields

$$\begin{pmatrix} a_{1m} & 0 & \cdots & 0 \\ a_{2m} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{m-1,m} & 0 & \cdots & 0 \\ a_{mm} & 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \\ b_{11} & b_{12} & \cdots & b_{1r} \end{pmatrix},$$

where the former matrix always contains an entry equal to $a_{mm}$ and the latter always contains an entry equal to $b_{11}$. Hence

$$a_{im} = 0 \text{ for all } i < m, \tag{2.5.1}$$

$$b_{11} = a_{mm}, \text{ and} \tag{2.5.2}$$

$$b_{1j} = 0 \text{ for all } j > 1. \tag{2.5.3}$$

We deduce from the equality $AS_1 = S_1A + S_2C$ that

$$\begin{pmatrix} 0 & a_{11} & a_{12} & \cdots & a_{1,m-1} \\ 0 & a_{21} & a_{22} & \cdots & a_{2,m-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & a_{m-1,1} & a_{m-1,2} & \cdots & a_{m-1,m-1} \\ 0 & a_{m1} & a_{m2} & \cdots & a_{m,m-1} \end{pmatrix} = \begin{pmatrix} a_{21} & a_{22} & a_{23} & \cdots & a_{2m} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mm} \\ c_{11} & c_{12} & c_{13} & \cdots & c_{1m} \end{pmatrix},$$

where the former matrix always contains an entry equal to 0 and the latter always contains an entry equal to $c_{11}$. Thus $a_{ij} = a_{i+1,j+1}$ for all $i < m$ and $j < m$. Additionally, $a_{i1} = 0$ for all $i > 1$, and so $a_{ij} = 0$ whenever $i > j$. Similarly, we deduce from (2.5.1) that $a_{ij} = 0$ whenever $i < j$, and so

$$A = aI_m \text{ for some } a \in \mathbb{F}^\times. \tag{2.5.4}$$

We also conclude that

$$c_{1j} = 0 \text{ for all } j. \tag{2.5.5}$$

Hence if $r = 1$, then (2.5.2) implies that $K$ is a scalar matrix. We may therefore assume that $r > 1$.

Now, for integers $s$ and $t$, let $\gamma_{st} := \beta_{m+s}b_{tr}$. The equality $CS_2 + BS_4 = S_4B$ yields

$$\begin{pmatrix} c_{1m} + \gamma_{11} & b_{11} + \gamma_{21} & b_{12} + \gamma_{31} & \cdots & b_{1,r-1} + \gamma_{r1} \\ c_{2m} + \gamma_{12} & b_{21} + \gamma_{22} & b_{22} + \gamma_{32} & \cdots & b_{2,r-1} + \gamma_{r2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{r-1,m} + \gamma_{1,r-1} & b_{r-1,1} + \gamma_{2,r-1} & b_{r-1,2} + \gamma_{3,r-1} & \cdots & b_{r-1,r-1} + \gamma_{r,r-1} \\ c_{rm} + \gamma_{1r} & b_{r1} + \gamma_{2r} & b_{r2} + \gamma_{3r} & \cdots & b_{r,r-1} + \gamma_{rr} \end{pmatrix}$$

$$= \begin{pmatrix} b_{21} & b_{22} & b_{23} & \cdots & b_{2r} \\ b_{31} & b_{32} & b_{33} & \cdots & b_{3r} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{r1} & b_{r2} & b_{r3} & \cdots & b_{rr} \\ \sum_{i=1}^{r} \beta_{m+i}b_{i1} & \sum_{i=1}^{r} \beta_{m+i}b_{i2} & \sum_{i=1}^{r} \beta_{m+i}b_{i3} & \cdots & \sum_{i=1}^{r} \beta_{m+i}b_{ir} \end{pmatrix}.$$

By (2.5.3), $\gamma_{s1} = 0$ for all $s$. Hence a comparison of the first row of each matrix, together with (2.5.2), (2.5.4) and (2.5.5), shows that $b_{2j} = 0$ for all $j \neq 2$, and that $b_{22} = b_{11} = a$. Thus if $r > 2$, then $\gamma_{s2} = 0$ for all $s$, and we deduce by comparing the second row of each matrix that $b_{31} = c_{2m}$, $b_{33} = b_{22} = a$, and $b_{3j} = 0$ when $j = 2$ or $j > 3$. Proceeding by induction on successive rows (stopping after the penultimate row), we conclude that

$$b_{ij} = \begin{cases} a, & \text{if } i = j; \\ 0, & \text{if } i < j \text{ or } i = j+1; \\ c_{i-j,m}, & \text{if } i > j+1. \end{cases} \tag{2.5.6}$$

By comparing the $(r, r-1)$ entry of each matrix, we deduce that $b_{r,r-2} + \beta_{m+r-1}a = \sum_{i=1}^{r} \beta_{m+i} b_{i,r-1} = \beta_{m+r-1}a$. Hence $0 = b_{r,r-2} = c_{2m}$, and so $b_{ij} = 0$ whenever $i - j = 2$. By induction on successive entries of the final row of each matrix (starting from the $(r-2)$-th entry and working our way to the first entry), we similarly conclude that $c_{im} = 0$ for all $i$. Hence it follows from (2.5.6) that

$$B = aI_r. \tag{2.5.7}$$

It remains to show that $C = 0$. Consider the equality $CS_1 + BS_3 = S_3A + S_4C$. As $BS_3 = S_3A$ by (2.5.4) and (2.5.7), it follows that $CS_1 = S_4C$, i.e.,

$$\begin{pmatrix} 0 & c_{11} & c_{12} & \cdots & c_{1,m-1} \\ 0 & c_{21} & c_{22} & \cdots & c_{2,m-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & c_{r-1,1} & c_{r-1,2} & \cdots & c_{r-1,m-1} \\ 0 & c_{r1} & c_{r2} & \cdots & c_{r,m-1} \end{pmatrix}$$

$$= \begin{pmatrix} c_{21} & c_{22} & c_{23} & \cdots & c_{2m} \\ c_{31} & c_{32} & c_{33} & \cdots & c_{3m} \\ \vdots & \vdots & \cdots & \cdots & \vdots \\ c_{r1} & c_{r2} & c_{r3} & \cdots & c_{rm} \\ \sum_{i=1}^{r} \beta_{m+i} c_{i1} & \sum_{i=1}^{r} \beta_{m+i} c_{i2} & \sum_{i=1}^{r} \beta_{m+i} c_{i3} & \cdots & \sum_{i=1}^{r} \beta_{m+i} c_{im} \end{pmatrix},$$

where the former matrix always contains a column of zeroes. We observe from the first $r-1$ rows of each matrix that $c_{ij} = c_{i+1,j+1}$ for all $i < r$ and $j < m$. Additionally, a comparison of the first column of each matrix, together with (2.5.5), shows that $c_{ij} = 0$ whenever $1 \in \{i, j\}$. We therefore deduce that $C = 0$, as required. □

### 2.5.2 Irreducible cyclic subgroups of general linear groups

In this subsection, we prove several results about the irreducibility of certain cyclic subgroups of linear groups. In order to do so, we also explore the irreducibility and factorisation of related polynomials. The following proposition highlights the connection between these two concepts. Although this result is well known, it is often stated without a proof, and so we provide one here.

**Proposition 2.5.4** ([135, p. 119]). *Let $A \in \mathrm{GL}(n, \mathbb{F})$. Then $\chi_A$ is irreducible over $\mathbb{F}$ if and only if $\langle A \rangle$ acts irreducibly on the vector space $\mathbb{F}^n$. Hence if $\langle A \rangle$ acts irreducibly on $\mathbb{F}^n$, then $\mu_A = \chi_A$.*

*Proof.* We will prove the contrapositive of each direction of the main result. Suppose first that $\langle A \rangle$ acts reducibly on $\mathbb{F}^n$, so that $\langle A \rangle$ stabilises a $t$-dimensional subspace of $\mathbb{F}^n$, where $0 < t < n$. Then $A$ is similar to a block matrix $\begin{pmatrix} K & 0 \\ L & M \end{pmatrix}$, where $K$, $L$ and $M$ are matrices of dimensions $t \times t$, $(n-t) \times t$ and $(n-t) \times (n-t)$, respectively. As similar matrices have equal characteristic polynomials, $\chi_A \in \mathbb{F}[x]$ is equal to the determinant of $\begin{pmatrix} xI_t - K & 0 \\ -L & xI_{n-t} - M \end{pmatrix}$. By considering the calculation of this determinant via expansion along successive rows of the matrix, we see that $\chi_A = \det(xI_t - K)\det(xI_{n-t} - M)$, which is equal to $\chi_K \chi_M$. Thus $\chi_A$ is reducible over $\mathbb{F}$.

Conversely, suppose that $\chi_A$ is reducible over $\mathbb{F}$. Then Theorem 2.5.2 implies that $A$ is similar to a direct sum $B$ of hypercompanion matrices. We may view $B$ as a block matrix whose final row is $\begin{pmatrix} 0 & 0 & \cdots & 0 & X \end{pmatrix}$, where $X$ is a nonzero $t \times t$ matrix for some $0 < t < n$. This is the case even if $B$ is equal to a single hypercompanion matrix, as in this case $\chi_A$ is a proper power of an irreducible polynomial. Therefore, $\langle B \rangle$ stabilises the subspace of $\mathbb{F}^n$ spanned by the final $t$ basis vectors of $\mathbb{F}^n$. It follows immediately that $\langle A \rangle$ acts reducibly on $\mathbb{F}^n$. The fact that $\mu_A$ divides $\chi_A$ then yields the final part of the proposition. □

Throughout the rest of this section (with the exception of one definition), we assume that $\mathbb{F}$ is the finite field $\mathbb{F}_q$. In the proof of the following lemma, and many times throughout this thesis, we use the standard notation $(r, s) := \mathrm{GCD}(r, s)$ for integers $r$ and $s$. It will always be clear from the context whether $(r, s)$ refers to this greatest common divisor, to an ordered pair of objects, or to the image of a pair of vectors under a bilinear form.

**Lemma 2.5.5.** *Let $a \in \mathbb{F}_q^\times$. Then the set of irreducible factors in $\mathbb{F}_q[x]$ of the binomial $x^{q-1} - a$ is $\{x^{|a|} - b \mid b \in \mathbb{F}_q^\times, b^{(q-1)/|a|} = a\}$.*

*Proof.* For each positive integer $k$, let $H_k$ be the subgroup of $\mathbb{F}_q^\times$ consisting of $k$-th powers of elements. Then the map $\phi_k : \mathbb{F}_q^\times \to H_k$ that sends $u \in \mathbb{F}_q^\times$ to $u^k$ is an epimorphism. Since $u^k = 1$ if and only if $u^y = 1$ for some positive integer $y$ dividing both $k$ and $q-1$, the kernel of $\phi_k$ is precisely the unique subgroup of $\mathbb{F}_q^\times$ of order $(k, q-1)$. Therefore, $|H_k| = (q-1)/(k, q-1)$.

Now, let $r := |a|$ and $t := (q-1)/r$. Then $(t, q-1) = t$, and so $|H_t| = (q-1)/t = r$. This means that $H_t = \langle a \rangle$, and in particular, $a \in H_t$. Moreover, $|\ker(\phi_t)| = t$, and thus there are exactly $t$ distinct roots $b_1, \ldots, b_t \in \mathbb{F}_q^\times$ of the binomial $f(x) := x^t - a$. Hence $f(x) = \prod_{i=1}^t g_i(x)$, where $g_i(x) := x - b_i$ for each $i$, and it follows that

$$x^{q-1} - a = f(x^r) = \prod_{i=1}^t g_i(x^r) = \prod_{i=1}^t (x^r - b_i).$$

It remains to show that the binomial $x^r - b_i$ is irreducible over $\mathbb{F}_q$ for each $i$. Since $b_i^t = a$, the order $r$ of $a$ divides $|b_i|$. Additionally, if $r$ is divisible by 4, then so is $q-1$, and hence $q \equiv 1 \pmod 4$. By [93, Theorem 3.3, Theorem 3.35], it suffices to prove that $r$ is coprime to $u := (q-1)/|b_i|$.

Observe that, since $|H_u| = |b_i|$, there exists $c_i \in \mathbb{F}_q^\times$ with $c_i^u = b_i$, and hence $c_i^{ut} = a$. Therefore, $a$ is a $ut$-th power, i.e., $a \in H_{ut}$, and so $r$ divides $|H_{ut}| = (q-1)/(ut, q-1)$. Since $q - 1 = tr$, we conclude that $(q-1)/(ut, q-1) = (q-1)/(t(u, r)) = r/(u, r)$. Thus $r$ divides $r/(u, r)$, and so $(u, r) = 1$, as required. □

**Lemma 2.5.6.** *Let $A \in \mathrm{GL}(n, q)$. Suppose also that $A^{q-1} \in Z(\mathrm{GL}(n, q))$, and that $\langle A \rangle$ acts irreducibly on the vector space $\mathbb{F}_q^n$. Then $A$ is similar to the companion matrix $C(x^n - b)$, for some $b \in \mathbb{F}_q^\times$ such that $x^n - b$ is irreducible over $\mathbb{F}_q$.*

*Proof.* Since $A^{q-1} \in Z(\mathrm{GL}(n, q))$, there exists $a \in \mathbb{F}_q^\times$ such that $A^{q-1} - aI_n = 0$. Therefore, the polynomial $x^{q-1} - a \in \mathbb{F}_q[x]$ is divisible by $\mu_A$, which is irreducible and equal to $\chi_A$ by Proposition 2.5.4. It follows from Lemma 2.5.5, and from the fact that $\chi_A$ has degree $n$, that $\chi_A(x) = x^n - b$ for some $b \in \mathbb{F}_q^\times$. Hence Theorem 2.5.2 implies that $A$ is similar to the companion matrix $C_1(x^n - b) = C(x^n - b)$. □

A more detailed version of the following theorem, which applies to any odd prime power $q$, was proved by Carlitz [38, pp. 569–570] in the case where $q$ is an odd prime. In fact, our proof is similar to Carlitz's proof, and it is not difficult to extend our proof to show that Carlitz's result holds for all odd prime powers.

**Theorem 2.5.7.** *Suppose that $q$ is odd, and let $b, c \in \mathbb{F}_q$ Then the polynomial $x^4 + cx^2 + b^2 \in \mathbb{F}_q[x]$ is reducible.*

*Proof.* Let $f(x) := x^4 + cx^2 + b^2$. If $b = 0$, then $x^2$ is a factor of $f(x)$. Assume therefore that $b \neq 0$, and let $a := -c/2$. As each element of $\mathbb{F}_q$ is a square in $\mathbb{F}_{q^2}$, there exist $\alpha, \beta \in \mathbb{F}_{q^2}$ with $\alpha^2 = 2(a-b)$ and $\beta^2 = 2(a+b)$. Letting $r := \alpha/2$ and $s := \beta/2$, we see that

$$\begin{aligned}(x^2 + 2rx + r^2 - s^2)(x^2 - 2rx + r^2 - s^2) &= x^4 - 2(r^2+s^2)x^2 + (r^2-s^2)^2 \\ &= x^4 - (\alpha^2+\beta^2)x^2/2 + ((\alpha^2-\beta^2)/4)^2 \\ &= x^4 - 2ax^2 + b^2 = f(x).\end{aligned}$$

Similarly, $f(x) = (x^2 + 2sx + s^2 - r^2)(x^2 - 2sx + s^2 - r^2)$. As $r^2, s^2 \in \mathbb{F}_q$, it follows that $f(x)$ has quadratic factors in $\mathbb{F}_q[x]$ if $r \in \mathbb{F}_q$ or $s \in \mathbb{F}_q$.

Suppose finally that $r, s \notin \mathbb{F}_q$, so that $2(a-b)$ and $2(a+b)$ are not squares in $\mathbb{F}_q$. Then their product $4(a^2-b^2)$ is a square in $\mathbb{F}_q$, and hence so is $a^2-b^2$. Observe that $(\alpha\beta/2)^2 = a^2 - b^2$, and $f(x) = (x^2 - a - \alpha\beta/2)(x^2 - a + \alpha\beta/2)$. Thus the square roots $\pm\alpha\beta/2$ of $a^2-b^2$ are elements of $\mathbb{F}_q$, and $f(x)$ has quadratic factors in $\mathbb{F}_q[x]$. □

In order to prove the final result of this subsection, we will require some elementary field theory. For the following definition, recall that if $f$ is a non-constant polynomial in $\mathbb{F}[x]$, then each root of $f$ lies in some extension field of $\mathbb{F}$.

**Definition 2.5.8** ([122, p. 32])**.** Let $\mathbb{F} \subseteq K$ be a field extension, and let $f$ be a non-constant polynomial in $\mathbb{F}[x]$. Then $K$ is a *splitting field* for $f$ over $\mathbb{F}$ if $K$ contains each root of $f$, and if no proper subfield of $K$ contains $\mathbb{F}$ and all roots of $f$.

Note that each non-constant polynomial in $\mathbb{F}[x]$ has a unique splitting field over $\mathbb{F}$, up to isomorphism [93, Theorem 1.92].

**Proposition 2.5.9** ([122, p. 216])**.** *Let $f$ be an irreducible polynomial over $\mathbb{F}_q$ of degree $n$. Then $\mathbb{F}_{q^n}$ is the splitting field for $f$ over $\mathbb{F}_q$. Additionally, no root of $f$ lies in any proper subfield of $\mathbb{F}_{q^n}$.*

It follows from the above proposition that, for each positive integer $i$, the irreducible polynomial $f \in \mathbb{F}_q[x]$ is the product of $(i,n)$ irreducible factors over $\mathbb{F}_{q^i}$, each of degree $n/(i,n)$.

The hypotheses of the following proposition are similar to those of Lemma 2.5.6.

**Proposition 2.5.10.** *Let $A \in \mathrm{SL}(n,q)$. Suppose also that $A^{q^2-1} \in Z(\mathrm{SL}(n,q))$, and that $\langle A \rangle$ acts irreducibly on the vector space $\mathbb{F}_q^n$. Then $n \in \{1,2\}$.*

*Proof.* Proposition 2.5.4 implies that $\chi_A$ is irreducible over $\mathbb{F}_q$ and is equal to $\mu_A$. We also observe from Theorem 2.5.2 that $A$ is similar to the companion matrix $C(\chi_A)$, which therefore has determinant 1. Additionally, since $A^{q^2-1} \in Z(\mathrm{SL}(n,q))$, there exists $a \in \mathbb{F}_q^\times$ such that $A^{q^2-1} - aI_n = 0$. Thus $\chi_A$ divides the polynomial $x^{q^2-1} - a \in \mathbb{F}_q[x]$. Furthermore, the degree of $\chi_A$ is $n$, and thus by Proposition 2.5.9, $\mathbb{F}_{q^n}$ is the splitting field for $\chi_A$ over $\mathbb{F}_q$. To prove the required result, we will study $\chi_A$ as a polynomial in $\mathbb{F}_{q^2}[x]$. In particular, we will use the fact that the set of irreducible factors in $\mathbb{F}_{q^2}[x]$ of $x^{q^2-1} - a$ is $\{x^{|a|} - b \mid b \in \mathbb{F}_{q^2}^\times, b^{(q^2-1)/|a|} = a\}$, by Lemma 2.5.5.

Suppose first that $n$ is odd. Then $\chi_A$ is irreducible over $\mathbb{F}_{q^2}$, and it follows that $n = |a|$, and that $\chi_A = x^n - b$, for some $b \in \mathbb{F}_q^\times$ (since $\chi_A \in \mathbb{F}_q[x]$) with $b^{(q^2-1)/n} = a$. Since the determinant of the companion matrix $C(x^n - b)$ is equal to $b$, we deduce that $b = 1$. As $a$ is a power of $b$, it follows that $a = 1$, and thus $n = 1$.

Next, suppose that $n$ is even. Then each irreducible factor of $\chi_A$ in $\mathbb{F}_{q^2}$ has degree $n/2$. In particular, $|a| = n/2$, and there exist $b_1, b_2 \in \mathbb{F}_{q^2}^\times$ such that

$$\chi_A = (x^{n/2} - b_1)(x^{n/2} - b_2) = x^n - (b_1 + b_2)x^{n/2} + b_1 b_2,$$

with $b_1^{(q^2-1)/(n/2)} = b_2^{(q^2-1)/(n/2)} = a$ and $b_1 b_2, b_1 + b_2 \in \mathbb{F}_q$. Here, the determinant of $C(\chi_A)$ is equal to $b_1 b_2$, and thus $b_1 b_2 = 1$, i.e., $b_2 = b_1^{-1}$. Therefore, $a = (b_1^{-1})^{(q^2-1)/(n/2)} = (b_1^{(q^2-1)/(n/2)})^{-1} = a^{-1}$, and hence $n/2 = |a| \in \{1, 2\}$. In particular, if $q$ is even, then the element $a$ of $\mathbb{F}_q^\times$ has odd order, yielding $n = 2$. If instead $q$ is odd, then the irreducible polynomial $x^n - (b_1 + b_2)x^{n/2} + 1$ cannot have degree 4 by Theorem 2.5.7, and so we again conclude that $n = 2$. □

### 2.5.3 Singer cycles

We now discuss the important subgroups of $\mathrm{GL}(n,q)$ known as Singer cycles.

**Definition 2.5.11** ([50, p. 43])**.** A *Singer cycle* of $\mathrm{GL}(n,q)$ is a cyclic subgroup of $\mathrm{GL}(n,q)$ of order $q^n - 1$.

Certain other classical groups also have cyclic subgroups known as Singer cycles; see [10, §1] and [78]. Some of these will briefly appear in §4.2 and §6.5.

**Proposition 2.5.12** ([78, p. 493])**.** *All Singer cycles of* $\mathrm{GL}(n,q)$ *are conjugate.*

The following lemma will be useful when discussing the normaliser in $\mathrm{GL}(n,q)$ of a Singer cycle, whose structure is described in the subsequent proposition. The first part of the lemma is elementary, while the second part and its proof are from [81, p. 61]. Here, $V$ denotes the field $\mathbb{F}_{q^n}$ considered as the $n$-dimensional vector space

over $\mathbb{F}_q$. Then $\mathrm{GL}(V) \cong \mathrm{GL}(n,q)$, and the subfield $\mathbb{F}_q$ of $\mathbb{F}_{q^n}$ is a one-dimensional subspace of $V$.

**Lemma 2.5.13.** *Let $\phi$ be the field automorphism of $\mathbb{F}_{q^n}$ that maps each field element $\lambda$ to $\lambda^q$.*

(i) *$\phi \in \mathrm{GL}(V)$, and $\phi$ fixes each vector in the one-dimensional subspace $\mathbb{F}_q$ of $V$.*

(ii) *As elements of $\mathrm{GL}(n,q)$, the companion matrix $C(x^n-1)$ is similar to $\phi$.*

*Proof.*

(i) Let $\alpha \in \mathbb{F}_q$ and $\lambda, \mu \in V$. Then $\alpha^\phi = \alpha^q = \alpha$, i.e., $\phi$ fixes $\alpha$. Moreover,

$$(\lambda+\mu)^\phi = (\lambda+\mu)^q = \lambda^q + \mu^q = \lambda^\phi + \mu^\phi,$$

and

$$(\alpha\lambda)^\phi = (\alpha\lambda)^q = \alpha^q\lambda^q = \alpha\lambda^q = \alpha\lambda^\phi.$$

Thus $\phi$ acts linearly on $V$. Since $\phi$ is a field automorphism of $\mathbb{F}_{q^n}$, it is a bijection from $V$ to itself, and hence $\phi \in \mathrm{GL}(V)$.

(ii) The Normal Basis Theorem [93, Theorem 2.35] states that there exists $\gamma \in V$ such that $\{\gamma, \gamma^q, \gamma^{q^2}, \ldots, \gamma^{q^{n-1}}\}$ is an $\mathbb{F}_q$-basis for $V$. With respect to this basis, the matrix of $\phi$ is

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix} = C(x^n-1). \qquad \square$$

**Proposition 2.5.14** ([83, pp. 187–188])**.** *Suppose that $n > 1$, and let $S$ be a Singer cycle of $\mathrm{GL}(n,q)$. Then $Z(\mathrm{GL}(n,q)) < S$, and $N := N_{\mathrm{GL}(n,q)}(S)$ is equal to $S{:}\langle B\rangle$, where $B$ is a $\mathrm{GL}(n,q)$-conjugate of the field automorphism $\lambda \mapsto \lambda^q$ of $\mathbb{F}_{q^n}$. In particular, $|N| = n(q^n-1)$. Moreover, $A^B = A^q$ for each $A \in S$.*

Our next result is closely linked with §2.5.2.

**Proposition 2.5.15** ([50, Proposition 3.6.1])**.** *Let $A \in \mathrm{GL}(n,q)$. If $\langle A\rangle$ acts irreducibly on the vector space $\mathbb{F}_q^n$, then $A$ lies in a Singer cycle of $\mathrm{GL}(n,q)$.*

The following yields a partial converse to the above proposition.

**Proposition 2.5.16** ([131, Proposition 4.2.2])**.** *Suppose that $n$ is prime, and let $H$ be a subgroup of a Singer cycle of $\mathrm{GL}(n,q)$. Then $H$ acts irreducibly on $\mathbb{F}_q^n$ if and only if $|H|$ does not divide $q-1$.*

**Corollary 2.5.17.** *Suppose that $n$ is an odd prime. Additionally, let $S$ be a Singer cycle of $\mathrm{GL}(n,q)$, and let $A \in (S \cap \mathrm{SL}(n,q)) \setminus Z(\mathrm{SL}(n,q))$. Then $A^{q-1} \notin Z(\mathrm{SL}(n,q))$.*

*Proof.* By Proposition 2.5.14, $S$ contains $Z(\mathrm{GL}(n,q))$, which has order $q-1$. As $S$ is cyclic, it follows that subgroups of $Z(\mathrm{GL}(n,q))$ are precisely the subgroups of $S$ whose orders divide $q-1$. Hence Proposition 2.5.16 implies that $\langle A \rangle$ acts irreducibly on $\mathbb{F}_q^n$. Proposition 2.5.10 now shows that $A^{q^2-1}$ does not lie in $Z(\mathrm{SL}(n,q))$, and hence neither does $A^{q-1}$, as $(q-1) \mid (q^2-1)$. □

# Chapter 3

# Base sizes of primitive subspace actions

## 3.1 Preliminaries, main theorems and applications

In this chapter, we consider the base sizes of primitive subspace actions of finite almost simple classical groups. In particular, we prove lower bounds for the base size of such a group acting on subspaces of its natural module, and upper bounds for the base size of a linear group acting on pairs of subspaces. Using small computational examples, we will show that these bounds are, in general, tight.

### 3.1.1 Base sizes and subspace actions

We begin by formally defining base sizes of permutation groups and subspace actions of finite almost simple classical groups. In addition, we state important results related to the base sizes of these classical groups. Let $G$ be a permutation group acting faithfully on a set $\Omega$. Throughout this chapter, for a subset $\Delta$ of $\Omega$, we write $G_{(\Delta)}$ to denote the pointwise stabiliser $\bigcap_{\delta\in\Delta} G_\delta$ of $\Delta$ in $G$.

**Definition 3.1.1** ([94, p. 11])**.** A *base* for $G$ (with respect to its action on $\Omega$) is a subset $\Delta$ of $\Omega$ such that $G_{(\Delta)} = 1$. The *base size* of $G$, denoted by $b(G,\Omega)$, or by $b(G)$ if $\Omega$ is clear from the context, is the minimal size of a base for $G$.

It is clear that if $H$ is a subgroup of $G$, then $b(H,\Omega) \leqslant b(G,\Omega)$.

Note that our notation $b(G,\Omega)$ is a blend of the notation $b_\Omega(G)$ from [72] and the notation $b(G,H)$ from [27], where $H$ is a point stabiliser in $G$.

While base sizes of infinite permutation groups are well-defined, our results in this chapter will apply only to finite groups. However, we will compare several of our results with analogous results from [27, §4.1], which are related to (infinite) *simple algebraic groups*, defined over algebraic closures of finite fields. Note that a simple algebraic group is not necessarily simple as an abstract group. For an introduction to these groups, see [109].

The following example is standard (see, e.g., [100, p. 147]).

**Example 3.1.2.** Let $\Omega := \{1, \ldots, n\}$, where $n > 1$ is an integer. We will determine the base sizes of the actions of the symmetric group $S_n$ and the alternating group $A_n$, respectively, on $\Omega$.

For each non-negative integer $r$, with $r < n$, let $\Delta_r$ be a subset of $\Omega$ of size $r$. Observe that if an element $x \in S_n$ fixes all points in $\Delta_{n-1}$, then $x$ also fixes the unique point in $\Omega \setminus \Delta_{n-1}$, and hence $x$ is the identity. On the other hand, if $\alpha_1$ and $\alpha_2$ are distinct points in $\Omega \setminus \Delta_{n-2}$, then $(\alpha_1, \alpha_2) \in S_n$ fixes each point in $\Delta_{n-2}$. Hence $b(S_n) = n - 1$.

Assume now that $n \geqslant 3$. Then no element of $A_n$ transposes two points in $\Omega$ while fixing the remaining points. However, letting $\beta_1, \beta_2$ and $\beta_3$ be the distinct points in $\Omega \setminus \Delta_{n-3}$, the element $(\beta_1, \beta_2, \beta_3)$ of $A_n$ fixes each point in $\Delta_{n-3}$. Thus $b(A_n) = n - 2$.

We now define subspace actions, i.e., the group actions that are the main focus of this chapter. The set $\Omega$ on which the group $G$ acts should not be confused with the orthogonal group $\Omega^\varepsilon(n, q)$, or more generally, with the group $\Omega(\kappa)$ from (2.3.1). Recall that $\Omega^\varepsilon(n, q) \cong \mathrm{P}\Omega^\varepsilon(n, q)$ when $n$ is odd or $q$ is even (and in certain other cases), that $\mathrm{Sp}(n, q) \cong \mathrm{PSp}(n, q)$ when $q$ is even, and that the derived subgroup $\mathrm{PSp}(4, 2)'$ of $\mathrm{PSp}(4, 2)$ is isomorphic to the alternating group $A_6$. In addition, recall Definition 2.3.3 of the natural module for a classical group. Note in particular that the natural module for $\mathrm{PSL}(n, q)$ is equipped with the zero form, and hence every subspace of this vector space is totally singular.

**Definition 3.1.3** ([23, Definition 2.1])**.** Suppose that $G$ is a finite almost simple classical group, and let $H$ be a subgroup of $G$ that does not contain $G_0 := \mathrm{soc}(G)$. Let $V := \mathbb{F}_{q^u}^n$ be the natural module for $G_0$, so that $q$ is a prime power, $n$ is an integer greater than 1, $u = 2$ if $G$ is unitary, and $u = 1$ otherwise. Then $H$ is a *subspace subgroup* of $G$ if, for each maximal subgroup $M$ of $G_0$ that contains $H \cap G_0$, one of the following holds:

(i) $M$ is the stabiliser in $G_0$ of a proper nonzero totally singular or non-degenerate subspace of $V$;

(ii) $G_0 = \Omega^\pm(n, q)$, $q$ is even, and $M$ is the stabiliser in $G_0$ of a one-dimensional nonsingular subspace of $V$; or

(iii) $G_0 = \mathrm{Sp}(n, q)'$, $q$ is even, and $M = \mathrm{GO}^\pm(n, q)$.

A faithful, transitive action of $G$ on a set $\Omega$ is a *subspace action* if the point stabiliser is a subspace subgroup of $G$.

Note that the definition of a subspace action given in [99, §1.1] is slightly different, and excludes certain cases that follow from the definition above (we will specify these cases shortly).

Using the notation of (2.3.2), we recall from §2.3–2.4 that a given finite almost simple classical group $G$ satisfies $\mathrm{soc}(G) = \mathrm{P}\Omega(\kappa)'$ for some classical form $\kappa$, and either $G \leqslant \mathrm{P}A(\kappa)$; $\mathrm{soc}(G) = \mathrm{Sp}(4,q)'$ with $q$ even and $G \not\leqslant \mathrm{PC\Gamma Sp}(4,q)$; or $\mathrm{soc}(G) = \mathrm{P}\Omega^+(8,q)$ and $G \not\leqslant \mathrm{PC\Gamma O}^+(8,q)$. Recall also from §2.3 that $G \cap \mathrm{P}A(\kappa)$ has a natural action on the set of subspaces of the natural module for $G$. We will see that in certain cases where $G \not\leqslant \mathrm{P}A(\kappa)$, this action extends naturally to an action of $G$ on the same set.

The following two propositions give a more precise description of each subspace action $(G,\Omega)$ of a finite almost simple classical group $G$, and of the set $\Omega$ for most of these actions (see also the discussion following the first proposition's proof).

**Proposition 3.1.4.** *Let $G$, $G_0$, $V$, $n$ and $q$ be as in Definition 3.1.3, and let $k$ be a positive integer less than $n$. Suppose also that $G$ acts on a set $\Omega$ with point stabiliser $H$, such that $(G,\Omega)$ is a primitive subspace action. Then one of the following holds.*

(i) *$H$ is the stabiliser in $G$ of a totally singular $k$-dimensional subspace of $V$. Up to equivalence of actions, we may assume that $k \leqslant n/2$, or that $k < n/2$ if $G_0 = \mathrm{P}\Omega^-(n,q)$. Furthermore, if $G_0 = \mathrm{PSL}(n,q)$ and $G \not\leqslant \mathrm{P\Gamma L}(n,q)$, then $k = n/2$.*

(ii) *$H$ is the stabiliser in $G$ of a non-degenerate $k$-dimensional subspace of $V$. We may assume that $k \leqslant n/2$ if $G_0 = \mathrm{P}\Omega^-(n,q)$ and $4 \mid n$, or that $k < n/2$ otherwise. Additionally, if $G_0 = \mathrm{P}\Omega^\pm(n,q)$ and $k$ is odd, then $q$ is odd.*

(iii) *$G_0 = \Omega^\pm(n,q)$ with $n$ and $q$ even, and $H$ is the stabiliser of a nonsingular one-dimensional subspace of $V$.*

(iv) *$G_0 = \mathrm{Sp}(n,q)'$ with $q$ even, and $H \cap G_0 = \mathrm{GO}^\pm(n,q)$.*

(v) *$G_0 = \mathrm{PSL}(n,q)$ with $n \geqslant 3$, $G \not\leqslant \mathrm{P\Gamma L}(n,q)$, and $\Omega$ is the set of unordered pairs $\{X,Y\}$ of subspaces of $V$ such that $\dim(X) = k < n/2$, $\dim(Y) = n-k$, and $X \subseteq Y$.*

(vi) *$G_0 = \mathrm{PSL}(n,q)$ with $n \geqslant 3$, $G \not\leqslant \mathrm{P\Gamma L}(n,q)$, and $\Omega$ is the set of unordered pairs $\{X,Y\}$ of subspaces of $V$ such that $\dim(X) = k < n/2$ and $X \oplus Y = V$.*

(vii) $G_0 = \mathrm{Sp}(4,q)'$ *with* $q$ *even, and* $G \not\leqslant \mathrm{P\Gamma Sp}(4,q)$.

(viii) $G_0 = \mathrm{P\Omega}^+(8,q)$, *and* $G \not\leqslant \mathrm{P\Gamma O}^+(8,q)$.

*Proof.* We split the proof into three cases.

**Case (a)**: $H \cap G_0$ is not a maximal subgroup of $G_0$. By the proof of [113, Proposition 8], $G_0$ and $G$ are as in one of (v)–(viii). In particular, if $G_0$ is linear, then [89, Table 3.5.A, Tables 3.5.G–3.5.H] and the tables in [17, §2.2.1, §8.2] show that either (v) or (vi) holds.

**Case (b)**: $H \cap G_0$ is a maximal subgroup of $G_0$, and is not the stabiliser in $G_0$ of a subspace of $V$. By Definition 3.1.3, (iv) holds.

**Case (c)**: $H \cap G_0$ is both a maximal subgroup of $G_0$ and the stabiliser in $G_0$ of a $k$-dimensional subspace $X$ of $V$. Assume first that $X$ is totally singular. If $G_0$ is linear and $k \neq n/2$, then $n \geqslant 3$. Note that $G$ must lie in $\mathrm{P\Gamma L}(n,q)$ in this case, as otherwise $H$ would not be a maximal subgroup of $G$, and would in fact lie in the stabiliser of a pair of subspaces described in (v) or (vi) (see [89, Table 3.5.A, Table 3.5.G] and the tables in [17, §8.2]). Moreover, if $k > n/2$, then Proposition 2.3.5 shows that in the action of $\mathrm{Aut}(G_0)$ on the set of subspaces of $V$, each element of $\mathrm{Aut}(G_0) \setminus \mathrm{P\Gamma L}(n,q)$ interchanges $X$ and a subspace of dimension $n-k$. Thus the action of $G$ on $k$-dimensional subspaces of $V$ is equivalent to its action on $(n-k)$-dimensional subspaces (as observed in [89, p. 83]). We may therefore assume, as in (i), that $k \leqslant n/2$.

If instead $G_0$ is not linear, then $V$ is equipped with a non-degenerate classical form. We see from Lemma 2.2.2 (and the fact that a totally singular subspace is totally isotropic) that any totally singular subspace of $V$ has dimension at most $n/2$, and so $k \leqslant n/2$. In fact, if $G_0 = \mathrm{P\Omega}^-(n,q)$, then each totally singular subspace of $V$ has dimension at most $n/2-1$ [89, Proposition 2.5.4(i)], and so $k < n/2$ as in (i).

Assume now that $X$ is non-degenerate, so that $G_0$ is not linear. If $G_0 = \mathrm{P\Omega}^{\pm}(n,q)$ and $k$ is odd, then $q$ must be odd, as otherwise $V$ has no non-degenerate $k$-dimensional subspace, by Lemma 2.2.9(iii). Additionally, Lemma 2.2.2 and Corollary 2.2.8 show that $H$ stabilises the $(n-k)$-dimensional subspace $X^\perp$ of $V$, and so we may assume that $k \leqslant n/2$. By [89, Tables 3.5.B–3.5.F] and the tables in [17, §8.2], the action with $k = n/2$ is primitive only if $G_0 = \mathrm{P\Omega}^-(n,q)$ and $4 \mid n$.

Finally, assume that $X$ is neither totally singular nor non-degenerate. Then by Definition 3.1.3, (iii) holds. □

Note that in case (ii) of the above proposition, when $G_0 = \Omega(n,q)$ with $n$ and $k$ odd, $G$ has two distinct actions on non-degenerate $k$-dimensional subspaces of $V$,

corresponding to the two isometry types of such subspaces from Lemma 2.2.9. In each case, the point stabiliser also stabilises a non-degenerate $(n-k)$-dimensional subspace of $V$, but the type of this subspace depends on the action (see, for example, [25, Remark 4.1.3]). Additionally, in case (iv), if we generalise the definition of orthogonal groups of odd dimension to allow $q$ to be even, then we can consider $G_0$ as the isomorphic group $\mathrm{GO}(n+1,q)$, and $\Omega$ as the set of non-degenerate $n$-dimensional subspaces of a given type of the quadratic space $\mathbb{F}_q^{n+1}$ (see [25, Remark 2.5.1], [99, p. 498], [89, Table 3.5.C] and [17, Table 8.1]).

We can also use [17, Tables 8.14–8.15, Table 8.50] and [25, §5.9] to deduce more information about the subspace actions in cases (vii) and (viii). In particular, if case (viii) holds and $q$ is odd, then the action of $G_0$ on totally singular two-dimensional subspaces of $V$ extends to an action of $G$ on this set. Thus cases (i) and (viii) can hold simultaneously.

As mentioned above, the definition of a subspace action given in [99, §1.1] is slightly different to Definition 3.1.3. Specifically, according to the former definition, the actions in cases (i)–(vi) of Proposition 3.1.4 are precisely the primitive subspace actions, and cases (vii)–(viii) do not apply. In fact, the former definition is also used by Halasi, Liebeck and Maróti [72, §3], and the two excluded cases are not explicitly mentioned in the proof [72, §3.3] of their upper bound on the base size of a primitive action of an almost simple classical group. Moreover, their upper bound on the base size of a primitive subspace action in cases (i)–(iii) of Proposition 3.1.4 was proved in [72, §3.1] without explicitly considering case (iii). However, this case is addressed in [113, Lemma 7].

The following assumption will be used in the subsequent proposition, where we consider the case where $(G,\Omega)$ is a transitive (and not necessarily primitive) subspace action, with $\Omega$ a set of subspaces of $V$.

**Assumption 3.1.5.** Let $G$, $G_0$ and $V$ be as in Definition 3.1.3, and let $k$ be a positive integer at most $n/2$. Additionally, let $\Omega$ be a set of $k$-dimensional subspaces of $V$ so that $(G,\Omega)$ is a transitive subspace action satisfying the conditions in one of the cases (i)–(iii) of Proposition 3.1.4. If $G_0$ is orthogonal and $\Omega$ contains a non-degenerate subspace $U$, then let $\Delta$ be the set of all $k$-dimensional subspaces $W$ of $V$, such that $W$ is similar to $U$ and $W^\perp$ is similar to $U^\perp$. Otherwise, let $\Delta$ be the set of all $k$-dimensional subspaces of $V$ of the same type as the subspaces in $\Omega$, i.e., totally singular, non-degenerate, or nonsingular.

Our definition of $\Delta$ accounts for the two distinct actions of $G$ on non-degenerate $k$-dimensional subspaces, when $k$ and $\dim(V)$ are odd and $G$ is orthogonal. On the other hand, in the orthogonal non-degenerate case where either $k$ or $\dim(V)$ is even,

the type of $U^\perp$ is completely determined by the type of $U$ and the type of $V$ (see [17, Table 2.2]).

**Proposition 3.1.6.** *Let $G$, $G_0$, $V$, $n$ and $q$ be as in Definition 3.1.3. In addition, let $\Omega$ and $\Delta$ be as in Assumption 3.1.5, so that each subspace in $\Omega$ has dimension $k \leqslant n/2$, and suppose that $G$ does not act transitively on $\Delta$. Then $G$ has exactly two orbits on $\Delta$, each of size $|\Delta|/2 = |\Omega|$, and either:*

(a) *$G_0 = \mathrm{P\Omega}^+(n,q)$, $k = n/2$, the subspaces in $\Omega$ are totally singular, and $\mathrm{PGO}^+(n,q) \cap G$ is a subgroup of $\mathrm{PSO}^+(n,q)$ if $q$ is odd or of $\mathrm{P\Omega}^+(n,q)$ if $q$ is even; or*

(b) *$G_0 = \mathrm{P\Omega}^\pm(n,q)$, $k$ and $q$ are odd, and the subspaces in $\Omega$ are non-degenerate. In this case, the two orbits on $\Delta$ correspond to the similar but non-isometric non-degenerate quadratic forms on $k$-dimensional subspaces of $V$ mentioned in Lemma 2.2.9(iii).*

*Furthermore, no almost simple group with socle $G_0$ acts primitively on $\Delta$. If, in addition, $G \leqslant \mathrm{Aut}(G_0)$, then the actions of $G$ on the two orbits of $\Delta$ are equivalent.*

*Proof.* We deduce from [25, Remark 4.1.2] that either (b) holds (and in particular, $G$ has two orbits on $\Delta$), or $G_0$ and $\Omega$ are as in (a). In the latter case, [89, Lemma 2.5.8] shows that $G$ is as specified in (a), and again that $G$ has two orbits on $\Delta$. Additionally, in case (b), [89, Tables 3.5.E–G] and the tables in [17, §8.2] imply that $G$ is a proper subgroup of $\mathrm{Aut}(G_0)$. Thus in each case, some almost simple group with socle $G_0$ acts transitively on $\Delta$. It now follows from elementary permutation group theory (see [51, Theorem 1.6A]) that no almost simple group with socle $G_0$ acts primitively on $\Delta$, and that if $G \leqslant \mathrm{Aut}(G_0)$, then the actions of $G$ on the two orbits of $\Delta$ are equivalent. □

It is in fact possible to describe more precisely which subgroups of $\mathrm{Aut}(G_0)$ act transitively on $\Delta$ when (a) and (b) hold; see [89, Tables 3.5.E–3.5.G] and the tables in [17, §8.2].

We conclude this section by highlighting an important property of the finite almost simple classical groups, and then proving a related lemma regarding base sizes of primitive actions. We deduce the following proposition from the statements about the structure of $\mathrm{Out}(G_0)$ in [89, §2.2–2.8]. A similar claim is made in [72, p. 29]; however, the 8-dimensional orthogonal exception is not mentioned here.

**Proposition 3.1.7.** *Let $G$ be a finite almost simple classical group and $G_0 := \mathrm{soc}(G)$. If $G_0 = \mathrm{P\Omega}^+(8,q)$ with $q$ odd, and if $G$ contains a triality automorphism of*

*$G_0$, then $G/G_0$ has a subnormal series of length at most 4, with each factor group cyclic. Otherwise, $G/G_0$ has a normal series of length at most 3, again with each factor group cyclic.*

This proposition implies that if $H$ is a subnormal subgroup of $G$ that contains $G_0$, then $G$ has a series $H = T_0 \trianglelefteq T_1 \trianglelefteq \ldots \trianglelefteq T_r = G$ of subnormal subgroups, with each factor group cyclic. For example, we may choose an appropriate subseries of a composition series for $G$ that contains $H$.

The lemma below is very similar to [113, Lemma 11], and our proof is essentially the same (see also [72, §3.3]).

**Lemma 3.1.8.** *Let $G$ be a finite almost simple classical group acting primitively and faithfully on a set $\Omega$, and let $H$ be a subnormal subgroup of $G$ containing $G_0 := \mathrm{soc}(G)$. Suppose also that $G$ has a series $H = T_0 \trianglelefteq T_1 \trianglelefteq \ldots \trianglelefteq T_r = G$ of subnormal subgroups, with each factor group cyclic. Then $b(G,\Omega) \leqslant b(H,\Omega) + r$.*

*Proof.* We may assume that $H < G$. Suppose first that $(G_0, \Omega)$ is equivalent to the action $(A_m, \{1,\ldots,m\})$, for some $m \geqslant 5$. Since $G$ acts primitively on $\Omega$, it is clear that $G$ is isomorphic to a subgroup of $S_m$. Hence $H \cong A_m$ and $G \cong S_m$, and the result follows from Example 3.1.2.

In the remaining cases, let $i \in \{1,\ldots,r\}$, let $\mathcal{B}$ be a base for $T_{i-1}$ of size $b(T_{i-1})$, and let $K := (T_i)_{(\mathcal{B})}$. As $K \cap T_{i-1} = 1$, the Second Isomorphism Theorem shows that $K$ is isomorphic to a subgroup of the cyclic group $T_i/T_{i-1}$. Furthermore, as $(G_0,\Omega)$ is not equivalent to $(A_m, \{1,\ldots,m\})$ for any $m$, there exists a $K$-orbit $\Delta$ of $\Omega$ on which the cyclic group $K$ acts regularly [67, Theorem 1.2]. Thus for any choice of $\alpha \in \Delta$, the set $\mathcal{B} \cup \{\alpha\}$ is a base for $T_i$ of size at most $b(T_{i-1}) + 1$ (if $K = 1$, then we can choose $\alpha \in \mathcal{B}$). As this holds for each $i$, we obtain the result. □

### 3.1.2 Main theorems

We now state our theorems that bound the base sizes of primitive subspace actions of finite almost simple classical groups. Note that we restrict our attention to cases (i)–(iii), (v) and (vi) of Proposition 3.1.4. See [113, Proposition 1, Proposition 8] for results about the base sizes of the actions in cases (iv), (vii) and (viii), or [72, p. 30] in case (iv) when the dimension is less than 6.

First, we focus on the primitive actions of finite almost simple classical groups on subspaces of the natural module. Here, $\delta_{1k}$ is the Kronecker delta.

**Theorem 3.1.9.** *Suppose that $G$ is a finite almost simple classical group, and let $V := \mathbb{F}_{q^u}^n$ be the natural module for $G_0 := \mathrm{soc}(G)$, so that $q$ is a prime power, $n$ is*

*an integer greater than* 1, $u = 2$ *if* $G$ *is unitary, and* $u = 1$ *otherwise. Additionally, let* $k$ *be a positive integer less than* $n$*, and let* $t := \lceil n/k \rceil$*. Finally, let* $\Omega$ *be a set of* $k$*-dimensional subspaces of* $V$*, such that* $(G, \Omega)$ *is a primitive subspace action.*

(i) *Suppose that* $G_0$ *is linear. Then either:*

  (a) $b(G, \Omega) \geqslant t + 1$*; or*

  (b) $k = 1$*,* $q = 2$*, and* $b(G, \Omega) = n$*.*

(ii) *Suppose that* $G_0$ *is symplectic. Then either:*

  (a) $b(G, \Omega) \geqslant t$*; or*

  (b) $k = 1$*,* $G = \mathrm{PSp}(4, 2)'$*, and* $b(G, \Omega) = 3$*.*

(iii) *Suppose that* $G_0$ *is unitary. Then either:*

  (a) $b(G, \Omega) \geqslant t$*; or*

  (b) $k \mid (n - 1)$*,* $(q + 1) \mid n$*,* $\mathrm{PGU}(n, q) \not\trianglelefteqslant G$*, and* $b(G, \Omega) \geqslant t - 1$*.*

(iv) *Suppose that* $G_0 = \mathrm{P}\Omega^{\varepsilon}(n, q)$*, with* $\varepsilon \in \{\circ, +, -\}$*. Then either:*

  (a) $b(G, \Omega) \geqslant t$*;*

  (b) $k \mid (n - 1)$*, and* $b(G, \Omega) \geqslant t - 1$*; or*

  (c) $k \mid (n - 2)$*,* $n$ *is even,* $q \leqslant 3$*,* $\mathrm{PSO}^{\varepsilon}(n, q) \not\trianglelefteqslant G$*,* $b(G, \Omega) \geqslant t - 1 - \delta_{1k}$*, and if* $q = 3$*, then* $4 \mid n$ *if and only if* $\varepsilon = +$*.*

As stated in §1.0.1, for most of the families of actions $(G, \Omega)$ specified in the above theorem, no reasonable lower bounds for $b(G, \Omega)$ were previously known. The following observation will be useful when proving this theorem.

**Remark 3.1.10.** Recall that $b(H, \Omega) \leqslant b(G, \Omega)$ for any subgroup $H$ of $G$. Additionally, if $H \trianglelefteqslant G$ and $(G, \Omega)$ is a primitive subspace action, then $H$ acts transitively on $\Omega$ (see [51, Theorem 1.6A]). Hence to prove Theorem 3.1.9, it suffices to consider the transitive subspace actions of $G_0$, $\mathrm{PSp}(4, 2)$, and, where appropriate, $\mathrm{PGU}(n, q)$ and $\mathrm{PSO}^{\varepsilon}(n, q)$, that satisfy the conditions in one of the cases (i)–(iii) of Proposition 3.1.4.

It is not sufficient, however, to consider the finite almost simple classical groups up to isomorphism. This is because if $G_1$ and $G_2$ are isomorphic finite almost simple classical groups that are related to geometric spaces of different types or dimensions, then a given primitive subspace action of $G_1$ may not be a subspace action of $G_2$; see [23, Remark 1.1].

In certain cases with $k \leqslant 2$, [113, §2.1–2.2] gives upper bounds for the base size of the group $\mathrm{P}I(\kappa)$ from (2.3.2), acting primitively on a set of subspaces of $V = (V, \kappa)$. In the subsequent sections of this chapter, we will combine these upper bounds with Theorem 3.1.9 to obtain a very narrow range (and sometimes an exact value) for the base sizes of almost simple subgroups of $\mathrm{P}I(\kappa)$, in the relevant cases. In fact, in the case where $\kappa$ is quadratic, $n$ is even and at least 6, and each subspace in $\Omega$ is one-dimensional, [113, Lemma 8] shows directly that $b(\mathrm{P}I(\kappa))$ is always equal to our lower bound of $t - 1$.

Next, we consider the primitive action of a finite linear group on a set $\Omega$ of pairs $\{X, Y\}$ of subspaces of the natural module $V$. By Proposition 3.1.4, $\Omega$ is either a set of complementary pairs, i.e., with $X \oplus Y = V$, or a set of *nested* pairs, i.e., with $X \subseteq Y$ or $Y \subseteq X$. Additionally, one subspace in each pair has dimension less than $\dim(V)/2$. Recall that the graph automorphism of $\mathrm{PSL}(n, q)$ is the image in $\mathrm{Aut}(G_0)$ of the duality automorphism of $\mathrm{SL}(n, q)$, which maps each matrix in the group to its inverse transpose.

**Theorem 3.1.11.** *Let $q$ be a prime power and $n$ an integer at least 3, such that $G_0 := \mathrm{PSL}(n, q)$ is almost simple, and let $H := \langle \mathrm{PGL}(n, q), \theta \rangle$, where $\theta$ is the graph automorphism of $\mathrm{PSL}(n, q)$. Additionally, let $V := \mathbb{F}_q^n$ be the natural module for $G$, and let $\Omega$ be a set of pairs $\{X, Y\}$ of subspaces of $V$ such that $k := \dim(X) < \dim(Y)$ and $(H, \Omega)$ is a primitive subspace action. Then either:*

(i) $b(H, \Omega) \leqslant \lceil n/k \rceil$; *or*

(ii) $k > 1$, $\lceil n/k \rceil = 3$, *each element of $\Omega$ is a pair of nested subspaces of $V$, and* $b(H, \Omega) \leqslant 4$.

Now, we observe from [89, Table 3.5.A] and the tables in [17, §8.2] that $K := \mathrm{Aut}(\mathrm{PSL}(n, q))$ acts primitively on $\Omega$, and from [89, §2.2] that $K/H$ is cyclic. Hence $b(K, \Omega) \leqslant b(H, \Omega) + 1$ by Lemma 3.1.8. As $b(R, \Omega) \leqslant b(K, \Omega)$ for any subgroup $R$ of $K$ containing $\langle \mathrm{PSL}(n, q), \theta \rangle$, Theorem 3.1.11 in fact gives an upper bound for the base size of any such $R$. We will see that, at least when $k = 1$, the base size of $K$ can achieve the upper bound of $\lceil n/k \rceil + 1$. Of course, if $q$ is prime, then $\mathrm{PSL}(n, q)$ has no nontrivial field automorphisms, and so $K = H$.

Note also that Halasi, Liebeck and Maróti [72, Proposition 3.5] proved that the (imprimitive) action of $\mathrm{PSL}(n, q)$ on $\Omega$ has a base size of at most $n/k + 11$. As $H/\mathrm{PSL}(n, q)$ has a normal series of length at most 2, with each factor group cyclic (see [89, §2.2]), Lemma 3.1.8 shows that this corresponds to an upper bound of $n/k + 13$ for $b(H, \Omega)$. Our upper bound from Theorem 3.1.11 is significantly lower.

The subsequent sections of this chapter are dedicated to proving the above two theorems. In fact, in the symplectic, unitary and orthogonal cases of Theorem 3.1.9, we will prove more general results about pointwise stabilisers of sets of subspaces of $V$.

Many of the arguments in the remaining proofs in this chapter were inspired by those used in [27, §4.1] to prove results regarding base sizes of subspace actions of simple algebraic groups, and involve similar ideas. However, our arguments are in general more detailed, and often require more technical details than their algebraic group counterparts.

### 3.1.3 Relationships between base size and other statistics

We conclude this section by discussing certain applications of the base size bounds from Theorems 3.1.9 and 3.1.11, in the context of other statistics related to permutation groups.

First, we compare our base size bounds with known bounds on the *irredundant base size* and *height* of the corresponding groups. The irredundant base size $I(G,\Omega)$ of a permutation group $(G,\Omega)$ is the maximum size of an ordered sequence $(\omega_1,\dots,\omega_r)$ of elements of $\Omega$ such that

$$1 = G_{(\omega_1,\dots,\omega_r)} < G_{(\omega_1,\dots,\omega_{r-1})} < \dots < G_{\omega_1} < G.$$

Additionally, the height $H(G,\Omega)$ is the maximum size of a subset $X$ of $\Omega$ such that $G_{(X)} < G_{(Y)}$ for each proper subset $Y$ of $X$. Note that $b(G,\Omega) \leqslant H(G,\Omega) \leqslant I(G,\Omega)$ (see [57, p. 3]).

Let $u \in \{1,2\}$, $n$, $q$, $k$, $G$ and $\Omega$ be as in Theorem 3.1.9, and suppose that the finite almost simple classical group $G$ lies in $\mathrm{PGL}(n,q^u)$ (for example, $G$ may be any almost simple subgroup of the group $\mathrm{P}\Delta(\kappa)$ from (2.3.2), with socle $\mathrm{P}\Omega(\kappa)'$). Then it follows from [86, Lemma 2.3.3] and [87, Theorem 3.1] that $I(G,\Omega) \leqslant (k+1)n-2k+1$. Hence the ratio between this upper bound for $I(G,\Omega)$ and the lower bound for $b(G,\Omega)$ from Theorem 3.1.9 is equal to $((k+1)n-2k+1)/(\lceil n/k\rceil + c)$, where $c$ is a constant. For a fixed value of $k$, as $n$ tends to infinity, this ratio tends to the constant $k(k+1)$. Note that the general ratio does not depend on $q$. As $H(G,\Omega) \leqslant I(G,\Omega)$, this is also a ratio between an upper bound for $H(G,\Omega)$ and our lower bound for $b(G,\Omega)$. Note that [57, Lemma 7.6] gives a larger (or equal when $k=1$) upper bound of $2kn-1$ for $H(G,\Omega)$.

Next, let $n$, $q$, $k$, $H$ and $\Omega$ be as in Theorem 3.1.11. The proof of [57, Lemma 7.7] shows that the action of $H$ on $\Omega$ has a height of at most $4kn$ (note that the $2\log\log_p q$ term from this proof is not relevant here, as $H$ contains no nontrivial field

automorphisms of $\mathrm{PSL}(n,q)$). Although we will not prove a lower bound for $b(H,\Omega)$, we will present in §3.3 the exact value of $b(H,\Omega)$ for specific examples, determined using Magma. Based on these examples, it seems reasonable to conjecture that there exists an absolute non-negative constant $c'$ such that $b(H,\Omega) \geqslant \lceil n/k \rceil - c'$ (when $\lceil n/k \rceil > 3$). If this is indeed the case, then as $n$ tends to infinity with $k$ fixed, the ratio between the upper bound for the height and the lower bound for the base size tends to the constant $4k^2$.

Now, given a finite permutation group $(J,\Delta)$ and a positive integer $r$, let $J^{(r),\Delta}$ denote the *$r$-closure* of $(J,\Delta)$, i.e., the largest subgroup of the symmetric group $\mathrm{Sym}(\Delta)$ that has the same orbits as $J$ on the set of ordered $r$-tuples of elements of $\Delta$. Wielandt [145, Theorem 5.8, Theorem 5.12] proved that $J = J^{(r),\Delta}$ for all $r \geqslant b(J,\Delta)+1$.

The related *closure number* $k(J)$ of the finite abstract group $J$, defined in [55], is the smallest positive integer $r$ such that $J = J^{(r),\Delta}$ for each set $\Delta$ on which $J$ acts faithfully (but not necessarily transitively). Let $G$ be a finite simple classical group with natural module $V$. Using Wielandt's result and the upper bounds from [72, §3.1] and [113, §2] for the base size of a primitive subspace action of $G$, an upper bound for $k(G)$ is determined in [55]. In particular, if $\dim(V)$ is sufficiently large, then $k(G)$ is at most $\dim(V)+c$, where $c$ is a constant that depends only on the type of $G$ (linear, unitary, symplectic or orthogonal).

Finally, fix the type of $G$, and let $\Omega$ be a set of one-dimensional subspaces of $V$ on which $G$ acts primitively (such a set exists by the tables in [89, §3.5] and [17, §8.2]). As observed in [55], there is an infinite family of such groups $G$, of unbounded dimension, for which the bound on $k(G)$ from the previous paragraph is equal to one plus the lower bound on $b(G,\Omega)$ from Theorem 3.1.9. Therefore, for every such group $G$, it is not possible to obtain a better upper bound on $k(G)$ solely by considering base sizes and applying Wielandt's result.

## 3.2 Linear groups acting on subspaces

Let $n$ be an integer and $q$ a prime power such that $\mathrm{PSL}(n,q)$ is simple, and let $\Omega$ be the set of $k$-dimensional subspaces of $V := \mathbb{F}_q^n$, for some positive integer $k$. In this section, we prove the linear case of Theorem 3.1.9. By Proposition 3.1.4, we may assume that $k \leqslant n/2$. In addition, Proposition 3.1.6 shows that $\mathrm{PSL}(n,q)$ acts transitively on $\Omega$. Indeed, it suffices by Remark 3.1.10 to consider the action of $\mathrm{PSL}(n,q)$ on $\Omega$.

Recall that the action on $\Omega$ of a group $G$ satisfying $\mathrm{PSL}(n,q) \leqslant G \leqslant \mathrm{PGL}(n,q)$ is

induced by the action on this set of the group $K$ satisfying $\mathrm{SL}(n,q) \leqslant K \leqslant \mathrm{GL}(n,q)$ and $G \cong K/Z(K)$. Thus, in this section and the next, we often identify $G$ with $K$. In particular (with a slight abuse of notation), for a subset $\Delta$ of $\Omega$, we write "$G_{(\Delta)} = 1$" if $G_{(\Delta)}$ consists only of scalar matrices.

Additionally, throughout the remainder of this chapter, as well as in §6.4, we use the following notation.

**Definition 3.2.1.** For an integer $m$, let $I_m$ be the $m \times m$ identity matrix. Additionally, let $E_{i,j}$ be the $n \times n$ matrix whose $(i,j)$ entry is equal to 1, and whose remaining entries are equal to 0.

The $k = 1$ case of Theorem 3.1.9(i) is easy, and well known (for example, see [100, p. 147] for the case where $k = 1$ and $q > 2$).

**Proposition 3.2.2.** *Let $G$ be a group satisfying $\mathrm{PSL}(n,q) \leqslant G \leqslant \mathrm{PGL}(n,q)$, and let $\Omega$ be the set of one-dimensional subspaces of $V$. Additionally, let $\{e_1, e_2, \ldots, e_n\}$ be a basis for $V$. If $q = 2$, then $\mathcal{B} := \{\langle e_1\rangle, \ldots, \langle e_n\rangle\}$ is a base for $G$, and $b(G,\Omega) = n$. Otherwise, $\mathcal{B} \cup \{\langle e_1 + e_2 + \cdots + e_n\rangle\}$ is a base for $G$, and $b(G,\Omega) = n+1$.*

*Proof.* First observe that $I_n + E_{n,1}$ lies in $G$ and acts trivially on the hyperplane spanned by the first $n-1$ subspaces in $\mathcal{B}$. Since the fixed basis for $V$ can be chosen arbitrarily, we see that $G_{(\Delta)} > 1$ for each subset $\Delta$ of $\Omega$ whose span has dimension at most $n-1$. Hence $b(G) \geqslant n$, and each base for $G$ spans $V$. Conversely, the pointwise stabiliser $G_{(\mathcal{B})}$ is equal to the subgroup of $G$ consisting of all diagonal matrices. If $q = 2$, then this subgroup is trivial, as required.

Assume now that $q > 2$, and let $\omega$ be a primitive element of $\mathbb{F}_q$. If $n > 2$, then $G$ contains the non-scalar matrix $\mathrm{diag}(\omega, \omega^{-1}, 1, \ldots, 1)$, and if $n = 2$, then $G$ contains $\mathrm{diag}(\omega, \omega^{-1})$. As $G$ is almost simple, $q \neq 3$ in the latter case, and hence $\omega \neq \omega^{-1}$. Thus in each case $G_{(\mathcal{B})}$ contains a non-scalar matrix. It follows that no basis for $V$ is a base for $G$, and so $b(G,\Omega) > n$. On the other hand, any diagonal matrix that stabilises $\langle e_1 + e_2 + \cdots + e_n\rangle$ is a scalar matrix. Hence $\mathcal{B} \cup \{\langle e_1 + e_2 + \cdots + e_n\rangle\}$ is a base for $G$, and $b(G) = n+1$. □

Next, we consider the case $k > 1$.

**Proposition 3.2.3.** *Let $G := \mathrm{PSL}(n,q)$, and let $\Omega$ be the set of $k$-dimensional subspaces of $V$, with $1 < k \leqslant n/2$. Then $b(G,\Omega) \geqslant \lceil n/k \rceil + 1$.*

*Proof.* Let $t := \lceil n/k \rceil$, let $\mathcal{U} := \{U_1, \ldots, U_t\}$ be an arbitrary set of $t$ distinct $k$-dimensional subspaces of $V$, and let $X := \langle U_1, \ldots, U_{t-1}\rangle$. Additionally, choose a

basis $\mathcal{B} := \{e_1, \ldots, e_n\}$ for $V$ such that $\{e_1, \ldots, e_r\}$ is a basis for $X$ and $\{e_1, \ldots, e_s\}$ is a basis for $\langle \mathcal{U} \rangle$. It suffices to show that $G_{(\mathcal{U})} \neq 1$.

Observe that $r < n$. If $s < n$, then (with respect to $\mathcal{B}$) the matrix $I_n + E_{n,1}$ fixes each vector in the span of $\mathcal{U}$. Hence this matrix lies in $G_{(\mathcal{U})}$, and so $G_{(\mathcal{U})} \neq 1$. If instead $s = n$, then we may assume that $e_n \in U_t$. As $\dim(U_t) = k > 1$, it follows that $U_t$ contains some nonzero vector $a := \sum_{i=1}^{n-1} \alpha_i e_i$, where $\alpha_i \in \mathbb{F}_q$ for each $i$. Let $A := I_n + \sum_{i=1}^{n-1} \alpha_i E_{n,i}$. Notice that the image under $A$ of any vector $b := \sum_{i=1}^{n} \beta_i e_i \in U_t$ is equal to $b + \beta_n a \in U_t$, while $A$ fixes each vector in $X$. Thus $A \in G_{(\mathcal{U})}$, and we again conclude that $G_{(\mathcal{U})} \neq 1$. □

By the reasoning of Remark 3.1.10, this completes the proof of the linear case of Theorem 3.1.9.

We will now compare the lower bounds for $b(G, \Omega)$ from Theorem 3.1.9(i), in the case $k > 1$, with known upper bounds for $b(\mathrm{PSL}(n, q), \Omega)$. We first note that [27, Theorem 4(i)] gives very narrow bounds, and exact values in some cases, for analogous actions of certain algebraic groups, namely, the special linear groups defined over algebraic closures of finite fields. In particular, if $k$ divides $n$, then the base size of the action is equal to $n/k + 2$ if $1 < k < n/2$, and to 5 if $1 < k = n/2$. If instead $k$ does not divide $n$, then the base size lies between $\lceil n/k \rceil + 1$ and $\lceil n/k \rceil + 3$, with an upper bound of $\lceil n/k \rceil + 2$ if $\lceil n/k \rceil \neq 3$. The lower bound from Theorem 3.1.9(i) agrees with the lower bound in the algebraic case, in particular in the case where $k$ does not divide $n$.

Focusing now on finite groups, it is proved in [72, p. 24] that, if $k$ divides $n$, then $b(\mathrm{PSL}(n, q), \Omega) \leqslant n/k + 3$, and otherwise this base size is at most $\lceil n/k \rceil + 4$. In particular, when $k = n/2$, this upper bound is equal to the exact value in the algebraic case. Additionally, in the case where $k = 2$ and $n \geqslant 5$, [113, Lemma 4] gives an improved upper bound of $\lceil n/k \rceil + 2$ for $b(\mathrm{PGL}(n, q), \Omega)$, which agrees with the algebraic case. Note that this upper bound for the base size of $\mathrm{PGL}(n, q)$ is also an upper bound for the base size of its subgroup $\mathrm{PSL}(n, q)$. In general, since $\mathrm{PGL}(n, q)/\mathrm{PSL}(n, q)$ is cyclic (and since $\mathrm{PGL}(n, q)$ acts primitively on $\Omega$ by the tables in [89, §3.5] and [17, §8.2]), Lemma 3.1.8 yields $b(\mathrm{PGL}(n, q)) \leqslant b(\mathrm{PSL}(n, q)) + 1$. Combining these upper bounds with our lower bound of $\lceil n/k \rceil + 1$ yields a fairly narrow range for the base size. In particular, we obtain the following proposition.

**Proposition 3.2.4.** *Let $G$ be a group satisfying $\mathrm{PSL}(n, q) \leqslant G \leqslant \mathrm{PGL}(n, q)$, and let $\Omega$ be the set of $k$-dimensional subspaces of $V$, with $1 < k \leqslant n/2$. Then $\lceil n/k \rceil + 1 \leqslant b(G, \Omega) \leqslant \lceil n/k \rceil + 5$. Moreover, if $n \geqslant 5$ and $k = 2$, then $\lceil n/2 \rceil + 1 \leqslant b(G, \Omega) \leqslant \lceil n/2 \rceil + 2$.*

In fact, we will show in Lemma 3.3.5(i) below that the upper bound $b(G,\Omega) \leqslant n/k+2$ also applies whenever $k \mid n$ and $n/k \geqslant 3$. This improves the upper bound of $n/k+3$ from [72, p. 24].

We can gain an idea of how tight these bounds are by calculating the exact base sizes for actions of relatively small degree, using the Magma code in `base_size_linear`. For certain sets $\Omega$ of $k$-dimensional subspaces of $V$ (i.e., for certain values of $n$, $q$ and $k$), Table 3.2.1 gives the base size of $b(\mathrm{PSL}(n,q),\Omega)$, which is in fact equal to $b(\mathrm{PGL}(n,q),\Omega)$ in each considered case. For easy comparison between the actual base sizes and the known bounds, we specify the value $n/k$ in the table. The action in each case is primitive, as indicated by the corresponding tables in [17, §8.2].

In the calculated examples, we see that if $k \mid n$, then $b(\mathrm{PGL}(n,q),\Omega)$ is equal to the corresponding value from the algebraic case, except when $n/k = q = 2$ and $n \in \{4,6\}$, where the base size is equal to 4 instead of 5. Furthermore, when $k = 2$, $n \geqslant 5$ and $k \mid n$, the upper bound of $n/k+2$ from Proposition 3.2.4 is achieved. On the other hand, in each example with $k \nmid n$, the base size is equal to $\lceil n/k \rceil + 1$, which is equal to the lower bound given in Theorem 3.1.9(i). Hence, in general, this lower bound is tight. However, none of our examples achieve the upper bound of $\lceil n/k \rceil + 4$ from [72, p. 24]. Thus it seems possible that this upper bound could be reduced to $\lceil n/k \rceil + 3$, i.e., the base size achieved in the second row of Table 3.2.1.

Table 3.2.1: The base size of $\mathrm{PSL}(n,q)$ or $\mathrm{PGL}(n,q)$ acting primitively on a set $\Omega$ of $k$-dimensional subspaces of $\mathbb{F}_q^n$. Here, $r$ denotes any prime power between 3 and 9, inclusive.

| $n/k$ | $(n,q,k)$ | $b(\mathrm{PSL}(n,q),\Omega) = b(\mathrm{PGL}(n,q),\Omega)$ |
|---|---|---|
| 2 | $(4,2,2),(6,2,3)$ | 4 |
| 2 | $(4,r,2),(6,3,3),(8,2,4)$ | 5 |
| 7/3 | $(7,2,3)$ | 4 |
| 5/2 | $(5,2,2),(5,3,2),(5,4,2),(5,5,2)$ | 4 |
| 8/3 | $(8,2,3)$ | 4 |
| 3 | $(6,2,2),(6,3,2),(6,4,2)$ | 5 |
| 7/2 | $(7,2,2),(7,3,2)$ | 5 |
| 4 | $(8,2,2)$ | 6 |
| 9/2 | $(9,2,2)$ | 6 |

Next, we will briefly consider $b(G,\Omega)$ in certain cases where the almost simple linear group $G$ properly contains $\mathrm{PGL}(n,q)$. It follows from [89, Proposition 2.2.3] that if $\mathrm{P\Gamma L}(n,q) \neq \mathrm{PGL}(n,q)$, so that $q$ is not prime, then the quotient

of the two groups is cyclic. Similarly, if $\mathrm{Aut}(\mathrm{PSL}(n,q)) \neq \mathrm{P\Gamma L}(n,q)$, so that $n \geqslant 3$, then the quotient of these groups is again cyclic. Hence Lemma 3.1.8 shows that $b(\mathrm{PGL}(n,q)) \leqslant b(\mathrm{P\Gamma L}(n,q)) \leqslant b(\mathrm{PGL}(n,q)) + 1$, and $b(\mathrm{PGL}(n,q)) \leqslant b(\mathrm{Aut}(\mathrm{PSL}(n,q))) \leqslant b(\mathrm{PGL}(n,q)) + 2$, assuming that the larger group acts primitively on $\Omega$ in each case. Recall from Proposition 3.1.4 that if $\mathrm{Aut}(\mathrm{PSL}(n,q))$ is primitive, then $k = n/2$.

Table 3.2.2 compares the values of $b(\mathrm{PGL}(n,q),\Omega)$ and $b(\mathrm{P\Gamma L}(n,q),\Omega)$ for certain sets $\Omega$ of subspaces of $V$. Proposition 3.2.2 yields $b(\mathrm{PGL}(n,q))$ in the case $k = 1$, and the remaining base sizes here were again computed using the Magma code in `base_size_linear`. We see that $b(\mathrm{P\Gamma L}(n,q))$ can indeed be equal either to $b(\mathrm{PGL}(n,q))$ or $b(\mathrm{PGL}(n,q)) + 1$. We can also use the Magma code in `base_size_linear` to show that $b(\mathrm{Aut}(\mathrm{PSL}(n,q)),\Omega) = b(\mathrm{PGL}(n,q),\Omega) = 5$ when $n = 4$, $q \leqslant 5$ and $k = 2$, or when $n = 6$, $q = 2$ and $k = 3$. As above, the tables in [17, §8.2] imply that the actions described here are all primitive.

Table 3.2.2: The base sizes of $\mathrm{PGL}(n,q)$ and $\mathrm{P\Gamma L}(n,q)$ acting primitively on a set $\Omega$ of $k$-dimensional subspaces of $\mathbb{F}_q^n$. Here, $r$ denotes any integer in the set $\{4,8,9\}$, and $s$ denotes any integer in the set $\{4,8,9,16,25\}$.

| $n/k$ | $(n,q,k)$ | $b(\mathrm{PGL}(n,q),\Omega)$ | $b(\mathrm{P\Gamma L}(n,q),\Omega)$ |
|---|---|---|---|
| 2 | $(2,r,1)$ | 3 | 4 |
| 2 | $(4,s,2)$ | 5 | 5 |
| 5/2 | $(5,4,2)$ | 4 | 5 |
| 3 | $(3,r,1)$ | 4 | 5 |
| 3 | $(6,4,2)$ | 5 | 5 |
| 4 | $(4,r,1)$ | 5 | 6 |

## 3.3 Linear groups acting on pairs of subspaces

Let $n \geqslant 3$ be an integer, $q$ a prime power, $G := \mathrm{PGL}(n,q)$ and $H := \langle G, \theta \rangle$, where $\theta$ is the graph automorphism of $\mathrm{PSL}(n,q)$, i.e., the image in $\mathrm{Aut}(\mathrm{PSL}(n,q))$ of the duality automorphism of $\mathrm{SL}(n,q)$ (which maps each matrix to its inverse transpose). Additionally, let $\Omega$ be a set of unordered pairs of subspaces of $V := \mathbb{F}_q^n$, such that $H$ acts primitively on $\Omega$. As in §3.2, we identify $G$ with $\mathrm{GL}(n,q)$, and for a subset $\Delta$ of $\Omega$, we write "$G_{(\Delta)} = 1$" if $G_{(\Delta)}$ contains only scalar matrices.

The purpose of this section is to prove Theorem 3.1.11 and determine tight upper bounds for $b(H,\Omega)$. By Proposition 3.1.4, there exists a positive integer $k < n/2$ such that $\Omega$ is either the set of nested pairs $\{X,Y\}$ of subspaces of $V$, with $\dim(X) = k$,

$\dim(Y) = n - k$, and $X \subseteq Y$; or the set of complementary pairs $\{X, Y\}$, with $\dim(X) = k$ and $X \oplus Y = V$. In each case, $\lceil n/k \rceil \geqslant 3$.

The following lemma is a key component in the proof of Theorem 3.1.11.

**Lemma 3.3.1.** *Let $\mathcal{K} := \{\{X_0, Y_0\}, \{X_1, Y_1\}, \ldots, \{X_r, Y_r\}\}$ be a subset of $\Omega$, with $\dim(X_i) = k$ for each $i$. If exactly one of $\langle X_0, X_1, \ldots, X_r\rangle = V$ and $\bigcap_{i=1}^{r} Y_i = \{0\}$ holds, then no element of $H \setminus G$ stabilises $\mathcal{K}$ pointwise.*

*Proof.* Let $\alpha \in H \setminus G$. Suppose first that $\langle X_0, X_1, \ldots, X_r\rangle = V$, so that $V$ is the only subspace of $V$ that contains $X_i$ for all $i$. It follows from Proposition 2.3.5 that $V^\alpha = \{0\}$ is the only subspace of $V$ that lies in $X_i^\alpha$ for all $i$. Hence $\bigcap_{i=1}^{r} X_i^\alpha = \{0\}$. If $\bigcap_{i=1}^{r} Y_i \neq \{0\}$, then we conclude that $X_i^\alpha \neq Y_i$ for some $i$. In particular, $\alpha$ does not stabilise $\mathcal{K}$ pointwise. By duality, we reach the same conclusion if $\bigcap_{i=1}^{r} Y_i = \{0\}$ and $\langle X_0, X_1, \ldots, X_r\rangle \neq V$. □

Throughout the remainder of this section, we fix a basis $\{e_1, e_2, \ldots, e_n\}$ for $V$. In the following definition, we highlight several important subspaces of $V$ in the case $k \mid n$. Note that $\mathrm{GL}(k, q)$ is 2-generated [141, pp. 228–229].

**Definition 3.3.2.** Suppose that $k \mid n$ (so that $n/k \geqslant 3$), and let

$$X_i := \langle e_{1+ik}, e_{2+ik}, \ldots, e_{k+ik}\rangle$$

for each $i \in \{0, 1, \ldots, n/k - 1\}$. Additionally, let $\{x_1, y_1\}$ be a generating pair for $\mathrm{GL}(k, q)$, let $x$ be the element of $\mathrm{GL}(n, q)$ that acts as $x_1$ on $X_1$ and as the identity on $\langle X_j \mid j \neq 1\rangle$, and let $y$ be the element of $\mathrm{GL}(n, q)$ that acts as $y_1$ on $X_2$ and as the identity on $\langle X_j \mid j \neq 2\rangle$. We define

$$R := \langle e_j + e_{j+k} + \cdots + e_{j+(n/k-1)k} \mid j \in \{1, 2, \ldots, k\}\rangle$$

and

$$W := \langle e_j + (e_{j+k})^x + (e_{j+2k})^y + e_{j+3k} \cdots + e_{j+(n/k-1)k} \mid j \in \{1, 2, \ldots, k\}\rangle.$$

We first consider the case $k = 1$. An important observation here, and in the general case $k \geqslant 1$, is that if an element $g \in G$ stabilises a pair $\{X, Y\} \in \Omega$, then $g$ stabilises each of $X$ and $Y$, since $\dim(X) \neq \dim(Y)$. Hence if $g$ stabilises each pair in a subset $\{\{X_1, Y_1\}, \ldots, \{X_j, Y_j\}\}$ of $\Omega$, then $g$ stabilises each intersection of any number of the subspaces labelled $X_i$ or $Y_i$.

**Lemma 3.3.3.** *Suppose that $n \geqslant 3$ and $k = 1$. Then $b(H, \Omega) \leqslant n$.*

*Proof.* Let $R$ and $X_i$ be the subspaces of $V$ from Definition 3.3.2. We split the proof into three cases.

**Case (a)**: Each element of $\Omega$ is a pair of nested subspaces of $V$, and $n = 3$. It is clear that

$$\mathcal{K} := \{\{X_0, \langle X_0, X_2\rangle\}, \{X_1, \langle X_1, X_2\rangle\}, \{R, \langle R, X_2\rangle\}\}$$

is a subset of $\Omega$. Additionally, the intersection $U$ of $\langle X_0, X_2\rangle$, $\langle X_1, X_2\rangle$ and $\langle R, X_2\rangle$ is equal to $X_2$. Hence $G_{(\mathcal{K})} \leqslant G_{(X_0,X_1,X_2,R)}$, which is trivial by Proposition 3.2.2. Furthermore, $\langle X_0, X_1, R\rangle = V$, while $U$ is nonzero. Hence Lemma 3.3.1 implies that $\mathcal{K}$ is a base for $H$.

**Case (b)**: Each element of $\Omega$ is a pair of nested subspaces of $V$, and $n > 3$. For each $j \in \{0, \dots, n-3\}$, let $Y_j$ be the subspace of $V$ spanned by the collection of subspaces $X_i$ for $i \neq j+1$. Additionally, let $Y_{n-2} := \langle R, X_i \mid i \notin \{0, 1\}\rangle$. Then $X_i \subset Y_i$ for each $i \in \{0, \dots, n-2\}$, $R \subset Y_{n-2}$, and $\bigcap_{j=0}^{n-2} Y_j = X_{n-1}$.

Thus

$$\mathcal{L} := \{\{X_0, Y_0\}, \{X_1, Y_1\}, \dots, \{X_{n-2}, Y_{n-2}\}, \{R, Y_{n-2}\}\}$$

is a subset of $\Omega$ of size $n$, and $G_{(\mathcal{L})} \leqslant G_{(X_0,X_1,\dots X_{n-1},R)}$, which is again trivial by Proposition 3.2.2. Moreover, no element of $H \setminus G$ maps $Y_{n-2}$ to both $X_{n-2}$ and $R$. Therefore, $\mathcal{L}$ is a base for $H$.

**Case (c)**: Each element of $\Omega$ is a pair of complementary subspaces of $V$. For each $j \in \{0, \dots, n-2\}$, let $Y_j$ be the subspace of $V$ spanned by each $X_i$ except for $X_j$. Then $X_i \oplus Y_i = V$ for each $i$, and $\bigcap_{j=1}^{n-2} Y_j = X_{n-1}$. Note also that $R \oplus Y_0 = V$. Hence

$$\mathcal{M} := \{\{X_0, Y_0\}, \{X_1, Y_1\}, \dots, \{X_{n-2}, Y_{n-2}\}, \{R, Y_0\}\}$$

is a subset of $\Omega$ of size $n$, and $G_{(\mathcal{M})} \leqslant G_{(X_0,X_1,\dots,X_{n-1},R)} = 1$. Furthermore, no element of $H \setminus G$ maps $Y_0$ to both $X_0$ and $R$. Thus $\mathcal{M}$ is a base for $H$. □

Using the Magma code in `base_size_linear`, we can calculate $b(H, \Omega)$ when $k = 1$, for various small values of $n$ and $q$. For most of our computational examples here and throughout this section, it suffices to calculate $b(G, \Omega)$, as this base size achieves the theoretical upper bound for $b(H, \Omega)$, and hence $b(H, \Omega) = b(G, \Omega)$. In each case where this does not occur, $q = 2$, and so $H = \mathrm{Aut}(\mathrm{PSL}(n, q))$ is easily constructed in Magma.

Table 3.3.1 summarises our results and shows that the upper bound for the base size given in Lemma 3.3.3 is tight, but is not always achieved when $q = 2$. We can also use Magma to determine the base size of $K := \mathrm{Aut}(\mathrm{PSL}(n, q))$ in its action on $\Omega$, in certain cases where $H < K$ (and $k = 1$). In particular, when $n \in \{3, 4\}$

and $q \in \{4, 8, 9\}$, the base size of $K$ is always equal to $n$, except in the nested case with $n = 3$ and $q = 4$, where $b(K, \Omega) = n + 1 = 4$. This exceptional case achieves the maximum base size of $b(H, \Omega) + 1$, as discussed below the statement of Theorem 3.1.11. Note also that all of the actions of $H$ and $K$ mentioned here are primitive by the tables in [17, §8.2].

Table 3.3.1: The base size of $H = \langle \mathrm{PGL}(n, q), \theta \rangle$ acting primitively on a set $\Omega$ of complementary or nested pairs of subspaces $\{X, Y\}$ of $\mathbb{F}_q^n$ with $1 = \dim(X) < \dim(Y)$. Here, $r$ denotes a prime power between 3 and 9, inclusive, and $\Delta$ denotes the difference between the upper bound for the base size given in Lemma 3.3.3 and the actual base size.

| $(n, q)$ | Pair type | $b(H, \Omega)$ | $\Delta$ |
|---|---|---|---|
| $(3, 2)$ | Complementary | 2 | 1 |
| $(3, 2)$ | Nested | 3 | 0 |
| $(3, r)$ | Either | 3 | 0 |
| $(4, 2)$ | Either | 3 | 1 |
| $(4, r)$ | Either | 4 | 0 |
| $(5, 2)$ | Either | 4 | 1 |
| $(6, 2)$ | Either | 5 | 1 |

From now on, we assume that $k > 1$. In our next few results, we also assume that $k \mid n$.

**Proposition 3.3.4.** *Suppose that $k \mid n$ and $k > 1$, and let $s \in \{0, 1, \ldots, n/k - 1\}$. Additionally, let $X_i$, $R$ and $W$ be the subspaces of $V$ from Definition 3.3.2, and let $T_s := \langle X_i \mid i \neq s \rangle$. Then $T_s \oplus R = T_s \oplus W = V$.*

*Proof.* Let $U \in \{R, W\}$, and let $x$ and $y$ be as in Definition 3.3.2. We claim that if $\sum_{r=0}^{n} \alpha_r e_r$ is a nonzero vector in $U$ (with each $\alpha_r \in \mathbb{F}_q$), then there exists $m \in \{1, \ldots, n\}$ such that $e_m \in X_s$ and $\alpha_m \neq 0$. If $U = R$, or if $U = W$ and $s \notin \{1, 2\}$, then this is clear from the definitions of $R$ and $W$. If instead $U = W$ and $s = 1$, then $x$ stabilises $X_s$. Hence the images under $x$ of the basis vectors in $X_s$ are linearly independent vectors in $X_s$, and we again deduce the claim using the definition of $W$. We reach the same conclusion if $U = W$ and $s = 2$, by considering the action of $y$ on $X_2$. Therefore, in each case, $T_s \cap U = \{0\}$. As $\dim(T_s) = n - k$ and $\dim(U) = k$, we conclude that $T_s \oplus U = V$. □

The statement and proof of the first part of the following lemma are adapted from the proof of [27, Proposition 4.2]. Note that the subspaces in the stabilised set in the second part of this lemma are not all equidimensional.

**Lemma 3.3.5.** *Suppose that $k \mid n$ and $k > 1$, and let $X_i$, $R$ and $W$ be the subspaces of $V$ from Definition 3.3.2.*

(i) *$\{X_0, X_1, \ldots, X_{n/k-1}, R, W\}$ is a base for $G$, with respect to its usual action on $k$-dimensional subspaces of $V$. In particular, $b(G) \leqslant n/k + 2$.*

(ii) *Suppose that $n/k > 3$. Then $G_{(X_0, X_1, \ldots, X_{n/k-1}, R, \langle X_{n/k-1}, W\rangle)} = 1$.*

*Proof.* Let $x$, $y$, $x_1$ and $y_1$ be as in Definition 3.3.2, let $t := n/k - 1$, and for each $i \in \{0, 1, \ldots, t\}$, let $\theta_i$ be the isomorphism from $X_0$ to $X_i$ that maps $e_j$ to $e_{j+ik}$ for all $j \in \{1, 2, \ldots, k\}$. Additionally, for a vector $w \in W$, let $w_i$ be the projection of $w$ onto $X_i$.

Observe that each element of $G_{(X_0, X_1, \ldots, X_t)}$ is a block diagonal matrix, with each diagonal block equal to an element of $\mathrm{GL}(k, q)$. It follows that any given element $g \in G_{(X_0, X_1, \ldots, X_t, R)}$ has all diagonal blocks equal to a fixed matrix $A \in \mathrm{GL}(k, q)$ (determined by $g$). Hence $v^{A\theta_i} = v^{\theta_i A}$ for each $v \in X_0$ and $i \in \{0, 1, \ldots, t\}$ (note that we are slightly abusing notation here and considering $A$ as an element of both $\mathrm{GL}(X_0)$ and $\mathrm{GL}(X_i)$).

(i) Suppose that $g \in G_{(X_0, X_1, \ldots, X_t, R, W)}$, let $w \in W$, and let $z := w^g$. Then $z_i = w_i^A$ for all $i \in \{0, 1, \ldots, t\}$. The definition of $W$ yields

$$w_0^{\theta_1 x_1 A} = w_1^A = z_1 = z_0^{\theta_1 x_1} = w_0^{A\theta_1 x_1} = w_0^{\theta_1 A x_1}.$$

This holds for all $w_0 \in X_0$, and hence $[A, x_1] = 1$. Similarly, $[A, y_1] = 1$. Thus $A$ centralises $\langle x_1, y_1\rangle = \mathrm{GL}(k, q)$, and so $A$ is a scalar matrix. This implies that $g$ itself is a scalar matrix. Hence $\{X_0, X_1, \ldots, X_t, R, W\}$ is a base for $G$, as required.

(ii) Let $w \in W$, let $S := \{X_0, X_1, \ldots, X_t, R, \langle X_t, W\rangle\}$, and suppose that $g \in G_{(S)}$. Then $w^g = u + h$ for some $u \in W$ and $h \in X_t$. In particular, $w_t^A = u_t + h$, and $w_j^A = u_j$ for all $j \in \{0, 1, \ldots, t-1\}$. Using the definition of $W$, we deduce that $w_t^A = w_0^{\theta_t A} = w_0^{A\theta_t} = u_0^{\theta_t} = u_t$. Hence $h = 0$, and so $G_{(S)} = G_{(X_0, X_1, \ldots, X_t, R, W)}$, which is equal to 1 by (i). □

Note that Lemma 3.3.5(i) implies that the action of $\mathrm{PSL}(n, q)$ on $k$-dimensional subspaces of $V$ also has a base size of at most $n/k+2$, when $k \mid n$ and $n/k \geqslant 3$. This improves the upper bound $b(\mathrm{PSL}(n, q)) \leqslant n/k + 3$ that was derived in [72, p. 24].

We are now able to complete the proof of Theorem 3.1.11 in the case $k \mid n$.

**Lemma 3.3.6.** *Suppose that $k \mid n$ and $1 < k < n/2$. If each element of $\Omega$ is a pair of nested subspaces of $V$ and $n/k = 3$, then $b(H, \Omega) \leqslant 4$. Otherwise, $b(H, \Omega) \leqslant n/k$.*

*Proof.* Let $X_i$, $R$ and $W$ be the subspaces of $V$ from Definition 3.3.2. We split the proof into four cases, depending on the type of $\Omega$ and whether or not $n/k = 3$.

**Case (a)**: Each element of $\Omega$ is a pair of nested subspaces of $V$, and $n/k = 3$. Let

$$\mathcal{K} := \{\{X_0, \langle X_0, R\rangle\}, \{X_1, \langle X_1, R\rangle\}, \{X_2, \langle X_2, W\rangle\}, \{W, \langle X_2, W\rangle\}\}.$$

We deduce from Proposition 3.3.4 that $\mathcal{K} \subset \Omega$, and that $\langle X_0, R\rangle \cap \langle X_1, R\rangle = (X_0 \oplus R) \cap (X_1 \oplus R) = R$. Hence $G_{(\mathcal{K})} \leqslant G_{(X_0,X_1,X_2,R,W)}$, which is trivial by Lemma 3.3.5(i). Moreover, no element of $H \setminus G$ maps $\langle X_2, W\rangle$ to both $X_2$ and $W$, and thus $\mathcal{K}$ is a base for $H$.

**Case (b)**: Each element of $\Omega$ is a pair of complementary subspaces of $V$, and $n/k = 3$. For each $j \in \{0, 1, 2\}$, let $Y_j := \langle X_i \mid i \neq j\rangle$. Then

$$\mathcal{L} := \{\{R, Y_0\}, \{R, Y_1\}, \{W, Y_2\}\}$$

is a subset of $\Omega$ by Proposition 3.3.4. Additionally, $\{Y_0 \cap Y_1, Y_0 \cap Y_2, Y_1 \cap Y_2\} = \{X_2, X_1, X_0\}$. Hence $G_{(\mathcal{L})} \leqslant G_{(X_0,X_1,X_2,R,W)} = 1$. As no element of $H \setminus G$ maps $R$ to both $Y_0$ and $Y_1$, we deduce that $\mathcal{L}$ is a base for $H$.

**Case (c)**: Each element of $\Omega$ is a pair of nested subspaces of $V$, and $n/k > 3$. For each $j \in \{0, \ldots, n/k - 4\}$, let $Y_j$ be the sum of $W$ and $\langle X_i \mid i \notin \{j+1, j+2\}\rangle$. Additionally, let $Y_{n/k-3}$ be the sum of $W$ and $\langle X_i \mid i \notin \{0, n/k-2\}\rangle$. Proposition 3.3.4 shows that each of these sums is direct, and hence $\bigcap_{j=0}^{n/k-3} Y_j = W \oplus X_{n/k-1}$. We also let $Y_{n/k-2} := \langle X_i \mid i \neq 0\rangle$, so that $\bigcap_{j=0}^{n/k-2} Y_j = X_{n/k-1}$. Finally, let $U$ be an $(n-k)$-dimensional subspace of $V$ that contains $R$ and $X_{n/k-1}$. Then the subset

$$\mathcal{M} := \{\{X_0, Y_0\}, \{X_1, Y_1\}, \ldots, \{X_{n/k-2}, Y_{n/k-2}\}, \{R, U\}\}$$

of $\Omega$ of size $n/k$ satisfies $G_{(\mathcal{M})} \leqslant G_{(X_0,X_1,\ldots,X_{n/k-1},R,\langle X_{n/k-1},W\rangle)}$, which Lemma 3.3.5(ii) shows is trivial. As $\langle X_0, X_1, \ldots, X_{n/k-2}, R\rangle = V$ while $\bigcap_{j=0}^{n/k-2} Y_j \cap U = X_{n/k-1}$, Lemma 3.3.1 implies that no element of $H \setminus G$ stabilises $\mathcal{M}$ pointwise. Thus $\mathcal{M}$ is a base for $H$.

**Case (d)**: Each element of $\Omega$ is a pair of complementary subspaces of $V$, and $n/k > 3$. For each $j \in \{0, \ldots, n/k - 3\}$, let $Y_j := \langle W, X_i \mid i \notin \{j, j+1\}\rangle$. Additionally, let $Y_{n/k-2} := \langle X_i \mid i \neq n/k - 2\rangle$. Then Proposition 3.3.4 shows that

$$\mathcal{N} := \{\{X_0, Y_0\}, \{X_1, Y_1\}, \ldots, \{X_{n/k-2}, Y_{n/k-2}\}, \{R, Y_{n/k-2}\}\}$$

is a subset of $\Omega$ of size $n/k$. This proposition also yields $\bigcap_{j=0}^{n/k-3} Y_j = \langle X_{n/k-1}, W\rangle$ and $\bigcap_{j=0}^{n/k-2} Y_j = X_{n/k-1}$. Thus $G_{(\mathcal{N})} \leqslant G_{(X_0,X_1,\ldots,X_{n/k-1},R,\langle X_{n/k-1},W\rangle)} = 1$. Finally, no element of $H \setminus G$ maps $Y_{n/k-2}$ to both $X_{n/k-2}$ and $R$, and so $\mathcal{N}$ is a base for $H$. □

Table 3.3.2 lists the base sizes $b(H, \Omega)$ for several small values of $n$ and $q$, with $n$ even and $k = 2$, again computed using the Magma code in `base_size_linear`. Observe that the upper bounds for $b(H, \Omega)$ from Lemma 3.3.6 are tight. However, in the nested case where the pair $(n, q)$ is equal to $(6, 2)$, the corresponding upper bound of 4 is not achieved. The actions here are again primitive by the tables in [17, §8.2].

Table 3.3.2: The base size of $H = \langle \mathrm{PGL}(n, q), \theta \rangle$ acting primitively on a set $\Omega$ of complementary or nested pairs of subspaces $\{X, Y\}$ of $\mathbb{F}_q^n$, with $2 = \dim(X) < \dim(Y)$ and $n$ even. Here, $\Delta$ denotes the difference between the upper bound for the base size given in Lemma 3.3.6 and the actual base size.

| $(n, q)$ | Pair type | $b(H, \Omega)$ | $\Delta$ |
|---|---|---|---|
| $(6, 2), (6, 3)$ | Complementary | 3 | 0 |
| $(6, 2)$ | Nested | 3 | 1 |
| $(6, 3)$ | Nested | 4 | 0 |
| $(8, 2)$ | Nested | 4 | 0 |

Finally, we consider the case $k \nmid n$. We begin by defining subspaces of $V$, some of which are analogous to those in Definition 3.3.2. In particular, the subspaces $R_1$ and $W_1$ defined below are analogous to (but distinct from) the subspaces $R$ and $W$ defined above. Recall Definition 2.5.1, of a companion matrix, and note that there exists a monic irreducible polynomial over $\mathbb{F}_q$ of degree $k$ [93, Corollary 2.11]. Additionally, $n \bmod k = n - (\lceil n/k \rceil - 1)k$.

**Definition 3.3.7.** Suppose that $k \nmid n$, let $t := \lceil n/k \rceil$, and let

$$X_i := \langle e_{1+ik}, e_{2+ik}, \ldots, e_{k+ik} \rangle$$

for each $i \in \{0, 1, \ldots, t-2\}$. Additionally, let

$$R_1 := \langle e_j + e_{j+k} + \cdots + e_{j+(t-2)k} \mid j \in \{1, 2, \ldots, k\} \rangle$$

and

$$J := \langle e_{j+k} + e_{j+2k} \mid j \in \{1, 2, \ldots, n-2k\} \rangle.$$

Next, let $s_j := e_{j+(t-1)k}$ for each $j \in \{1, 2, \ldots, n \bmod k\}$, and let $s_{n \bmod k+m} := e_m$ for each $m \in \{1, \ldots, k - n \bmod k\}$. We then define

$$S := \langle s_1, s_2, \ldots, s_k \rangle$$

and

$$T := \langle s_1, s_2, \ldots, s_{n \bmod k} \rangle.$$

Finally, let $u$ be the companion matrix of a monic irreducible polynomial over $\mathbb{F}_q$ of degree $k$. If $t = 3$, then we consider $u$ as an element of $\mathrm{GL}(X_1)$ and define

$$L := \langle e_j + (e_{j+k})^u \mid j \in \{1, 2, \ldots, k\} \rangle.$$

If instead $t > 3$, then we consider $u$ as an element of $\mathrm{GL}(X_2)$ and define

$$W_1 := \langle e_{j+k} + (e_{j+2k})^u + e_{j+3k} + \ldots + e_{j+(t-2)k} + s_j \mid j \in \{1, 2, \ldots, k\} \rangle.$$

Note that $T$ in the definition above is spanned by the final $n \bmod k$ vectors in $\{e_1, e_2, \ldots, e_n\}$.

Our next result is an analogue of Lemma 3.3.5 in the case $k \nmid n$. Again note that not all subspaces in the given stabilised sets are equidimensional. Additionally, the following result holds even if the (monic) polynomial associated with the matrix $u$ from Definition 3.3.7 is reducible over $\mathbb{F}_q$.

**Lemma 3.3.8.** *Suppose that $k \nmid n$, let $t := \lceil n/k \rceil$, and let $X_i$, $T$, $R_1$, $J$, $L$ and $W_1$ be the subspaces of $V$ from Definition 3.3.7.*

(i) *Suppose that $t = 3$. Then $G_{(X_0, X_1, T, R_1, J, L)} = 1$.*

(ii) *Suppose that $t > 3$. Then $G_{(X_0, X_1, \ldots, X_{t-3}, T, R_1, \langle X_{t-2}, T \rangle, W_1)} = 1$.*

*Proof.*

(i) Let $g \in G_{(X_0, X_1, T, R_1, J)}$. Note that $R_1$ is the standard diagonal subspace of $X_0 \oplus X_1$, while $J$ is the standard diagonal subspace of the direct sum of $T$ and the subspace of $V$ spanned by the first $\dim(T) = n - 2k$ vectors of $X_1$. Hence $g$ is a block matrix

$$\begin{pmatrix} A & 0 & 0 & 0 & 0 \\ C & B & 0 & 0 & 0 \\ 0 & 0 & A & 0 & 0 \\ 0 & 0 & C & B & 0 \\ 0 & 0 & 0 & 0 & A \end{pmatrix},$$

where $A \in \mathrm{GL}(n - 2k, q)$, $B \in \mathrm{GL}(3k - n, q)$, and $C$ is a $(3k - n) \times (n - 2k)$ matrix. We will write $K$ to denote the upper-left $k \times k$ block of $g$, i.e., $K = \begin{pmatrix} A & 0 \\ C & B \end{pmatrix}$. Additionally, let $\theta$ be the isomorphism from $X_0$ to $X_1$ that maps $e_j$ to $e_{j+k}$ for each $j \in \{1, 2, \ldots, k\}$. With a slight abuse of notation, we can consider $K$ as an element of both $\mathrm{GL}(X_0)$ and $\mathrm{GL}(X_1)$, so that $v^{K\theta} = v^{\theta K}$ for each $v \in X_0$.

Assume now that $g$ also stabilises $L$, and let $u$ be as in Definition 3.3.7. In addition, let $h \in L$, and let $h_0$ and $h_1$ be the projections of $h$ onto $X_0$ and $X_1$, respectively. Similarly, let $z := h^g$, and let $z_0$ and $z_1$ be the projections of $z$ onto $X_0$ and $X_1$, respectively. Then $z_0 = h_0^K$ and $z_1 = h_1^K$. It follows from the definition of $L$ that $h_0^{\theta uK} = h_1^K = z_1 = z_0^{\theta u} = h_0^{K\theta u} = h_0^{\theta Ku}$. As this holds for each $h_0 \in X_0$, we deduce that $[K, u] = 1$, and Proposition 2.5.3 implies that $K$ is a scalar matrix. Hence $g$ itself is a scalar matrix, and so $G_{(X_0,X_1,T,R_1,J,L)} = 1$.

(ii) Let $g \in G_{(X_0,X_1,\ldots,X_{t-3},T,R_1,\langle X_{t-2},T\rangle)}$. Then $g$ is equal to a block diagonal matrix $\mathrm{diag}(K_0, K_1, \ldots, K_{t-2}, N)$, with each $K_i$ a matrix in $\mathrm{GL}(k, q)$ and $N \in \mathrm{GL}(n \bmod k, q)$. In particular, the block to the right of $K_{t-2}$ is a zero matrix since $g$ stabilises $R_1$, and all blocks to the left of $K_{t-2}$ are zero matrices since $g$ stabilises $\langle X_{t-2}, T\rangle$. Moreover, as $g$ stabilises $R_1$, we deduce that each $K_i$ is equal to a fixed matrix $K$. We have also shown that $G_{(X_0,X_1,\ldots,X_{t-3},T,R_1,\langle X_{t-2},T\rangle)} = G_{(X_0,X_1,\ldots,X_{t-2},T,R_1)}$.

Assume now that $g$ also stabilises $W_1$, and let $u$ and $S$ be as in Definition 3.3.7. Additionally, let $w \in W_1$ and $z := w^g$, and for a subspace $U$ of $V$, let $w_U$ and $z_U$ be the projection of $w$ and $z$, respectively, onto $U$. Finally, let $\theta_1$ be the isomorphism from $S$ to $X_1$ that maps $s_j$ to $e_{j+k}$ for each $j \in \{1, 2, \ldots, k\}$. Observe from the definition of $W_1$ that the condition $w_S \in T$ is equivalent to each of $z_S \in T$, $w_{X_1} \in T^{\theta_1}$ and $z_{X_1} \in T^{\theta_1}$. Since $z_{X_1} = (w_{X_1})^g$, we deduce that $g$ stabilises $Y := T^{\theta_1} = \langle e_{1+k}, e_{2+k}, \ldots, e_{n \bmod k+k}\rangle$, and thus $K = K_1$ is a block matrix $\begin{pmatrix} D_1 & 0 \\ D_2 & D_3 \end{pmatrix}$, with $D_1 \in \mathrm{GL}(n \bmod k, q)$ and $D_3 \in \mathrm{GL}(k - n \bmod k, q)$. We observe that $(w_T)^{\theta_1 D_1} = (w_Y)^{D_1} = z_Y = (z_T)^{\theta_1} = (w_T)^{N\theta_1}$ for each $w_T \in T$, and it follows from the definition of $\theta_1$ that $D_1 = N$.

Next, let $\theta_2$ be the isomorphism from $X_1$ to $X_2$ that maps $e_{j+k}$ to $e_{j+2k}$ for each $j \in \{1, 2, \ldots, k\}$. Then $(w_{X_1})^{K\theta_2} = (w_{X_1})^{\theta_2 K}$ (with $K$ considered as an element of both $\mathrm{GL}(X_1)$ and $\mathrm{GL}(X_2)$). It follows from the definition of $W_1$ that $(w_{X_1})^{\theta_2 uK} = (w_{X_2})^K = z_{X_2} = (z_{X_1})^{\theta_2 u} = (w_{X_1})^{K\theta_2 u} = (w_{X_1})^{\theta_2 Ku}$. This holds for each $w_1 \in X_1$, and so $[K, u] = 1$. Hence Proposition 2.5.3 implies that $K$ is a scalar matrix. As $D_1 = N$, we conclude that $g$ is a scalar matrix, and therefore $G_{(X_0,X_1,\ldots,X_{t-3},T,R_1,\langle X_{t-2},T\rangle,W_1)} = 1$. □

We can now determine an upper bound for $b(H, \Omega)$ when $k \nmid n$.

**Lemma 3.3.9.** *Suppose that $k \nmid n$. If each element of $\Omega$ is a pair of nested subspaces of $V$ and $\lceil n/k \rceil = 3$, then $b(H, \Omega) \leqslant 4$. Otherwise, $b(H, \Omega) \leqslant \lceil n/k \rceil$.*

*Proof.* Let $X_i$, $T$, $R_1$, $J$, $L$ and $W_1$ be the subspaces of $V$ from Definition 3.3.7. We again split the proof into four cases, depending on the type of $\Omega$ and whether or not $t := \lceil n/k \rceil$ is equal to 3.

**Case (a)**: Each element of $\Omega$ is a pair of nested subspaces of $V$, and $t = 3$. Let $M$ be an $(n-k)$-dimensional subspace of $V$ that contains $R_1$, and let $Y_0 := \langle X_0, T\rangle$ and $Y_1 := \langle X_1, T\rangle$. Since each nonzero vector in $L$ projects nontrivially onto $X_0$, while each vector in $J$ projects trivially onto $X_0$, the intersection $J \cap L$ is trivial. Thus $F := \langle L, J\rangle$ has dimension $n-k$. As $\dim(Y_0) = \dim(Y_1) = n-k$, it follows that

$$\mathcal{K} := \{\{X_0, Y_0\}, \{X_1, Y_1\}, \{L, F\}, \{R_1, M\}\}$$

is a subset of $\Omega$. Moreover, $Y_1$ contains $J$, and each vector in $F \setminus J$ projects nontrivially onto $X_0$. Hence $Y_1 \cap F = J$. In addition, $Y_0 \cap Y_1 = T$. Therefore, $G_{(\mathcal{K})} \leqslant G_{(X_0,X_1,T,R_1,J,L)}$, which is trivial by Lemma 3.3.8(i). Finally, $\langle X_0, X_1, L, R_1\rangle = \langle X_0, X_1\rangle$, which is a proper subspace of $V$. However, $Y_0 \cap Y_1 \cap F \cap M \subseteq T \cap F$, which is trivial, as each nonzero vector in $F$ projects nontrivially onto either $X_0$ or $X_1$. It follows from Lemma 3.3.1 that $\mathcal{K}$ is a base for $H$.

**Case (b)**: Each element of $\Omega$ is a pair of complementary subspaces of $V$, and $t = 3$. Let $Y_0 := \langle X_1, T\rangle$, $F := \langle L, J\rangle$ and $A := \langle L, T\rangle$. We claim that

$$\mathcal{L} := \{\{X_0, Y_0\}, \{X_1, F\}, \{R_1, A\}\}$$

is a subset of $\Omega$. As in the previous case, $\dim(F) = n-k$, and it is clear that $\dim(A) = n-k$ and $\{X_0, Y_0\} \in \Omega$. Moreover, each nonzero vector in $F$ projects nontrivially onto $X_0$ or $T$, and so $\{X_1, F\} \in \Omega$. Suppose for a contradiction that $R_1 \cap A$ contains a nonzero vector $v$. Then $v \in L$, since no vector in $R_1$ projects nontrivially onto $T$. It follows from the definitions of $R_1$ and $L$ that there exists a nonzero vector $w \in X_1$ such that $w = w^u$, where $u \in \mathrm{GL}(X_1)$ is as in Definition 3.3.7. Since $u$ is the companion matrix of an irreducible polynomial over $\mathbb{F}_q$, Theorem 2.5.2 and Proposition 2.5.4 imply that $\langle u\rangle$ acts irreducibly on $X_1$. As $k > 1$, this contradicts the requirement that $u$ fixes a nonzero vector in $X_1$. Hence $\{R_1, A\} \in \Omega$, proving the claim.

Now, let $\theta$ be the isomorphism from $X_0$ to $X_1$ that maps $e_j$ to $e_{j+k}$ for each $j \in \{1, 2, \ldots, k\}$, and let $\phi$ be the monomorphism from $T$ to $X_1$ that maps $e_{j+2k}$ to $e_{j+k}$ for each $j \in \{1, 2, \ldots, n-2k\}$. Additionally, let $f \in F \cap A$. Using the definitions of $L$, $J$ and $T$, we deduce that there exist $a, b \in X_0$ and $s, t \in T$ such that

$$a + a^{\theta u} + s + s^{\phi} = f = b + b^{\theta u} + t.$$

Projecting onto $X_0$, $X_1$ and $T$, we observe that $a = b$, $a^{\theta u} + s^{\phi} = b^{\theta u}$ and $s = t$. Hence $s^{\phi} = 0$, and so $s = t = 0$. Thus $F \cap A = L$. Notice also that $Y_0 \cap F = J$ and $Y_0 \cap A = T$. Therefore, $G_{(\mathcal{L})} \leqslant G_{(X_0,X_1,T,R_1,J,L)} = 1$, and $Y_0 \cap F \cap A = \{0\}$. Since $\langle X_0, X_1, R_1\rangle = \langle X_0, X_1\rangle$ is a proper subset of $V$, it follows from Lemma 3.3.1 that $\mathcal{L}$ is a base for $H$.

**Case (c)**: Each element of $\Omega$ is a pair of nested subspaces of $V$, and $t > 3$. For each $j \in \{0, 1, \ldots, t-4\}$, let $Y_j := \langle X_i, T \mid i \neq j+1\rangle$, and let $Y_{t-3} := \langle X_i, T \mid i \neq 0\rangle$. In addition, let $A_1 := \langle X_i, R_1, T \mid i \notin \{0, t-2\}\rangle$, and let $A_2$ be an $(n-k)$-dimensional subspace of $V$ that contains $W_1$ and $T$. Note that $\dim(A_1) = n-k$, as each nonzero vector in $R_1$ projects nontrivially onto $X_0$. Thus

$$\mathcal{M} := \{\{X_0, Y_0\}, \{X_1, Y_1\}, \ldots, \{X_{t-3}, Y_{t-3}\}, \{R_1, A_1\}, \{W_1, A_2\}\}$$

is a subset of $\Omega$ of size $t$. We also see that $\bigcap_{j=0}^{t-3} Y_j = \langle X_{t-2}, T\rangle$ and $\bigcap_{j=0}^{t-3} Y_j \cap A_1 = T$. Hence $G_{(\mathcal{M})} \leqslant G_{(X_0,X_1,\ldots,X_{t-3},T,R_1,\langle X_{t-2},T\rangle,W_1)}$, which is trivial by Lemma 3.3.8(ii). In fact, since $\bigcap_{j=0}^{t-3} Y_j \cap A_1 \cap A_2 = T$, while $\langle X_0, X_1, \ldots, X_{t-3}, R_1, W_1\rangle = V$, Lemma 3.3.1 implies that $\mathcal{M}$ is a base for $H$.

**Case (d)**: Each element of $\Omega$ is a pair of complementary subspaces of $V$, and $t > 3$. For each $j \in \{0, 1, \ldots, t-2\}$, let $Y_j := \langle X_i, T \mid i \neq j\rangle$. Observe that each vector in $W_1$ that projects nontrivially onto $T$ also projects nontrivially onto $X_1$. Hence $W_1 \cap T = \{0\}$, and so there exists an $(n-k)$-dimensional subspace $A$ of $V$ that contains $T$ and intersects trivially with $W_1$. Additionally, each nonzero vector in $R_1$ projects nontrivially onto $X_{t-2}$. Thus

$$\mathcal{N} := \{\{X_0, Y_0\}, \{X_1, Y_1\}, \ldots, \{X_{t-3}, Y_{t-3}\}, \{R_1, Y_{t-2}\}, \{W_1, A\}\}$$

is a subset of $\Omega$ of size $t$. Furthermore, since $\bigcap_{j=0}^{t-3} Y_j = \langle X_{t-2}, T\rangle$ and $\bigcap_{j=0}^{t-2} Y_j = T$, it follows that $G_{(\mathcal{N})} \leqslant G_{(X_0,X_1,\ldots,X_{t-3},T,R_1,\langle X_{t-2},T\rangle,W_1)} = 1$. As in Case (c), we conclude from Lemma 3.3.1 that $\mathcal{N}$ is a base for $H$. □

Theorem 3.1.11 now follows from Lemmas 3.3.3, 3.3.6 and 3.3.9.

We again use the Magma code in `base_size_linear` to calculate $b(H, \Omega)$ for certain values of $n$, $k$ and $q$. The results of these calculations are summarised in Table 3.3.3. Similarly to the case $k \mid n$, we see that the upper bounds given in Lemma 3.3.9 are tight, but not always achieved when $q = 2$. We also calculate using Magma that when the triple $(n, q, k)$ is equal to $(5, 4, 2)$, the base size of $H$ is equal to that of $\mathrm{Aut}(\mathrm{PSL}(n, q))$ in each of the nested and complementary cases. As above, the actions described here are primitive by the tables in [17, §8.2].

Table 3.3.3: The base size of $H = \langle \mathrm{PGL}(n,q), \theta \rangle$ acting primitively on a set $\Omega$ of complementary or nested pairs of subspaces $\{X, Y\}$ of $\mathbb{F}_q^n$, with $k = \dim(X) < \dim(Y)$ and $k \nmid n$. Here, $\Delta$ denotes the difference between the upper bound for the base size given in Lemma 3.3.9 and the actual base size.

| $n/k$ | $(n,q,k)$ | Pair type | $b(H)$ | $\Delta$ |
|---|---|---|---|---|
| 5/2 | $(5,2,2),(5,3,2),(5,4,2)$ | Complementary | 3 | 0 |
| 5/2 | $(5,2,2)$ | Nested | 3 | 1 |
| 5/2 | $(5,3,2),(5,4,2)$ | Nested | 4 | 0 |
| 7/2 | $(7,2,2)$ | Either | 3 | 1 |
| 7/2 | $(7,3,2)$ | Nested | 4 | 0 |
| 7/3 | $(7,2,3),(7,3,3)$ | Nested | 4 | 0 |

## 3.4 Symplectic groups

Let $G$ be equal to $\mathrm{PSp}(n,q)$ or its derived subgroup, with $n$ and $q$ such that the derived subgroup of $G$ is simple. Thus if $G$ is not simple, then $G = \mathrm{PSp}(4,2)$. Additionally, let $V := \mathbb{F}_q^n$ be the natural module for $G$, so that $V$ is a non-degenerate symplectic space. In this section, we prove the symplectic case of Theorem 3.1.9, associated with the primitive action of an almost simple group with socle $G$ on a set $\Omega$ of subspaces of $V$. As mentioned below the statement of this theorem, we do not need to consider the base size of any group properly containing $\mathrm{PSp}(n,q)$, as the base size of any such group is no smaller than that of $\mathrm{PSp}(n,q)$. By Proposition 3.1.4, we may also assume that the dimension $k$ of each subspace in $\Omega$ is at most $n/2$, with $k < n/2$ when the subspaces are non-degenerate.

First recall from Lemma 2.2.9(ii) that each non-degenerate subspace of $V$ has even dimension. In particular, any one-dimensional subspace of $V$ is its own radical, and is therefore totally singular. Since $\mathrm{Sp}(2,q) = \mathrm{SL}(2,q)$ for all $q$, each symplectic subspace action in the case $n = 2$ is an action on the set of all one-dimensional subspaces of $\mathbb{F}_q^2$. As $q \neq 2$, Proposition 3.2.2 shows that $b(G) = n + 1 = 3$, which is greater than the lower bound of $n = 2$ required by Theorem 3.1.9(ii). Hence to complete the proof of Theorem 3.1.9(ii), we may assume that $n \geqslant 4$.

Suppose now that $G = \mathrm{PSp}(4,2)'$. We must consider the action of $G$ on the set of (totally singular) one-dimensional subspaces of $V$, and the action of $G$ on the set of totally singular two-dimensional subspaces of $V$. Using the Magma code in `base_size_s_u_o`, we deduce the following.

**Proposition 3.4.1.** *Suppose that $G = \mathrm{PSp}(4,2)'$, and let $\Omega$ be the set of totally singular $k$-dimensional subspaces of $V$, with $k \in \{1,2\}$. Then $b(G,\Omega) = 3$.*

For the remainder of this section, we may assume that $G = \mathrm{PSp}(n, q)$, with $n \geqslant 4$. We will prove the following result, which is more general than Theorem 3.1.9(ii).

**Theorem 3.4.2.** *Suppose that $G = \mathrm{PSp}(n, q)$, with $n \geqslant 4$. Additionally, let $k$ be a positive integer less than $n$, and let $\Delta$ be a set of $k$-dimensional subspaces of $V$, with $|\Delta| < \lceil n/k \rceil$. Then $G_{(\Delta)} \neq 1$.*

Note that the above result does not assume primitivity, or even transitivity, of an action of $G$ on any set of subspaces of $V$ containing $\Delta$. Indeed, $\Delta$ may be a combination of non-degenerate, totally singular and other $k$-dimensional subspaces of $V$. In addition, Theorem 3.4.2 is analogous to statements in the proof of Proposition 4.3 and above Lemma 4.6 in [27], regarding symplectic algebraic groups. The second of these statements is also an analogue of the following lemma, which is the key ingredient in the proof of Theorem 3.4.2. Recall Definition 3.2.1, of the matrices $I_m$ and $E_{i,j}$.

**Lemma 3.4.3.** *Let $W$ be an $(n-1)$-dimensional subspace of $V$. Then $\mathrm{Sp}(n, q)$ contains a non-scalar matrix that acts trivially on $W$.*

*Proof.* Let $\{e_1, \ldots, e_n\}$ be the basis for $V$ corresponding to the non-degenerate symplectic form given in Proposition 2.2.11. Since $V$ is non-degenerate, $W^\perp$ is a one-dimensional subspace of $V$ by Lemma 2.2.2, and (using Lemma 2.2.9(ii)) is therefore totally singular. Furthermore, we deduce from Witt's Lemma (see also Proposition 3.1.6) that $\mathrm{Sp}(n, q)$ acts transitively on the set of one-dimensional (totally singular) subspaces of $V$. As $(W^\perp)^\perp = W$ by Lemma 2.2.2, Lemma 2.2.7 shows that $\mathrm{Sp}(n, q)$ acts transitively on the set of $(n-1)$-dimensional subspaces of $V$. Hence we may assume that $W = \langle e_1, e_2, \ldots, e_{n-1} \rangle$. We now observe, using Lemma 2.2.6, that the non-scalar matrix $I_n + E_{n,1}$ lies in $\mathrm{Sp}(n, q)$ and acts trivially on $W$. □

*Proof of Theorem 3.4.2.* Notice that $\langle \Delta \rangle$ is a subspace of an $(n-1)$-dimensional subspace $W$ of $V$. By Lemma 3.4.3, $\mathrm{Sp}(n, q)$ contains a non-scalar matrix $A$ that acts trivially on $W$, and hence on $\langle \Delta \rangle$. The image of $A$ in $G$ lies in $G_{(\Delta)} \setminus \{1\}$, completing the proof. □

Hence we have proved the symplectic case of Theorem 3.1.9 (see Remark 3.1.10).

Now, let $\Omega$ be a set of totally singular or non-degenerate $k$-dimensional subspaces of $V$, such that $G = \mathrm{PSp}(n, q)$ acts primitively on $\Omega$. Then by Proposition 3.1.6, $\Omega$ is equal to the full set of subspaces of $V$ of the given type. We will compare the lower bound of $\lceil n/k \rceil$ for $b(G, \Omega)$ from Theorem 3.1.9(ii) with known bounds for this

base size in the algebraic and finite cases, and with computational examples. First, [27, Theorem 4(ii)] gives the base size of the corresponding action of a symplectic algebraic group defined over the algebraic closure of a finite field. Namely, if this base size is not equal to $\lceil n/k \rceil$, then the base size is equal to 4, and either $k = n/2$, or the pair $(n, k)$ is equal to $(6, 2)$.

For the finite symplectic group $G$, [72, p. 26, p. 28] gives an upper bound of $n/k+11$ for $b(G, \Omega)$ when the $k$-dimensional subspaces in $\Omega$ are non-degenerate, and an upper bound of $n/k + 10$ when the subspaces are totally singular. Additionally, [113, Lemma 3, Lemma 5, Lemma 9] gives improved upper bounds when $k \leqslant 2$. Namely, if $k = 1$, then $b(G, \Omega) \leqslant n$, and if $k = 2$, then $b(G, \Omega)$ is at most 4 if $n \leqslant 6$ (as in the algebraic case), and at most $\lceil n/2 \rceil$ if $n \geqslant 8$. Notice that, excluding the cases where $k = 2$ and $n \leqslant 6$, these improved upper bounds are equal to the lower bounds from Theorem 3.1.9(ii). Therefore, we deduce the following.

**Proposition 3.4.4.** *Let $k \in \{1, 2\}$, and suppose that $n \geqslant 4$, with $n \geqslant 8$ if $k = 2$. Additionally, let $\Omega$ be a set of $k$-dimensional subspaces of $V$, such that the action $(\mathrm{PSp}(n, q), \Omega)$ is primitive. Then $b(\mathrm{PSp}(n, q), \Omega) = \lceil n/k \rceil$.*

Table 3.4.1 lists several examples for $b(G, \Omega)$, with each subspace in $\Omega$ totally singular, calculated using the Magma code in `base_size_s_u_o`. In the case where each subspace in $\Omega$ is instead a non-degenerate two-dimensional subspace of $V$, we can use this code to show that $b(G, \Omega) = 3$ when $n = 6$ and $q \in \{2, 3\}$; and $b(G, \Omega) = 4$ when the pair $(n, q)$ lies in the set $\{(6, 4), (6, 5), (8, 2)\}$. By the tables in [17, §8.2], each action mentioned here is primitive.

Our computed base sizes agree with those in the algebraic case, except for certain examples where $n = 6$ and $q \in \{2, 3\}$, and the examples where $n = 8$ and $q \in \{3, 4\}$. We also see that the upper bounds given by [113] in the case $k = 2$ and $n \leqslant 6$ are tight, but are not always achieved. In general, we observe that the lower bound of $\lceil n/k \rceil$ from Theorem 3.1.9(ii) is tight, even when $k > 2$, as in the cases where $n = 8$, $q = 2$ and $k \in \{3, 4\}$. However, it may be possible to improve this bound in certain cases, in particular those corresponding to the exceptional cases for symplectic algebraic groups. It also seems reasonable to conjecture that the general upper bounds given by [72] could be significantly improved.

## 3.5 Unitary groups

Let $G := \mathrm{PSU}(n, q)$, with $n$ and $q$ such that $G$ is simple. Additionally, let $H := \mathrm{PGU}(n, q)$, and let $V := \mathbb{F}_{q^2}^n$ be the natural module for $G$, so that $V$ is a non-degenerate unitary space. This section serves as a proof of the unitary case of

Table 3.4.1: The base size of $\mathrm{PSp}(n,q)$ acting primitively on the set $\Omega$ of $k$-dimensional totally singular subspaces of $\mathbb{F}_q^n$. Here, $r$ denotes any prime power between 2 and 19, inclusive.

| $n/k$ | $(n,q,k)$ | $b(\mathrm{PSp}(n,q),\Omega)$ |
|---|---|---|
| 2 | $(4,r,2),(6,2,3),(6,3,3),(6,4,3),(6,5,3),(8,2,4)$ | 4 |
| 8/3 | $(8,2,3)$ | 3 |
| 8/3 | $(8,3,3),(8,4,3)$ | 4 |
| 3 | $(6,2,2),(6,3,2)$ | 3 |
| 3 | $(6,4,2),(6,5,2)$ | 4 |
| 4 | $(4,r,1),(8,2,2)$ | 4 |
| 6 | $(6,2,1),(6,3,1),(6,4,1),(6,5,1)$ | 6 |
| 8 | $(8,2,1)$ | 8 |

Theorem 3.1.9, associated with the primitive action of an almost simple group with socle $G$ on a set $\Omega$ of subspaces of $V$. As in the symplectic case, we may assume by Proposition 3.1.4 that each subspace in $\Omega$ has dimension $k \leqslant n/2$, with $k < n/2$ when the subspaces are non-degenerate.

Recall that when $n = 2$, the group $G$ is isomorphic to $\mathrm{PSL}(2,q)$. Additionally, in this case, the only relevant action of $G$ is the action on one-dimensional totally singular subspaces of $V$. In fact, this action is equivalent to the action of $\mathrm{PSL}(2,q)$ on one-dimensional subspaces of $\mathbb{F}_q^n$ (see [17, Table 2.3, Table 8.1]). Since $q \neq 2$, Proposition 3.2.2 shows that $b(G) = n+1 = 3$, which is greater than the lower bound of $n = 2$ required by Theorem 3.1.9(iii). Hence to complete the proof of Theorem 3.1.9(iii), it suffices to assume that $n \geqslant 3$. We will make this assumption for the remainder of this section.

Similarly to the symplectic case, we prove a theorem that is more general than Theorem 3.1.9(iii). This more general theorem will also be useful in Chapters 4 and 6.

**Theorem 3.5.1.** *Suppose that $n \geqslant 3$, let $k$ be a positive integer less than $n$, and let $\Delta$ be a set of $k$-dimensional subspaces of $V$.*

(i) *Suppose that $|\Delta| < \lceil n/k \rceil$. Then $H_{(\Delta)} \neq 1$. Moreover, if $(q+1) \nmid n$, or if $k \nmid (n-1)$, then $G_{(\Delta)} \neq 1$.*

(ii) *Suppose that $|\Delta| < \lceil n/k \rceil - 1$. Then $G_{(\Delta)} \neq 1$.*

Hence if $|\Delta| < \lceil \frac{n-1}{k} \rceil$, then $G_{(\Delta)} \neq 1$. The proof of this theorem follows the same general idea as the proof of Theorem 3.4.2, and again, we do not require $G$

to act transitively on any set of subspaces containing $\Delta$. However, the situation here is slightly more complicated, as $\mathrm{SU}(n,q)$ is in general a proper subgroup of the isometry group $\mathrm{GU}(n,q)$, and not all one-dimensional subspaces of $V$ are totally singular. Additionally, unlike the symplectic case above and the orthogonal case below, there is no analogue of the above theorem in the case of algebraic groups; indeed, there are no simple algebraic groups that are direct analogues of the finite unitary groups.

The following lemma is the main result used in the proof of Theorem 3.5.1. Recall that, with $m$ a positive integer, $I_m$ denotes the $m \times m$ identity matrix.

**Lemma 3.5.2.** *Let $W$ be an $(n-1)$-dimensional subspace of $V$. Then $\mathrm{GU}(n,q)$ contains a non-scalar matrix that acts trivially on $W$. Furthermore, $\mathrm{SU}(n,q)$ contains a non-scalar matrix that acts as a scalar on $W$ if and only if either $W^\perp$ is totally singular or $q+1$ does not divide $n$.*

*Proof.* By Proposition 2.2.10, we may assume that $I_n$ is the Gram matrix associated with $V$. Then Lemma 2.2.6 shows that a matrix $A \in \mathrm{GL}(n,q^2)$ lies in $\mathrm{GU}(n,q)$ if and only if $AA^{\sigma T} = I_n$, where $A^\sigma$ is the matrix obtained from $A$ by raising each entry to its $q$-th power.

As $V$ is non-degenerate, $\dim(W^\perp) = 1$ by Lemma 2.2.2. Therefore, if $W^\perp$ is degenerate, then it is totally singular. Witt's Lemma implies that $\mathrm{GU}(n,q)$ acts transitively on the set of non-degenerate one-dimensional subspaces of $V$, and also on the set of totally singular one-dimensional subspaces of $V$. By Proposition 3.1.6, the same is true for $\mathrm{SU}(n,q)$. Since $(W^\perp)^\perp = W$ by Lemma 2.2.2, it follows from Lemma 2.2.7 that it suffices to consider only two choices for $W$: any one choice with $W^\perp$ non-degenerate, and any one choice with $W^\perp$ totally singular. We split the proof into these two cases. In each case, let $\{e_1, \ldots, e_n\}$ be the basis for $V$ corresponding to the Gram matrix $I_n$, and let $\omega$ be a primitive element of $\mathbb{F}_{q^2}$.

**Case (a)**: $W^\perp$ is non-degenerate. We may assume that $W^\perp = \langle e_1 \rangle$, so that $W = \langle e_2, e_3, \ldots, e_n \rangle$. By Corollary 2.2.8, any matrix in $\mathrm{GU}(n,q)$ that acts as a scalar on $W$ also stabilises $W^\perp$. Hence any such matrix is equal to $B_{\alpha,\gamma} := \mathrm{diag}(\alpha, \gamma, \gamma, \ldots, \gamma)$ for some $\alpha, \gamma \in \mathbb{F}_{q^2}^\times$. Observe also that $B_{\alpha,\gamma} \in \mathrm{GU}(n,q)$ if and only if $\alpha^{q+1} = 1 = \gamma^{q+1}$.

Let $\lambda := \omega^{q-1}$. Then $|\lambda| = q+1 > 1$, and $B_{\lambda,1}$ is a non-scalar matrix in $\mathrm{GU}(n,q)$ that acts trivially on $W$. Notice that if $q+1$ does not divide $n$, then $\lambda^n \neq 1$, and so $(\lambda^{n-1})^{-1} \neq \lambda$. Hence in this case, $B_{(\lambda^{n-1})^{-1},\lambda}$ is a non-scalar matrix in $\mathrm{SU}(n,q)$ that acts as the scalar $\lambda$ on $W$. If instead $q+1$ *does* divide $n$, then any scalar $\alpha \in \mathbb{F}_{q^2}^\times$ satisfying $\alpha^{q+1} = 1$ also satisfies $\alpha^n = 1$, i.e., $(\alpha^{n-1})^{-1} = \alpha$. Therefore, in this case, no non-scalar matrix in $\mathrm{SU}(n,q)$ acts as a scalar on $W$.

**Case (b)**: $W^\perp$ is totally singular. If $q$ is even, then let $\gamma := \omega^{q+1}$ and $\delta := 1$, and otherwise, let $\gamma := \omega$ and $\delta := \omega^{(q-1)/2}$. Then, for all $q$,

$$\delta^{q+1} = -1, \tag{3.5.1}$$

and thus $(\delta e_1 + e_2, \delta e_1 + e_2) = 0$. Hence we may assume that $W^\perp = \langle \delta e_1 + e_2 \rangle$, so that $W = \langle \delta e_1 + e_2, e_3, \ldots, e_n \rangle$. Observe also that $\gamma^{q-1} = \delta^2$. Therefore,

$$\gamma^q = \gamma\delta^2, \tag{3.5.2}$$

and so (3.5.1) gives

$$(\gamma\delta)^q = \gamma\delta^{q+2} = -\gamma\delta. \tag{3.5.3}$$

Let $S$ be the direct sum of $C := \begin{pmatrix} 1+\gamma\delta & \gamma \\ -\gamma\delta^2 & 1-\gamma\delta \end{pmatrix}$ and $I_{n-2}$. Then $S$ acts trivially on $W$, $\det(S) = 1$, and (3.5.2) and (3.5.3) yield $C^{\sigma T} = \begin{pmatrix} 1-\gamma\delta & -\gamma \\ \gamma\delta^2 & 1+\gamma\delta \end{pmatrix}$. It is now easy to check that $SS^{\sigma T} = I_n$, and hence the non-scalar matrix $S$ lies in $\mathrm{SU}(n,q)$. □

**Corollary 3.5.3.** *Let $U$ be an $(n-2)$-dimensional subspace of $V$. Then $\mathrm{SU}(n,q)$ contains a non-scalar matrix that acts as a scalar on $U$.*

*Proof.* The subspace $U^\perp$ of $V$ is two-dimensional by Lemma 2.2.2. We claim that $U^\perp$ contains a totally singular one-dimensional subspace $X$. By [89, p. 22], this is indeed the case if $U^\perp$ is non-degenerate, and otherwise, each one-dimensional subspace of the radical of $U^\perp$ is totally singular. As $\dim(X^\perp) = n-1$ and $(X^\perp)^\perp = X$, again by Lemma 2.2.2, it follows from Lemma 3.5.2 that $\mathrm{SU}(n,q)$ contains a non-scalar matrix $A$ that acts as a scalar on $X^\perp$. Moreover, since $X \subseteq U^\perp$, Proposition 2.2.3 yields $U \subseteq X^\perp$. Therefore, $A$ acts as a scalar on $U$. □

*Proof of Theorem 3.5.1.* If $|\Delta| < \lceil n/k \rceil$, then $\langle \Delta \rangle$ lies in an $(n-1)$-dimensional subspace $W$ of $V$. Lemma 3.5.2 shows that if $K = \mathrm{GU}(n,q)$, or if $K = \mathrm{SU}(n,q)$ and $(q+1) \nmid n$, then $K$ contains a non-scalar matrix that acts as a scalar on $W$, and hence on $\langle \Delta \rangle$. Therefore, the pointwise stabiliser of $\Delta$ in the corresponding projective group ($H$ or $G$) is nontrivial.

It remains to show that $G_{(\Delta)} \neq 1$ when $|\Delta| < \lceil n/k \rceil - 1$, or when $|\Delta| = \lceil n/k \rceil - 1$ and $k \nmid (n-1)$. In each case, $\langle \Delta \rangle$ lies in an $(n-2)$-dimensional subspace $U$ of $V$. Corollary 3.5.3 shows that $\mathrm{SU}(n,q)$ contains a non-scalar matrix that acts as a scalar on $U$, and hence on $\langle \Delta \rangle$. Thus $G_{(\Delta)} \neq 1$. □

This completes the proof of the unitary case of Theorem 3.1.9 (see Remark 3.1.10).

As previously mentioned, there are no simple algebraic groups that are direct analogues of the finite unitary groups. However, we can compare the lower bounds for base sizes from Theorem 3.1.9(iii) with known upper bounds for finite groups. As in the symplectic case, [72, p. 26, p. 28] shows that $b(G,\Omega)$ is at most $n/k+11$ for the action of $G$ on non-degenerate $k$-dimensional subspaces of $V$, and at most $n/k+10$ for the action on totally singular $k$-dimensional subspaces. Moreover, there are tighter upper bounds known in the case $k \leqslant 2$, proved in [113, Lemma 3, Lemmas 5–6, Lemma 9]. If $k=1$, then $b(H,\Omega) \leqslant n$, and if $k=2$, then $b(H)$ is at most 5 if $n=4$, at most 4 if $n \in \{5,6\}$, and at most $\lceil n/2 \rceil$ if $n \geqslant 7$. Thus if $k=1$ and $n \geqslant 3$, or if $k=2$ and $n \geqslant 7$, then this upper bound is equal to our lower bound for $b(H,\Omega)$ from Theorem 3.1.9(iii). Additionally, since $H/G$ is cyclic [89, §2.3], we deduce from Lemma 3.1.8 (with $G$ in place of $H$ and vice versa) that $b(G) \leqslant b(H) \leqslant b(G)+1$, when $(H,\Omega)$ is primitive. Hence $b(G) \in \{b(H), b(H)-1\}$, and we obtain the following result.

**Proposition 3.5.4.** *Let $k \in \{1,2\}$, and suppose that $n \geqslant 3$ if $k=1$, or that $n \geqslant 7$ if $k=2$. Additionally, let $\Omega$ be a set of $k$-dimensional subspaces of $V$, such that the action $(\mathrm{PGU}(n,q),\Omega)$ is primitive. Then $b(\mathrm{PGU}(n,q),\Omega) = \lceil n/k \rceil$, and $\lceil n/k \rceil - 1 \leqslant b(\mathrm{PSU}(n,q),\Omega) \leqslant \lceil n/k \rceil$.*

We now consider several concrete examples of base sizes of unitary groups, computed using the Magma code in `base_size_s_u_o`. Table 3.5.1 lists base sizes for $G$ acting on the set $\Omega$ of $k$-dimensional totally singular subspaces of $V$, for certain values of $n$, $q$ and $k$. Among these examples, if either $n=q+1$, or $n=6$ and $q \neq k$, then $b(H,\Omega) = b(G,\Omega)+1$. In the remaining examples, $b(H,\Omega) = b(G,\Omega)$. In fact, for each triple $(n,q,k)$ represented in the table where $k < n/2$ and $(n,q,k) \neq (5,5,2)$, we compute $b(G,\Omega) = b(G,\Omega')$, where $\Omega'$ is the set of $k$-dimensional non-degenerate subspaces of $V$. In the case $(n,q,k)=(5,5,2)$, the degree of the action is too large to construct the corresponding permutation group in Magma. Excluding this large case, we also see that $b(H,\Omega) = b(H,\Omega')$, except when $(n,q,k) \in \{(5,4,2),(6,3,2)\}$, in which case $b(H,\Omega') = b(G,\Omega) = 3 = b(H,\Omega)-1$. Note that each action discussed here is primitive by the tables in [17, §8.2].

Comparing these examples with the lower bounds from Theorem 3.1.9(iii), we see that the lower bounds for $b(G)$ and $b(H)$ are achieved in the examples where the hypotheses of Proposition 3.5.4 are satisfied, and in certain other examples with $k=2$. However, these lower bounds are not always achieved. Thus although these bounds are tight in general, it may be possible to improve them in certain cases. As in the symplectic case, it also seems likely that the upper bounds given by [72] could

Table 3.5.1: The base size of $\mathrm{PSU}(n,q)$ acting primitively on a set $\Omega$ of $k$-dimensional totally singular subspaces of $\mathbb{F}_{q^2}^n$. Here, $r$ denotes any prime power between 3 and 13, inclusive.

| $n/k$ | $(n,q,k)$ | $b(\mathrm{PSU}(n,q),\Omega)$ |
|---|---|---|
| 2 | $(4,2,2),(4,3,2),(6,2,3)$ | 4 |
| 2 | $(4,4,2),(4,5,2),(4,7,2),(6,3,3)$ | 5 |
| 5/2 | $(5,4,2)$ | 3 |
| 5/2 | $(5,2,2),(5,3,2),(5,5,2)$ | 4 |
| 3 | $(3,r,1),(6,2,2),(6,3,2)$ | 3 |
| 4 | $(4,3,1)$ | 3 |
| 4 | $(4,2,1),(4,4,1),(4,5,1)$ | 4 |
| 5 | $(5,4,1)$ | 4 |
| 5 | $(5,2,1),(5,3,1)$ | 5 |
| 6 | $(6,2,1)$ | 5 |

be significantly reduced. Finally, the aforementioned exceptional upper bounds for $b(H)$ in the case $k=2$ and $n \leqslant 6$ are sometimes, but not always, achieved.

## 3.6 Orthogonal groups

Let $G := \mathrm{P}\Omega^{\varepsilon}(n,q)$, with $n$, $q$ and $\varepsilon \in \{\circ,+,-\}$ such that $G$ is simple. Then $n \geqslant 3$, with $q>3$ if $n=3$ and $\varepsilon=-$ if $n=4$. Additionally, let $H := \mathrm{PSO}^{\varepsilon}(n,q)$, and let $V := \mathbb{F}_q^n$ be the natural module for $G$, so that $V$ is a non-degenerate quadratic space. In this section, we will prove Theorem 3.1.9(iv), associated with the primitive action of an almost simple group with socle $G$ on a set of $k$-dimensional subspaces of $V$. This will complete the proof of Theorem 3.1.9. We may assume by Proposition 3.1.4 that $k \leqslant n/2$, and that if $k=n/2$, then either the action is on totally singular subspaces and $\varepsilon=+$; or the action is on non-degenerate subspaces, $\varepsilon=-$, and $4 \mid n$.

Theorem 3.1.9(iv) is a consequence of the following more general theorem, whose proof is the main focus of this section. For convenience, let $\mathcal{O}$ be the set of groups $\mathrm{P}\Omega^{\varepsilon}(n,q)$ such that $n$ is even, $q \leqslant 3$, and if $q=3$, then $4 \mid n$ if and only if $\varepsilon=+$. Additionally, $\delta_{1k}$ is the Kronecker delta.

**Theorem 3.6.1.** *Let $k$ be a positive integer less than $n$, and let $\Delta$ be a set of $k$-dimensional subspaces of $V$.*

(i) *Suppose that $|\Delta| < \lceil n/k \rceil$, with $|\Delta| < \lceil n/k \rceil - 1$ if $k \mid (n-1)$. Then $H_{(\Delta)} \neq 1$. Moreover, if $k \nmid (n-2)$, or if $G \notin \mathcal{O}$, then $G_{(\Delta)} \neq 1$.*

(ii) *If* $|\Delta| < \lceil n/k \rceil - 1 - \delta_{1k}$, *then* $G_{(\Delta)} \neq 1$.

Note that the hypothesis on $|\Delta|$ in the first part of the above theorem is precisely that $|\Delta| < \lceil \frac{n-1}{k} \rceil$. The proof of this theorem uses similar techniques to those in the proof of Theorem 3.5.1, but this orthogonal case is significantly more complicated. We still, however, do not require any assumptions regarding transitivity in the action of $G$ on a set of subspaces of $V$ containing $\Delta$.

In what follows, we write $Q$ to denote the non-degenerate quadratic form preserved by $\Omega^\varepsilon(n,q)$ and $\mathrm{SO}^\varepsilon(n,q)$. Recall that, for vectors $u, v \in V$, we write $(u,v)$ to denote the image of this pair of vectors under the polar form of $Q$.

**Proposition 3.6.2.** *Let $U$ be a two-dimensional subspace of $V$. Suppose also that $U$ is degenerate but not totally singular, and choose $u_1 \in U$ such that $Q(u_1) \neq 0$.*

(i) *There exists $u_2 \in U$ such that $\{u_1, u_2\}$ is a basis for $U$ and $Q(u_2) = (u_1, u_2) = 0$.*

(ii) *Let $H$ be the subgroup of $\mathbb{F}_q^\times$ consisting of squares. In addition, let $X$ be a two-dimensional subspace of $V$ that is degenerate but not totally singular, such that $X$ contains a vector $x$ with $HQ(x) = HQ(u_1)$. Suppose also that $\Omega^\varepsilon(n,q)$ contains a non-scalar matrix that acts as a scalar on $U^\perp$. Then $\Omega^\varepsilon(n,q)$ contains a non-scalar matrix that acts as the same scalar on $X^\perp$.*

*Proof.*

(i) Suppose first that $q$ is odd. Since $U$ is degenerate, its radical contains a nonzero vector $u_2$. In particular, $(u_2, u_2) = 0 = (u_1, u_2)$. As $q$ is odd, this implies that $Q(u_2) = 0$. Moreover, $u_1$ does not lie in the radical $\langle u_2 \rangle$ of $U$. Thus $\{u_1, u_2\}$ is a basis for $U$.

Next, suppose that $q$ is even. Then the polar form of $Q$ is symplectic, and hence its restriction to each one-dimensional subspace of $U$ is the zero form. As $U$ is degenerate, it follows that $U$ is totally isotropic. Thus, for any choice of $v \in U \setminus \langle u_1 \rangle$, the set $\{u_1, v\}$ is a basis for $U$, and $(u_1, v) = 0$. Hence if $Q(v) = 0$, then we can set $u_2 = v$. Otherwise, let $u_2 := u_1 + (Q(u_1)Q(v)^{-1})^{q/2} v$. Then $\{u_1, u_2\}$ is another basis for $U$, $(u_1, u_2) = 0$, and (2.2.1) yields

$$Q(u_2) = Q(u_1) + Q(u_1)Q(v)^{-1}Q(v) = 0.$$

(ii) Since $HQ(x) = HQ(u_1)$, there exists $\gamma \in \mathbb{F}_q^\times$ such that $Q(u_1) = \gamma^2 Q(x)$. Hence $Q(\gamma x) = Q(u_1)$ by (2.2.1). It follows from (i) that there exists an isometry from $U$ to $X$ that maps $u_1$ to $\gamma x$. By Witt's Lemma, this extends to

an isometry of $Q$, i.e., an element $g \in \mathrm{GO}^\varepsilon(n,q)$. In fact, Lemma 2.2.7 shows that $(U^\perp)^g = X^\perp$.

Now, let $A$ be a non-scalar matrix in $\Omega^\varepsilon(n,q)$ that acts as a scalar $z$ on $U^\perp$. Then $A^g$ is a non-scalar matrix that acts as $z$ on $X^\perp$, and that lies in the normal subgroup $\Omega^\varepsilon(n,q)$ of $\mathrm{GO}^\varepsilon(n,q)$. □

**Proposition 3.6.3.** *Let $X$ be a three-dimensional subspace of $V$. Then $X$ contains a degenerate two-dimensional subspace.*

*Proof.* If $X$ is degenerate, so that its radical $X \cap X^\perp$ is nonzero, then any two-dimensional subspace of $X$ that intersects $X^\perp$ nontrivially is degenerate. Suppose therefore that $X$ is non-degenerate. Then $X$ contains a totally singular one-dimensional subspace $U$ [89, Proposition 2.5.4(ii)], and we observe from Lemma 2.2.2 that the perpendicular space of $U$, with respect to $X$, is degenerate and two-dimensional. □

The following lemma is analogous to a statement in the proof of [27, Lemma 4.14], regarding special orthogonal algebraic groups. Here, the matrices $I_m$ and $E_{i,j}$ are as in Definition 3.2.1. Recall also from Proposition 2.3.2 that the centre of each of $\Omega^\varepsilon(n,q)$ and $\mathrm{SO}^\varepsilon(n,q)$ is equal to its subgroup of scalar matrices.

**Lemma 3.6.4.** *Let $W$ be an $(n-2)$-dimensional subspace of $V$. Then $\mathrm{SO}^\varepsilon(n,q)$ contains a non-scalar matrix that acts as a scalar on $W$. Furthermore, if $\Omega^\varepsilon(n,q)$ does not contain such a matrix, then $W^\perp$ is non-degenerate of plus type, and either:*

(i) *$q = 2$; or*

(ii) *$q = 3$, $n$ is even, and $n \equiv 1 - \varepsilon 1 \pmod 4$.*

*Proof.* Let $\hat{H} := \mathrm{SO}^\varepsilon(n,q)$ and $\hat{G} := \Omega^\varepsilon(n,q)$, and recall that $n \geqslant 3$. Assume first that $n = 3$, so that $q > 3$ and $\hat{G}$ is simple. Then $\dim(W) = 1$, and so any element of $\hat{G}$ that stabilises $W$ acts as a scalar on this subspace. Additionally, $W$ is either non-degenerate or totally singular. In either case, we deduce from [17, Table 8.7] (see also [17, Table 2.3]) that the stabiliser of $W$ in $\hat{G}$ is nontrivial[1]. As $\hat{G}$ is simple, it contains no scalar matrices, and the result follows.

Suppose for the rest of the proof that $n \geqslant 4$. We may assume that the matrices $M_Q$ and $M_{\beta_Q}$ associated with the form $Q$ and its polar form $\beta_Q$, respectively, are as

[1]The subspace stabiliser of shape $D_{q-1}$ is not included in [17, Table 8.7] when $q = 5$ as it is not maximal in $\hat{G}$ in this case, but it is of course still nontrivial.

in Proposition 2.2.12. Let $\{e_1, \dots, e_n\}$ be the basis for $V$ corresponding to $Q$. Additionally, let $\{w_1, w_2\}$ be a basis for the subspace $W^\perp$ of $V$, which is two-dimensional by Lemma 2.2.2.

Now, the subgroup of $\mathbb{F}_q^\times$ consisting of squares has index $(2, q-1)$ in $\mathbb{F}_q^\times$. Additionally, $(W^\perp)^\perp = W$ by Lemma 2.2.2. Hence Proposition 3.6.2 shows that, when considering subspaces $W$ with $W^\perp$ degenerate but not totally singular, it suffices to consider only $(2, q-1)$ choices for $W$, namely, one corresponding to each coset in $\mathbb{F}_q^\times$ of the subgroup of squares.

Similarly, since $(n, \varepsilon) \neq (4, +)$, Proposition 3.1.6 shows that $\hat{G}$ and $\hat{H}$ each act transitively on the set of totally singular two-dimensional subspaces of $V$; on the set of non-degenerate two-dimensional subspaces of $V$ of plus type; and on the set of non-degenerate two-dimensional subspaces of $V$ of minus type. Using Lemma 2.2.7 and the fact that $(W^\perp)^\perp = W$, we deduce that, along with the $(2, q-1)$ choices for $W$ from the previous paragraph, it suffices to consider only 3 additional choices for $W$: any one choice with $W^\perp$ totally singular, any one choice with $W^\perp$ non-degenerate of plus type, and any one choice with $W^\perp$ non-degenerate of minus type.

We split the proof into three cases, depending on whether $W^\perp$ is totally singular, non-degenerate, or neither. In each case, we show that there exists a matrix $D \in \hat{H} \setminus Z(\hat{H})$ that acts as a scalar on $W$. In fact, we choose $D \in \hat{G} \setminus Z(\hat{G})$, unless one of the exceptional cases listed in the statement of the theorem holds. Note that since $\hat{G}$ has index two in $\hat{H}$ (see §2.3.4), each square in $\hat{H}$ lies in $\hat{G}$, as does each product of two elements of $\hat{H} \setminus \hat{G}$. Note in particular that the lower unitriangular matrices (i.e., lower triangular matrices with all diagonal entries equal to 1) in $\mathrm{GL}(n, q)$ form a Sylow $p$-subgroup of $\mathrm{GL}(n, q)$, where $p$ is the prime dividing $q$ (see, e.g., [143, p. 454], though the matrices here are upper unitriangular). Thus when $q$ is odd, any lower unitriangular matrix $B \in \hat{H}$ has odd order and is therefore a square (one square root is $B^{(|B|+1)/2}$), and hence $B \in \hat{G}$.

Recall also from Lemma 2.2.6 that a matrix $A \in \mathrm{SL}(n, q)$ lies in $\hat{H}$ if and only if $AM_{\beta_Q}A^T = M_{\beta_Q}$ and each diagonal entry of $AM_QA^T$ is equal to the corresponding diagonal entry of $M_Q$. In addition, since $(n, \varepsilon) \neq (4, +)$, Proposition 2.3.7 shows that if $q$ is even, then a matrix $B \in \hat{H}$ lies in $\hat{G}$ if and only if $I_n + B$ has even rank.

**Case (a)**: $W^\perp$ is totally singular. As $V$ has no two-dimensional totally singular subspace when $(n, \varepsilon) = (4, -)$ [89, Proposition 2.5.4(i)], we may assume that $n \geqslant 5$. Here, $Q(w_1) = Q(w_2) = (w_1, w_2) = 0$. As $Q(e_1) = Q(e_2) = (e_1, e_2) = 0$, we may assume that $w_1 = e_1$ and $w_2 = e_2$. Then $W = \langle e_1, e_2, \dots, e_{n-2} \rangle$. Let $A := I_n + E_{n-1,1} - E_{n,2}$. It is easy to check that $A$ lies in $\hat{H} \setminus Z(\hat{H})$ and acts trivially on $W$. Moreover, $A$ is lower unitriangular, and if $q$ is even, then $I_n + A$ has rank 2.

Thus we can set $D = A$.

**Case (b)**: $W^\perp$ is non-degenerate. Let $H^*$ be the subgroup of $\hat{H}$ that stabilises $W^\perp$ and acts trivially on $W$, and let $G^* := H^* \cap \hat{G}$. As $V = W \oplus W^\perp$ by Lemma 2.2.2, we can choose $D$ to be any non-identity element of $G^*$, or of $H^*$ when one of the listed exceptions applies. By [89, Lemma 4.1.1], $G^* \cong \Omega^\nu(2,q)$ and $H^* \cong \mathrm{SO}^\nu(2,q)$, where $\nu \in \{+,-\}$ is the type of $W^\perp$. We deduce from [17, §1.6.4] that $H^*$ is always nontrivial, and that $G^*$ is nontrivial unless $\nu = +$ and $q \leqslant 3$. Thus it remains to show that there exists a suitable matrix $D \in \hat{G} \setminus Z(\hat{G})$ when $\nu = +$, $q = 3$, and (ii) does not hold.

By Proposition 2.2.12, we may assume that $Q(w_1) = Q(w_2) = 0$ and $(w_1, w_2) = 1$. As $Q(e_1) = Q(e_n) = 0$ and $(e_1, e_n) = 1$, we may also assume that $w_1 = e_1$ and $w_2 = e_n$. Then $W = \langle e_2, e_3, \ldots, e_{n-1} \rangle$. Assume first that $n$ is odd, let $B$ be the matrix obtained from $-I_n$ by swapping its first row and last row, and let $C := B - E_{1,n} - E_{n,1}$. Then $B$, $C$ and $BC$ act as scalars on $W$ and lie in $\hat{H} \setminus Z(\hat{H})$, and so at least one of these matrices lies in $\hat{G} \setminus Z(\hat{G})$. We can therefore set $D$ to be such a matrix.

Next, if $n \equiv 2 \pmod 4$ and $\varepsilon = +$, then $\hat{H}$ contains the block diagonal matrix $S := \mathrm{diag}(I_1, X_1, X_2, \ldots, X_{(n-2)/4}, Y_1, Y_2, \ldots, Y_{(n-2)/4}, I_1)$, where $X_i := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $Y_i := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ for each $i$. Furthermore, $S^2 = \mathrm{diag}(1, -1, -1, \ldots, -1, 1)$ acts as the scalar $-1$ on each vector in $W$. Thus we can set $D = S^2$.

Suppose finally that $n \equiv 0 \pmod 4$ and $\varepsilon = -$. As the polynomial $x^2 + x - 1$ is irreducible over $\mathbb{F}_3$ while $x^2 + x + 1$ is not, the element $\zeta \in \mathbb{F}_q^\times$ from Proposition 2.2.12 is equal to $-1$. We therefore calculate that $\hat{H}$ contains the block diagonal matrix $T := \mathrm{diag}(I_1, X_1, X_2, \ldots, X_{n/4-1}, K, Y_1, Y_2, \ldots, Y_{n/4-1}, I_1)$, where each $X_i$ and $Y_i$ is as in the previous paragraph, and $K := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. In particular, if $n = 4$, then $T = \mathrm{diag}(I_1, K, I_1)$. Similarly to the previous paragraph, $T^2 = \mathrm{diag}(1, -1, -1, \ldots, -1, 1)$ acts as the scalar $-1$ on each vector in $W$, and we can set $D = T^2$.

**Case (c)**: $W^\perp$ is degenerate but not totally singular. By Proposition 3.6.2(i), we may assume that $Q(w_1) = (w_1, w_2) = 0$ and $Q(w_2) = \mu$ for some $\mu \in \mathbb{F}_q^\times$. Suppose first that $n > 4$. By (2.2.1), $Q(e_2 + \mu e_{n-1}) = \mu(e_2, e_{n-1}) = \mu$. Additionally, $Q(e_1) = 0 = (e_1, e_2 + \mu e_{n-1})$. We may therefore assume that $w_1 = e_1$ and $w_2 = e_2 + \mu e_{n-1}$.

Then $W = \langle e_1, e_2 - \mu e_{n-1}, e_3, \ldots, e_{n-2}\rangle$. Let $S$ be the $n \times n$ matrix that acts as

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ -\mu & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ -\mu & 1 & \mu & 1 \end{pmatrix}$$

on $\langle e_1, e_2, e_{n-1}, e_n\rangle$, and as $I_{n-4}$ on $\langle e_3, \ldots, e_{n-2}\rangle$. Then $S$ fixes each vector in $W$, and $S \in \hat{H}$. As $S$ is lower unitriangular, we can set $D = S$ if $q$ is odd. If instead $q$ is even, then we may assume that $\mu = 1$. Notice that $I_n + S$ has rank 2, and so we can again set $D = S$.

Suppose finally that $n = 4$, so that $\varepsilon = -$. Then $Q(e_1) = (e_1, e_2) = 0$ and $Q(e_2) = 1$. Assume first that $q$ is even. Then we may assume that $\mu = 1$, $w_1 = e_1$ and $w_2 = e_2$, so that $W = W^\perp$. Then $\hat{H}$ contains the matrix

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

which acts trivially on $W$. Moreover, $I_4 + L$ has rank 2, and so we can set $D = L$.

Assume now that $q$ is odd, and write $w_2 = \sum_{i=1}^4 \alpha_i e_i$, with each $\alpha_i \in \mathbb{F}_q$. Recall from Proposition 3.1.6 that $\hat{G}$ acts transitively on the set of one-dimensional totally singular subspaces of $V$. As $Q(w_1) = 0 = Q(e_1)$, we may assume without loss of generality that $w_1 = e_1$. Then $\alpha_4 = (e_1, \sum_{i=1}^4 \alpha_i e_i) = (e_1, w_2) = (w_1, w_2) = 0$. Let $\zeta$ be the element of $\mathbb{F}_q^\times$ from Proposition 2.2.12, so that the polynomial $x^2 + x + \zeta$ is irreducible over $\mathbb{F}_q$. By (2.2.1), $Q(w_2) = \alpha_2^2 + \alpha_3^2\zeta + \alpha_2\alpha_3$ does not depend on $\alpha_1$, and so we may assume that $\alpha_1 = 0$.

Observe that $-2^{-1}$ is a root of the polynomial $x^2 + x + 4^{-1}$ in $\mathbb{F}_q[x]$, and hence $\zeta \neq 4^{-1}$. Therefore, $1 - 4\zeta \neq 0$, and we can define $\gamma := (1 - 4\zeta)^{-1}$. Assume first that $\alpha_2 = -2\alpha_3\zeta$. It is easy to check that $W = \langle e_1, e_3\rangle$, and that the lower unitriangular matrix

$$M := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \gamma\zeta & 2\gamma\zeta & -\gamma & 1 \end{pmatrix}$$

lies in $\hat{H}$ and acts trivially on $W$. Thus we can set $D = M$. If instead $\alpha_2 \neq -2\alpha_3\zeta$, then let $\delta := -(2\alpha_2 + \alpha_3)(\alpha_2 + 2\alpha_3\zeta)^{-1}$. We observe that $W = \langle e_1, e_2 + \delta e_3\rangle$, and

that

$$N := \begin{pmatrix} 1 & 0 & 0 & 0 \\ -\delta & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ (1+\delta+\delta^2\zeta)\gamma & -(1+2\delta\zeta)\gamma & (2+\delta)\gamma & 1 \end{pmatrix}$$

lies in $\hat{H}$ and acts trivially on $W$. As $N$ is lower unitriangular, we can set $D = N$. □

Later in this section, we will see using computational examples that the exceptions listed in the statement of Lemma 3.6.4 are necessary, and can result in differences between the base sizes of corresponding actions of $G$ and $H$.

We also note that, unlike in the symplectic and unitary cases, we cannot replace $n-2$ with $n-1$ in the above lemma, even when considering matrices in the group $\mathrm{GO}^\varepsilon(n,q)$. Indeed, using Theorem 2.2.6 and similar matrix calculations to those in the above proof, we can show that if a matrix $A \in \mathrm{GO}^\varepsilon(n,q)$ acts as a scalar on the subspace $\langle e_1, \ldots, e_{n-1}\rangle$ of $V$ (corresponding to the standard form from Proposition 2.2.12), then $A$ is in fact a scalar matrix. Here we also use the fact that the scalar $\zeta$ from Proposition 2.2.12 cannot be equal to $4^{-1}$ when $q$ is odd, as shown in the above proof.

**Corollary 3.6.5.** *Let $U$ be an $(n-3)$-dimensional subspace of $V$. Then $\Omega^\varepsilon(n,q)$ contains a non-scalar matrix that acts as a scalar on $U$.*

*Proof.* Lemma 2.2.2 shows that $U^\perp$ is a three-dimensional subspace of $V$. Hence $U^\perp$ contains a degenerate two-dimensional subspace $X$ by Proposition 3.6.3. It also follows from Lemma 2.2.2 that $\dim(X^\perp) = n-2$ and $(X^\perp)^\perp = X$. Thus Lemma 3.6.4 implies that $\Omega^\varepsilon(n,q)$ contains a non-scalar matrix $A$ that acts as a scalar on $X^\perp$. Furthermore, $U \subseteq X^\perp$ by Proposition 2.2.3, and so $A$ acts a scalar on $U$. □

*Proof of Theorem 3.6.1.* Suppose first that $|\Delta| < \lceil n/k \rceil$, with $|\Delta| < \lceil n/k \rceil - 1$ if $k \mid (n-1)$. Then $\langle\Delta\rangle$ lies in an $(n-2)$-dimensional subspace $W$ of $V$. It follows from Lemma 3.6.4 that if $K = \mathrm{SO}^\varepsilon(n,q)$, or if $K = \Omega^\varepsilon(n,q)$ and $K/Z(K) \notin \mathcal{O}$, then $K$ contains a non-scalar matrix that acts as a scalar on $W$, and hence on $\langle\Delta\rangle$. Hence $(K/Z(K))_{(\Delta)} \neq 1$.

It remains to show that $G_{(\Delta)} \neq 1$ when[2] $|\Delta| < \lceil n/k \rceil - 1 - \delta_{1k}$; or when $|\Delta| = \lceil n/k \rceil - 1$ and $k$ divides neither $n-1$ nor $n-2$. In each of these cases, $\langle\Delta\rangle$ lies in an $(n-3)$-dimensional subspace $U$ of $V$. Corollary 3.6.5 shows that $\Omega^\varepsilon(n,q)$ contains a non-scalar matrix that acts as a scalar on $U$, and hence on $\langle\Delta\rangle$. Therefore, $G_{(\Delta)} \neq 1$. □

[2]Note that the first possibility here includes the case where $|\Delta| < \lceil n/k \rceil - 1$, $k \mid (n-1)$, and $k \nmid (n-2)$.

This completes the proof of Theorem 3.1.9 (see Remark 3.1.10).

We will again compare the lower bounds for the base sizes of $G = \mathrm{P}\Omega^{\varepsilon}(n,q)$ and $H = \mathrm{PSO}^{\varepsilon}(n,q)$ from Theorem 3.1.9(iv) with known bounds in the algebraic and finite cases, and with computational examples. First, by [27, Theorem 4(iii)], if $n \geqslant 7$ and the base size of the special orthogonal algebraic group is not equal to $t := \lceil n/k \rceil$, then either $k \mid (n-1)$ and the base size is equal to $t-1$ (with $t \geqslant 4$ required in the totally singular case), or the action is on totally singular subspaces, and $n$, $k$ and $t$ must take certain values. These totally singular exceptions include the cases where $t = 3$, $k \nmid n$, and the base size is equal to 4; and the case where $n = 8$, $k = 4$, and the base size is equal to 7. The remaining exceptions assume that $n \geqslant 10$ and $k = n/2$. Certain related results in the case $n < 7$ are also given in [27, §4.1.3]. Note that, while the special orthogonal algebraic group is analogous to $H$, there is no algebraic group that is a direct analogue of $G$. Additionally, as noted in [72, p. 29], given $n$ and a prime $p$, there is a unique $n$-dimensional special orthogonal algebraic group defined over the algebraic closure of $\mathbb{F}_p$. In particular, this algebraic group corresponds to $\mathrm{SO}^{\varepsilon}(n,q)$ for each allowed value of $\varepsilon$ (and each power $q$ of $p$).

In the finite case, [72, p. 26, p. 28] again yields the general upper bounds of $n/k+11$ and $n/k+10$ for $b(G)$, in the non-degenerate and totally singular cases, respectively. Additionally, in the totally singular case where $n/k = 2$ and $\varepsilon = +$, [72, p. 28] gives a reduced upper bound of $n/k+7 = 9$.

Now, [113, Lemma 3, Lemma 5, Lemmas 7–10] gives upper bounds for the base sizes of subspace actions of $R := \mathrm{PGO}^{\varepsilon}(n,q)$ when $k \leqslant 2$, with certain restrictions on $n$. Suppose first that $k = 1$, with $n \geqslant 5$ in the totally singular case, and $n \geqslant 4$ otherwise. Then either $b(R) \leqslant n-1$; the action is non-degenerate or nonsingular and $b(R) \leqslant n = 5$; or $R = \mathrm{PGO}^{-}(4,3)$ and $b(R) = 4$. In fact, when $n \geqslant 6$ is even, $b(R)$ is equal to the upper bound of $n-1$. Finally, if $k = 2$ and $n \geqslant 7$, then $b(R) \leqslant \lceil n/2 \rceil$. Note that, if $n$ is even, $q$ is odd and the action of $R$ is on non-degenerate one-dimensional subspaces (so that case (b) of Proposition 3.1.6 applies), then $G$ acts transitively on the same set of subspaces as $R$; see [89, Tables 3.5.E–3.5.G] and the tables in [17, §8.2].

Since $|H : G|$ and $|R : H|$ are each at most 2 by [17, Table 1.3], it follows from Lemma 3.1.8 that if $H$ acts primitively on a set $\Omega$, then $b(G,\Omega) \leqslant b(H,\Omega) \leqslant b(G,\Omega)+1$, and if $R$ acts primitively, then $b(H,\Omega) \leqslant b(R,\Omega) \leqslant b(H,\Omega)+1$. Recall also from Proposition 3.1.6 that if a subgroup $T$ of $R$ contains $G$ and acts primitively on $\Omega$, then $G$ acts transitively on $\Omega$. By comparing the upper bounds in the case $k \leqslant 2$ from the previous paragraph with our lower bounds from Theorem 3.1.9(iv),

we obtain the following two results. Recall the definition of the set $\mathcal{O}$ from the start of this section.

**Proposition 3.6.6.** *Let $T$ be an almost simple group with socle $\mathrm{P\Omega}^\varepsilon(n,q)$, such that $T \leqslant \mathrm{PGO}^\varepsilon(n,q)$, and let $\Omega$ be a set of one-dimensional subspaces of $V$ such that the action $(T,\Omega)$ is primitive. Assume that either:*

(i) *each subspace in $\Omega$ is non-degenerate or nonsingular, $n = 4$, and $q \neq 3$;*

(ii) *each subspace in $\Omega$ is totally singular, and $n = 5$; or*

(iii) *$n \geqslant 6$.*

*Then $n-2 \leqslant b(T) \leqslant n-1$. Moreover, if either $\mathrm{PSO}^\varepsilon(n,q) \leqslant T$ or $\mathrm{P\Omega}^\varepsilon(n,q) \notin \mathcal{O}$, then $b(T) = n-1$.*

**Proposition 3.6.7.** *Let $T$ be an almost simple group with socle $\mathrm{P\Omega}^\varepsilon(n,q)$, such that $n \geqslant 7$ and $T \leqslant \mathrm{PGO}^\varepsilon(n,q)$, and let $\Omega$ be a set of two-dimensional subspaces of $V$ such that the action $(T,\Omega)$ is primitive. Then $\lceil n/2 \rceil - 1 \leqslant b(T) \leqslant \lceil n/2 \rceil$. Moreover, $b(T) = \lceil n/2 \rceil$ if either:*

(i) *$T = \mathrm{PGO}^\varepsilon(n,q)$; or*

(ii) *$n$ is even, and either $\mathrm{PSO}^\varepsilon(n,q) \leqslant T$ or $\mathrm{P\Omega}^\varepsilon(n,q) \notin \mathcal{O}$.*

In addition, when $n \leqslant 6$, we can use the tables in [17, §2.2, §8.2] to determine the maximal subgroup type of a point stabiliser of $(G,\Omega)$, considered as a subgroup of an isomorphic non-orthogonal classical group (see §2.4). In some cases, we are then able to deduce from [23, Tables 2–3] that $b(T,\Omega) \in \{2,3,4\}$ for each almost simple group $T$ with socle $G$ such that $(T,\Omega)$ is primitive. Among these cases, if $b(G,\Omega) = 4$, then $G = \mathrm{P\Omega}^-(6,3) \cong \mathrm{PSU}(4,3)$ [23, Proposition 4.1].

Now, we can use the Magma code in `base_size_s_u_o` to determine the base size of specific primitive actions of $G$ and $H$ on sets of subspaces. As there is a significant amount of data here, we will consider three separate cases, corresponding to the three possible values of $\varepsilon$. After discussing all three cases, we will summarise with a comment on the effectiveness of known bounds for the base size. We will see that when $n$, $k$ and the type of the action are all fixed, the base size of the action is often the same for multiple values of $q$. Thus, for prime powers $a$ and $b$, we write $[a,\ldots,b]$ to denote all prime powers between $a$ and $b$, inclusive, that are allowed for the given values of $k$ and $n$. Thus these are all such prime powers if $k$ and $n$ are even or the action is on degenerate subspaces, but only the prime powers that

are odd otherwise (see Proposition 3.1.4). If $a$ and $b$ are consecutive allowed prime powers, then we will instead write $[a, b]$.

In each case, we can use the tables in [17, §2.2.1, §8.2] to determine whether a given action is primitive (with the condition $n \leqslant 12$, as in all of our examples; for higher dimensions, see the tables in [89, §3.5]). In almost all of our examples, if $G$ acts primitively on a given set $\Omega$ of subspaces of $V$, then so does $H$. The only exceptions are those where $\varepsilon = +$, $q$ is even and $k = n/2$ (so that each subspace in $\Omega$ is totally singular). Here, the exceptional case (a) of Proposition 3.1.6 applies, and $H$ acts transitively, but not primitively, on a set of subspaces that properly contains $\Omega$.

First, assume that $\varepsilon = \circ$. Table 3.6.1 lists $b(G, \Omega)$ and $b(H, \Omega)$ for certain sets $\Omega$ of $k$-dimensional subspaces of $V$. In each case, the action is primitive, unless indicated otherwise. Recall that $q$ is odd in each case, and that for each $k < n/2$, the group $G$ has up to two primitive actions on non-degenerate $k$-dimensional subspaces of $V$, corresponding to the two isometry types of such subspaces. If $k$ is even, then we can characterise $\Omega$ according to the types (plus or minus) of its subspaces, and if $k$ is odd, then we can instead consider the types of the complements of the subspaces. Defining the tuple $(n, q, k, \theta)$ as in Table 3.6.1, we note that the (transitive) actions of both $G$ and $H$ corresponding to the tuples $(3, 5, 1, +)$, $(5, 3, 2, \pm)$ and $(7, 3, 2, +)$ are imprimitive.

We see that, in our single example[3] where $k$ does not divide $n - 1$ (with $n = 9$), the base size of $G$ achieves the lower bound of $t = \lceil n/k \rceil$ from Theorem 3.1.9. Furthermore, in several of the remaining examples, $b(G)$ achieves the lower bound of $t - 1$ that corresponds to the condition $k \mid (n - 1)$. In particular, this is the case when $k = 1$, $n = 5$ and each subspace is non-degenerate, indicating that the hypotheses of Proposition 3.6.6 are stronger than necessary. On the other hand, there are examples where $k \mid (n - 1)$ and $b(G) \in \{t, t + 1\}$.

Note that in each example with $b(G) = t + 1$, the subspaces in $\Omega$ are totally singular, $t = 3$, $k \nmid n$, and $b(H) = b(G)$. Hence the base sizes in these cases agree with the corresponding values in the algebraic case. There are also totally singular cases where $b(G) = b(H) = t = 3$, and this may be related to the requirement $t \geqslant 4$ in the totally singular algebraic case for the base size to be equal to $t - 1$. However, we observe that there is a totally singular case where $b(H) = t = 4$, and a totally singular case where $k \mid n$ and $b(H) = t + 1 = 4$. In addition, since $b(H) = 5$ when $(n, q, k, \theta) = (5, 3, 2, -)$, the aforementioned upper bound of 5 for $b(R)$, in the

[3] In each non-degenerate case where $k = 3$ and $(n, q) = (9, 3)$, the degree of the action is too large to construct the corresponding permutation group in Magma. This is also true for the totally singular case where $k = 3$ and $(n, q) = (9, 5)$.

Table 3.6.1: The base sizes $b_1$ of $\Omega(n,q)$ and $b_2$ of $\mathrm{SO}(n,q)$ acting on a set $\Omega$ of $k$-dimensional subspaces of $\mathbb{F}_q^n$ of type $\theta$. If each subspace in $\Omega$ is totally singular, then $\theta = 0$. If instead each subspace is non-degenerate, then $\theta \in \{+,-\}$ is the type of each subspace if $k$ is even, or the type of the complement of each subspace if $k$ is odd. Finally, * denotes an imprimitive action.

| $n/k$ | $(n,q,k,\theta)$ | $b_1$ | $b_2$ |
|---|---|---|---|
| 7/3 | $(7,3,3,+)$ | 2 | 2 |
| 7/3 | $(7,3,3,-)$ | 2 | 3 |
| 7/3 | $(7,3,3,0)$ | 4 | 4 |
| 5/2 | $(5,[5,7],2,+)$ | 2 | 2 |
| 5/2 | $(5,[5,7],2,-)$ | 2 | 3 |
| 5/2 | $(5,[3,\dots,11],2,0)$ | 4 | 4 |
| 3 | $(3,[7,\dots,11],1,+)$ | 2* | 2 |
| 3 | $(3,[7,9],1,-)$ | 2* | 3 |
| 3 | $(3,[13,\dots,25],1,+)$ | 2 | 2 |
| 3 | $(3,5,1,-),(3,[11,\dots,25],1,-)$ | 2 | 3 |
| 3 | $(3,[5,\dots,25],1,0)$ | 3 | 3 |
| 3 | $(9,3,3,0)$ | 3 | 4 |
| 7/2 | $(7,3,2,-)$ | 3 | 3 |
| 7/2 | $(7,3,2,0)$ | 3 | 4 |
| 5 | $(5,[3,\dots,7],1,0),(5,[3,\dots,7],1,+),(5,[5,7],1,-)$ | 4 | 4 |
| 5 | $(5,3,1,-)$ | 4 | 5 |
| 7 | $(7,3,1,0),(7,3,1,\pm)$ | 6 | 6 |

non-degenerate case with $n = 5$, is tight.

Next, assume that $\varepsilon = +$. Table 3.6.2 lists the base sizes for certain primitive actions of $G$ and $H$ on sets $\Omega$ of $k$-dimensional subspaces of $V$. As mentioned above, when $k = n/2$, $q$ is even, and the action is on totally singular subspaces, $H$ acts transitively but imprimitively on a set properly containing $\Omega$. Thus we do not include any such action of $H$. Additionally, for convenience, when $q$ is even, we will say that a one-dimensional nonsingular subspace has type $\circ$. Hence defining the triple $(n,q,k,\theta)$ as in Table 3.6.2, $(6,[3,\dots,7],1,\circ)$ corresponds to an action on non-degenerate subspaces when $q \in \{3,5,7\}$, and on nonsingular subspaces when $q = 4$. Recall however from Proposition 3.1.4 that if $k > 1$ and $\theta = \circ$, then $q$ is necessarily odd. We also note that the actions of both $G$ and $H$ corresponding to the tuples $(6,3,2,0)$, $(6,[2,3],2,+)$, $(8,[2,3],2,+)$ and $(8,3,3,0)$ are imprimitive.

In most of our examples, the corresponding lower bound from Theorem 3.1.9 is achieved. In particular, we observe that all conditions given in Theorem 3.1.9(iv)

Table 3.6.2: The base sizes $b_1$ of $\mathrm{P}\Omega^+(n,q)$ and $b_2$ of $\mathrm{PSO}^+(n,q)$ acting on a set $\Omega$ of $k$-dimensional subspaces of $\mathbb{F}_q^n$ of type $\theta$. If each subspace in $\Omega$ is totally singular, then $\theta = 0$, and if each subspace is non-degenerate or nonsingular, then $\theta \in \{\circ, +, -\}$ is the type of each subspace. Finally, * denotes an imprimitive action, and we have not included the actions of $\mathrm{PSO}^+(n,q)$ on totally singular $n/2$-dimensional subspaces when $q$ is even.

| $n/k$ | $(n,q,k,\theta)$ | $b_1$ | $b_2$ |
|---|---|---|---|
| 2 | $(6,2,3,0)$ | 4 | N/A |
| 2 | $(6,4,3,0)$ | 5 | N/A |
| 2 | $(6,3,3,0),(6,[5,7],3,0)$ | 5 | 5 |
| 2 | $(8,2,4,0)$ | 6 | N/A |
| 2 | $(8,3,4,0)$ | 6 | 6 |
| 2 | $(8,4,4,0)$ | 7 | N/A |
| 2 | $(8,5,4,0)$ | 7 | 7 |
| 8/3 | $(8,3,3,\circ)$ | 2 | 3 |
| 8/3 | $(8,2,3,0)$ | 4* | 4 |
| 3 | $(6,2,2,0)$ | 3* | 3 |
| 3 | $(6,[4,\ldots,7],2,+),(6,[3,\ldots,7],2,-)$ | 3 | 3 |
| 3 | $(6,2,2,-)$ | 3 | 4 |
| 3 | $(6,4,2,0)$ | 4* | 4 |
| 4 | $(8,[2,3],2,0),(8,3,2,-)$ | 3 | 4 |
| 4 | $(8,2,2,-)$ | 4 | 4 |
| 6 | $(6,2,1,0),(6,2,1,\circ)$ | 4 | 5 |
| 6 | $(6,[3,\ldots,7],1,0),(6,[3,\ldots,7],1,\circ)$ | 5 | 5 |
| 8 | $(8,[2,3],1,0),(8,[2,3],1,\circ)$ | 6 | 7 |

are necessary. Moreover, each example with $b(H) = b(G) + 1$ corresponds to an exceptional case listed in the statement of Lemma 3.6.4. However, the base sizes in the examples with $k = n/2$ are significantly higher than our lower bounds, suggesting that it may be possible to improve the bounds in this case. Note that when $n = 8$, $k = 4$ and $q \in \{4, 5\}$, the base size of 7 is equal to the aforementioned exceptional base size in the corresponding algebraic case. There are also certain cases with $k = q = 2$ where the base size does not achieve our lower bound. However, in the non-degenerate case with $n = 8$, the base size for $G$ does achieve the upper bound of $n/2$ from Proposition 3.6.7. Additionally, $b(H) = 4$ when $(n,q,k,\theta) = (8,2,3,0)$, agreeing with the corresponding exceptional algebraic case. We also note that our lower bound for $b(H)$ is not achieved when $(n,q,k,\theta) = (6,4,2,0)$.

Finally, assume that $\varepsilon = -$. The base sizes for certain primitive actions of $G$

on sets $\Omega$ of $k$-dimensional subspaces of $V$ are given in Table 3.6.3. Again, when $k = 1$, we write $\circ$ to denote the type of a subspace that is either non-degenerate or nonsingular, and $q$ is odd whenever $k > 1$ and $\theta = \circ$. The actions of $G$ and $H$ corresponding to the tuples $(4, 3, 2, \pm)$, $(6, [2, 3], 2, +)$, $(6, 2, 2, -)$ and $(8, [2, 3], 2, +)$ are imprimitive. Note also that the actions with $\theta = +$ and $\theta = -$ are equivalent when $q$ is fixed and $k = n/2$ (so that $4 \mid n$), as are the actions corresponding to the tuples $(4, 2, 2, \pm)$ and $(4, 2, 1, \circ)$.

Table 3.6.3: The base sizes $b_1$ of $\mathrm{P}\Omega^-(n, q)$ and $b_2$ of $\mathrm{PSO}^-(n, q)$ acting primitively on a set $\Omega$ of $k$-dimensional subspaces of $\mathbb{F}_q^n$ of type $\theta$. If each subspace in $\Omega$ is totally singular, then $\theta = 0$, and if each subspace is non-degenerate or nonsingular, then $\theta \in \{\circ, +, -\}$ is the type of each subspace.

| $n/k$ | $(n, q, k, \theta)$ | $b_1$ | $b_2$ |
|---|---|---|---|
| 2 | $(4, [5, 7], 2, \pm), (4, [9, \ldots, 13], \pm)$ | 2 | 2 |
| 2 | $(4, 2, 2, \pm), (4, 4, 2, \pm), (4, 8, 2, \pm), (8, 2, 4, \pm)$ | 2 | 3 |
| 8/3 | $(8, 3, 3, \circ)$ | 3 | 3 |
| 8/3 | $(8, [2, 3], 3, 0)$ | 4 | 4 |
| 3 | $(6, 3, 2, -)$ | 2 | 3 |
| 3 | $(6, [4, \ldots, 7], 2, \pm)$ | 3 | 3 |
| 3 | $(6, 3, 2, 0)$ | 3 | 4 |
| 3 | $(6, 2, 2, 0), (6, [4, \ldots, 7], 2, 0)$ | 4 | 4 |
| 4 | $(4, 2, 1, \circ)$ | 2 | 3 |
| 4 | $(4, 3, 1, 0), (4, [5, 7], 1, 0), (4, [9, \ldots, 13], 1, 0), (4, [3, \ldots, 13], 1, \circ)$ | 3 | 3 |
| 4 | $(4, 2, 1, 0), (4, 4, 1, 0), (4, 8, 1, 0), (8, 2, 2, -)$ | 3 | 4 |
| 4 | $(8, [2, 3], 2, 0), (8, 3, 2, -)$ | 4 | 4 |
| 6 | $(6, [2, 3], 1, 0), (6, [2, 3], 1, \circ)$ | 4 | 5 |
| 6 | $(6, [4, \ldots, 7], 1, 0), (6, [4, \ldots, 7], 1, \circ)$ | 5 | 5 |
| 8 | $(8, 2, 1, 0), (8, 2, 1, \circ)$ | 6 | 7 |
| 8 | $(8, 3, 1, 0), (8, 3, 1, \circ)$ | 7 | 7 |

As in the plus type case, our lower bounds from Theorem 3.1.9(iv) are achieved in most of our examples, and we see that all of the conditions given in this theorem are necessary. Additionally, many of our examples satisfying $b(H) = b(G) + 1$ correspond to the exceptional cases given in Lemma 3.6.4. Observe that, among the examples with $n/k = 2$, our lower bounds for $b(G)$ and $b(H)$ are sometimes achieved. However, our lower bound for $b(G)$ is not achieved when $(n, q, k) = (4, 2, 2)$, and our lower bound for $b(H)$ is not achieved when $n/k = 2$ and $q$ is even. Our lower bounds are also not achieved in the totally singular cases with $n = 6$ and $k = 2$, or with $n = 8$ and $k = 3$. In these latter cases, the base sizes are equal to the

exceptional value of 4 from the corresponding algebraic case. Finally, in the totally singular cases with $n/k = 4$, our lower bound for $b(G)$ is not achieved when $q = 2$, and our lower bound for $b(H)$ is not achieved when $n = 4$ and $q$ is even. However, when $n = 8$ and $q = k = 2$, the base size for $G$ achieves the upper bound from Proposition 3.6.7.

Summarising the overall orthogonal case, in most of our examples, $b(G, \Omega)$ and $b(H, \Omega)$ achieve the lower bounds from 3.1.9(iv). When these bounds are not met, the base size is sometimes equal to the upper bound from Proposition 3.6.7, or to the base size for the corresponding algebraic group. In general, it is likely that our lower bounds could be improved in various cases, especially when $k = n/2$ and $\varepsilon = +$, and that the upper bounds from [72, p. 26, p. 28] could be significantly reduced.

# Chapter 4

# The intersection graph of a finite simple group

## 4.1 Background and the main theorem

In this chapter, we determine a tight upper bound for the diameter of the intersection graph of a finite simple group. We begin by outlining basic graph theoretic terminology and notation that we will use throughout this thesis.

Let $\Gamma$ be a graph (with no loops) with vertex set $V(\Gamma)$ and edge set $E(\Gamma)$. For convenience, we will usually not distinguish between $\Gamma$ and $V(\Gamma)$. If $\{x, y\} \in E(\Gamma)$, then we write $x \sim_\Gamma y$, or $x \sim y$ if the underlying graph is clear. The subgraph of $\Gamma$ *induced* by a subset $\Delta$ of $V(\Gamma)$ is the graph whose vertex set is equal to $\Delta$, and whose edge set is equal to $E(\Gamma) \cap \{\{x, y\} \mid x, y \in \Delta\}$. A *spanning subgraph* of $\Gamma$ is a graph with the same vertex set as $\Gamma$, and whose edge set is a subset of that of $\Gamma$.

Now, a *walk* in $\Gamma$ is a sequence of vertices such that any two consecutive vertices are joined by an edge, and a *path* is a walk with all vertices distinct. The *length* of a walk is the corresponding number of traversed edges (with possible repeats). We say that $\Gamma$ is *connected* if there is a path in the graph between any given pair of vertices. More generally, a *connected component* of $\Gamma$ is an induced subgraph that is maximal among all connected induced subgraphs. A connected component is *trivial* if it consists of a single vertex, and we call any such vertex (i.e., a vertex with no neighbours) *isolated*.

The *distance* in $\Gamma$ between two vertices $x$ and $y$ is the length of the shortest path in $\Gamma$ between these vertices. We denote this distance by $d_\Gamma(x, y)$, or $d(x, y)$ if the underlying graph is clear. Note that $d(x, x) = 0$, and that if $x$ and $y$ lie in distinct connected components of $\Gamma$, then $d(x, y) = \infty$. The *diameter* $\mathrm{diam}(\Gamma)$ of $\Gamma$ is the maximal distance in $\Gamma$ among all pairs of vertices. Hence if $|\Gamma| \leqslant 1$, then $\mathrm{diam}(\Gamma) = 0$, and if $\Gamma$ is not connected, then $\mathrm{diam}(\Gamma) = \infty$. Note that the graph with no vertices is called the *empty graph*.

We now expand on the background of the intersection graph of a (finite) group

presented in §1.0.2 by formally defining this graph, and then summarising what is known about its diameter.

**Definition 4.1.1** ([48])**.** The intersection graph $\Delta_G$ of a group $G$ is the graph whose vertices are the nontrivial proper subgroups of $G$, with distinct subgroups joined by an edge if and only if they intersect nontrivially.

This graph was introduced as an analogue of the intersection graph of a semigroup, defined by Bosák [14].

**Theorem 4.1.2** ([48, pp. 242–243])**.** *Let $G$ be a nontrivial, non-simple finite group. Then the following statements hold.*

(i) *$\Delta_G$ is disconnected if and only if either $G \cong C_p \times C_q$ for (not necessarily distinct) primes $p$ and $q$, or $Z(G) = 1$ and each proper subgroup of $G$ is abelian.*

(ii) *If $\Delta_G$ is connected, then* $\operatorname{diam}(\Delta_G) \leqslant 4$.

A non-abelian group with all proper subgroups abelian is called *minimal non-abelian*, and the finite groups with this property were classified by Miller and Moreno [110] in 1903. We will discuss minimal non-abelian groups in more detail in §5.3.

We note that it is unknown whether there exists a non-simple finite group $G$ such that $\operatorname{diam}(\Delta_G) = 4$. However, Csákány and Pollák [48, §2] proved that any such group $G$ must be isomorphic to $S{:}C_p$ for some non-abelian simple group $S$ and some prime $p$. In fact, using their reasoning and Lemma 4.2.2 below, it is straightforward to see that $p$ must be odd.

Much more recently, the diameter of the intersection graph of a general linear group defined over a (finite or infinite) field or division ring was studied in [12, 70].

For the remainder of this chapter, we consider the case where $G$ is a non-abelian finite simple group. First, in their original paper on the intersection graph in 1969, Csákány and Pollák [48, p. 246] proved that if $G$ is a finite simple alternating group, then $3 \leqslant \operatorname{diam}(\Delta_G) \leqslant 4$, with $\operatorname{diam}(\Delta_G) = 3$ if the degree of $G$ is not prime. In fact, it is an open question whether there exists a finite alternating group whose intersection graph has diameter 4.

In 2010, Shen [126] proved that $\Delta_G$ is connected for each non-abelian finite simple group $G$, and posed two questions: Does the diameter of $\Delta_G$ in this case have an upper bound? If yes, does the upper bound of 4 from Theorem 4.1.2 apply here? In the same year, Herzog, Longobardi and Maj [77] independently answered Shen's first question in the affirmative, by studying the subgraph of $\Delta_G$ induced by

the maximal subgroups of $G$. In particular, they proved that the diameter of this subgraph is always at most 62. As each vertex of $\Delta_G$ is equal or adjacent to some maximal subgroup of $G$, their work implies that $\mathrm{diam}(\Delta_G) \leqslant 64$. This upper bound was reduced to 28 by Ma [106] in 2016.

In the other direction, $\mathrm{diam}(\Delta_G)$ has the following lower bound.

**Theorem 4.1.3** ([125, Theorem 3.7])**.** *Let $G$ be a non-abelian finite simple group. Then $\mathrm{diam}(\Delta_G) \geqslant 3$.*

This lower bound is best possible, as witnessed by the aforementioned finite simple alternating groups of composite degree.

In order to answer Shen's second question, and in particular to determine the best possible upper bound for $\mathrm{diam}(\Delta_G)$, we prove the following.

**Theorem 4.1.4.** *Let $G$ be a non-abelian finite simple group.*

(i) *$\Delta_G$ is connected with diameter at most 5.*

(ii) *If $G$ is the baby monster group $\mathbb{B}$, then $\mathrm{diam}(\Delta_G) = 5$.*

(iii) *If $\mathrm{diam}(\Delta_G) = 5$ and $G \ncong \mathbb{B}$, then $G$ is a unitary group $\mathrm{PSU}(n, q)$, with $n$ an odd prime and $q$ a prime power.*

This theorem provides a negative answer to Shen's second question: the upper bound of 4 from Theorem 4.1.2 is not sufficient for finite simple groups. We also prove the following result, which expands on Theorem 4.1.4(iii).

**Proposition 4.1.5.** *Let $k \in \{3, 4, 5\}$. Then there exists an odd prime $n$ and a prime power $q$ such that $G := \mathrm{PSU}(n, q)$ is simple and $\mathrm{diam}(\Delta_G) = k$. Indeed, $\Delta_{\mathrm{PSU}(7,2)}$ has diameter 5.*

We will prove Theorem 4.1.4 and Proposition 4.1.5 in §4.2. Note that the aforementioned results of Shen, Herzog et al. and Ma regarding the connectedness and diameter of $\Delta_G$ were proved by studying the close relationship between $\Delta_G$ and the *prime graph* (or *Gruenberg-Kegel graph*) of $G$. This latter graph was defined by Gruenberg and Kegel in 1975, in an unpublished manuscript; see [146]. The vertices of this graph are the prime divisors of $|G|$, with distinct vertices $p$ and $r$ joined by an edge if and only if $G$ contains an element of order $pr$. Our proof of Theorem 4.1.4 is more direct.

In Chapter 6, we will use Theorem 4.1.4(ii) and Proposition 4.1.5 to determine the diameters of the *non-commuting, non-generating graphs* and the *non-generating graphs* (see §1.0.2 or §5.1) of $\mathbb{B}$ and $\mathrm{PSU}(7, 2)$.

Theorem 4.1.4(ii) has also been used by Burness, Lucchini and Nemmi in [29, §4] to prove that the *soluble graph* of $\mathbb{B}$ is connected with diameter 4 or 5. The vertices of this graph are the non-identity elements of $\mathbb{B}$, with two elements adjacent if and only if they generate a soluble subgroup of $\mathbb{B}$. Note that Cameron's [34, §2.6] hierarchy of graphs, which we mentioned in §1.0.2, can be adapted to include the soluble graph of $G$ (assuming that $G$ is insoluble).

## 4.2 The diameter of the intersection graph of a finite simple group

The main focus of this section is the proof of Theorem 4.1.4. We will also prove here a more detailed result about distances between vertices in $\Delta_{\mathbb{B}}$, as well as Proposition 4.1.5. Here, $G$ denotes a non-abelian finite simple group, and for nontrivial proper subgroups $H$ and $K$ of $G$, we write $d(H,K) := d_{\Delta_G}(H,K)$.

We will begin by highlighting a few elementary yet useful observations that have previously been used to study the graph $\Delta_G$.

**Lemma 4.2.1** ([48, p. 246])**.** *The diameter of $\Delta_G$ is equal to the maximum distance in the graph between cyclic subgroups of $G$ of prime order.*

*Proof.* Let $H$ and $K$ be nontrivial proper subgroups of $G$, and let $P$ and $Q$ be cyclic subgroups of prime order of $H$ and $K$, respectively. Each subgroup of $G$ that intersects nontrivially with $P$ also intersects nontrivially with $H$, and similarly for $Q$ and $K$. Hence $d(H,K) \leqslant d(P,Q)$. □

The following was observed in [106, Lemma 2.2, Proof of Lemma 2.3], and a similar observation was made in [77, Proposition 3.1].

**Lemma 4.2.2.** *Let $H$ and $K$ be nontrivial proper subgroups of $G$. If $|H|$ and $|K|$ are even, then $d(H,K) \leqslant 2$. Hence, in general, if $H$ and $K$ lie in maximal subgroups of even order, then $d(H,K) \leqslant 4$. Furthermore, if every maximal subgroup of $G$ has even order, then* $\mathrm{diam}(\Delta_G) \leqslant 4$.

*Proof.* Suppose first that $|H|$ and $|K|$ are even. We may assume that $d(H,K) > 1$, so that $H \cap K = 1$. Let $a$ and $b$ be involutions of $H$ and $K$, respectively. Then $D := \langle a, b\rangle$ is a nontrivial dihedral subgroup of $G$. Moreover, as $G$ is simple, $D$ is a proper subgroup of $G$. Therefore, $(H, D, K)$ is a path in $\Delta_G$, and so $d(H,K) = 2$.

Now, without any assumptions on $|H|$ and $|K|$, suppose that $H$ and $K$ lie in maximal subgroups $L$ and $M$ of $G$, respectively, with $|L|$ and $|M|$ even. Then $H \sim L$ and $M \sim K$, and by the previous paragraph, $d(L,M) \leqslant 2$. Thus $d(H,K) \leqslant 4$.

If every maximal subgroup of $G$ has even order, then this holds for each pair of nontrivial proper subgroups of $G$, and so $\mathrm{diam}(\Delta_G) \leqslant 4$. □

Hence in order to prove Theorem 4.1.4, it suffices to consider the non-abelian finite simple groups with maximal subgroups of odd order. The following theorem, which will also be useful in Chapter 6, classifies these groups. This theorem is based on part of [95, Theorem 2], and incorporates more recent knowledge of the maximal subgroups of the monster group. Here, $(n, q)$ denotes an ordered pair consisting of an integer $n$ and a prime power $q$, and not the greatest common divisor of $n$ and $q$.

**Theorem 4.2.3.** *Let $G$ be a non-abelian finite simple group. Then $G$ contains a maximal subgroup of odd order if and only if $G$ is isomorphic to one of the following:*

(i) $A_p$, *with $p$ prime, $p \equiv 3 \pmod 4$ and $p \notin \{7, 11, 23\}$;*

(ii) $\mathrm{PSL}(2, q)$, *with $q$ a prime power and $q \equiv 3 \pmod 4$;*

(iii) $\mathrm{PSL}(n, q)$, *with $n$ an odd prime and $(n, q) \neq (3, 4)$;*

(iv) $\mathrm{PSU}(n, q)$, *with $n$ an odd prime and $(n, q) \notin \{(3, 3), (3, 5), (5, 2)\}$;*

(v) *the Mathieu group* $\mathrm{M}_{23}$*;*

(vi) *the Thompson group* Th*; or*

(vii) *the baby monster group* $\mathbb{B}$.

*Moreover, if $G$ is one of these groups, then $G$ has a unique conjugacy class of maximal subgroups of odd order.*

*Proof.* By Theorem 2 of [95] (see also the remark on p. 2778), each group in (i)–(vii) contains a unique conjugacy class of maximal subgroups of odd order. This theorem also states that if $G$ is any other non-abelian finite simple group containing a maximal subgroup $M$ of odd order, then $G$ is the monster group $\mathbb{M}$, and $M$ is one of two possible subgroups of $G$ (up to conjugacy): one of shape 59.29, and one of shape 71.35. However, these subgroups of $\mathbb{M}$ are not in fact maximal: the former subgroup lies in the maximal subgroup $\mathrm{L}_2(59)$ constructed in [79], and the latter lies in the maximal subgroup $\mathrm{L}_2(71)$ constructed in [80]. □

We are now able to prove this chapter's main theorem. In what follows, all information about the sporadic simple groups (including their maximal subgroups and the conjugacy classes and centraliser orders of their elements) is taken from the Atlas [42]; the list of corrections and additions to the Atlas given in [85,

Appendix 2]; and additional information from [149]. For the purpose of easy reference, Table 4.2.1 lists the maximal subgroups of the baby monster group (denoted using ATLAS notation) and their factorised orders, calculated using the maximal subgroup orders given in [147]. This table will also be useful in §6.3. Note that $|\mathbb{B}| = 2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$.

*Proof of Theorem 4.1.4.* By Lemma 4.2.2, we may assume that $G$ contains a maximal subgroup of odd order, i.e., that $G$ is a group listed in Theorem 4.2.3. Moreover, Lemma 4.2.1 implies that it suffices to show that the maximal distance in $\Delta_G$ between cyclic subgroups of prime order is 5 when $G \cong \mathbb{B}$; at most 5 when $G$ is a unitary group of odd prime dimension; and at most 4 otherwise.

Let $S_1$ and $S_2$ be cyclic subgroups of $G$ of prime order, and let $M_1$ and $M_2$ be maximal subgroups of $G$ that contain $S_1$ and $S_2$, respectively. If $|M_1|$ and $|M_2|$ are even, then $d(S_1, S_2) \leqslant 4$ by Lemma 4.2.2. We may therefore assume that $M_1$ belongs to the unique conjugacy class of maximal subgroups of $G$ mentioned in Theorem 4.2.3. In each case, [95, Theorem 2] yields the structure of $M_1$. Note however that $|M_2|$ may be even. We split the remainder of the proof into seven cases, corresponding to the groups listed in Theorem 4.2.3.

**Case (a)**: $G = A_p$, with $p$ prime, $p \equiv 3 \pmod 4$, and $p \notin \{7, 11, 23\}$. As mentioned in §4.1, Csákány and Pollák [48, Theorem 2] proved that the intersection graph of any simple alternating group has diameter at most 4 (see [126, Assertion I] for an alternative proof).

**Case (b)**: $G = \mathrm{PSL}(2, q)$, with $q$ a prime power and $q \equiv 3 \pmod 4$. By Proposition 3.1.6, $G$ acts transitively on the set $\Omega$ of one-dimensional subspaces of the vector space $\mathbb{F}_q^2$. Additionally, $M_1 = G_U$ for some $U \in \Omega$ (see [17, Table 8.1]), and by Proposition 3.2.2, $G_U \cap G_W \neq 1$ for each $W \in \Omega$. If $|M_2|$ is odd, then $M_2 = G_W$ for some $W$, and it follows that $M_1 \sim M_2$. Therefore, $S_1 \sim M_1 \sim M_2 \sim S_2$, and so $d(S_1, S_2) \leqslant 3$.

Assume now that $|M_2|$ is even, and let $g$ be an involution of $M_2$. By the previous paragraph, $g$ fixes no subspace in $\Omega$. However, $(U^g)^g = U^{g^2} = U$, and so $g \in G_{\{U,U^g\}}$. Since $G_U \cap G_{U^g}$ is nontrivial (by the previous paragraph) and lies in both $M_1 = G_U$ and $G_{\{U,U^g\}}$, we deduce that $S_1 \sim M_1 \sim G_{\{U,U^g\}} \sim M_2 \sim S_2$. Thus $d(S_1, S_2) \leqslant 4$.

**Case (c)**: $G = \mathrm{PSL}(n, q)$, with $n$ an odd prime, $q$ a prime power, and $G \ncong \mathrm{PSL}(3, 4)$. Similarly to the previous case, Proposition 3.1.6 shows that the group $G$ and its overgroup $R := \mathrm{PGL}(n, q)$ act transitively on the set $\Omega$ of one-dimensional subspaces of the vector space $V := \mathbb{F}_q^n$. Here, $M_1 = G \cap N_R(K)$, where $K$ is a Singer cycle of

Table 4.2.1: The maximal subgroups of the baby monster group and their factorised orders.

| Maximal subgroup | Factorised order |
|---|---|
| $2^{\cdot 2}E_6(2):2$ | $2^{38} \cdot 3^9 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$ |
| $2^{1+22}\cdot \mathrm{Co}_2$ | $2^{41} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$ |
| $\mathrm{Fi}_{23}$ | $2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$ |
| $2^{9+16}.\mathrm{PSp}(8,2)$ | $2^{41} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 17$ |
| Th | $2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$ |
| $(2^2 \times F_4(2)):2$ | $2^{27} \cdot 3^6 \cdot 5^2 \cdot 7^2 \cdot 13 \cdot 17$ |
| $2^{2+10+20}.(\mathrm{M}_{22}:2 \times S_3)$ | $2^{41} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11$ |
| $[2^{30}].\mathrm{PSL}(5,2)$ | $2^{40} \cdot 3^2 \cdot 5 \cdot 7 \cdot 31$ |
| $S_3 \times \mathrm{Fi}_{22}:2$ | $2^{19} \cdot 3^{10} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$ |
| $[2^{35}].(S_5 \times \mathrm{PSL}(3,2))$ | $2^{41} \cdot 3^2 \cdot 5 \cdot 7$ |
| $\mathrm{HN}:2$ | $2^{15} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$ |
| $\mathrm{P}\Omega^+(8,3):S_4$ | $2^{15} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 13$ |
| $3^{1+8}.2^{1+6}.\mathrm{PSU}(4,2).2$ | $2^{14} \cdot 3^{13} \cdot 5$ |
| $(3^2{:}D_8 \times \mathrm{PSU}(4,3).2.2).2$ | $2^{13} \cdot 3^8 \cdot 5 \cdot 7$ |
| $(5{:}4) \times (\mathrm{HS}{:}2)$ | $2^{12} \cdot 3^2 \cdot 5^4 \cdot 7 \cdot 11$ |
| $S_4 \times {}^2F_4(2)$ | $2^{15} \cdot 3^4 \cdot 5^2 \cdot 13$ |
| $[3^{11}].(S_4 \times 2S_4)$ | $2^7 \cdot 3^{13}$ |
| $S_5 \times \mathrm{M}_{22}:2$ | $2^{11} \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11$ |
| $(S_6 \times \mathrm{PSL}(3,4){:}2){:}2$ | $2^{12} \cdot 3^4 \cdot 5^2 \cdot 7$ |
| $5^{3\cdot}\mathrm{PSL}(3,5)$ | $2^5 \cdot 3 \cdot 5^6 \cdot 31$ |
| $5^{1+4}.2^{1+4}.A_5.4$ | $2^9 \cdot 3 \cdot 5^6$ |
| $(S_6 \times S_6).4$ | $2^{10} \cdot 3^4 \cdot 5^2$ |
| $5^2{:}4S_4 \times S_5$ | $2^8 \cdot 3^2 \cdot 5^3$ |
| $\mathrm{PSL}(2,49)\cdot 2_3$ | $2^5 \cdot 3 \cdot 5^2 \cdot 7^2$ |
| $\mathrm{PSL}(2,31)$ | $2^5 \cdot 3 \cdot 5 \cdot 31$ |
| $\mathrm{M}_{11}$ | $2^4 \cdot 3^2 \cdot 5 \cdot 11$ |
| $\mathrm{PSL}(3,3)$ | $2^4 \cdot 3^3 \cdot 13$ |
| $\mathrm{PSL}(2,17):2$ | $2^5 \cdot 3^2 \cdot 17$ |
| $\mathrm{PSL}(2,11):2$ | $2^3 \cdot 3 \cdot 5 \cdot 11$ |
| $47{:}23$ | $23 \cdot 47$ |

$R$, i.e., the projective version of a Singer cycle of $\mathrm{GL}(n,q)$ (see [83, pp.187–188] and [78, §1–2]). In particular, $K$ is a cyclic subgroup of order $(q^n-1)/(q-1)$.

Now, Lemma 2.5.13 and Proposition 2.5.14 show that $N_R(K)$ contains an element

$m$ whose preimage in $\mathrm{GL}(n,q)$ is conjugate to the companion matrix $C(x^n-1)$ (as in Definition 2.5.1), and $m$ fixes some subspace $X \in \Omega$. As $\det(C(x^n-1)) = (-1)^{n-1}$ and $n$ is odd, $m \in M_1$. Let $U \in \Omega$. Then, since the action of $K$ on $\Omega$ is transitive [78, p. 493], there exists $k \in K$ such that $U = X^k$. Observe also that $m^k \in M_1$, and that $(X^k)^{m^k} = X^k$. Therefore, if a non-identity element of $S_2$ fixes $U$, then $S_1 \sim M_1 \sim G_U \sim S_2$ and $d(S_1, S_2) \leqslant 3$.

Suppose now that no non-identity element of $S_2$ fixes a subspace in $\Omega$. Then each orbit of $S_2$ on $\Omega$ has size $|S_2|$, and so $|S_2|$ divides $|\Omega| = (q^n-1)/(q-1)$. We will show that $S_2$ acts irreducibly on $V$. Suppose for a contradiction that $S_2$ stabilises an $\ell$-dimensional subspace $W$ of $V$, with $1 < \ell < n$. Then no non-identity element of $S_2$ stabilises a one-dimensional subspace of $W$, and so $|S_2|$ divides $(q^\ell-1)/(q-1)$. Thus $|S_2|$ divides the greatest common divisor of $(q^\ell-1)/(q-1)$ and $(q^n-1)/(q-1)$, which is equal to $(q^{(\ell,n)}-1)/(q-1)$. As $n$ is prime, this is equal to 1, contradicting the fact that $|S_2| > 1$. Therefore, $S_2$ acts irreducibly on $V$.

Recall from Proposition 2.5.14 that $Z(\mathrm{GL}(n,q))$ lies in each Singer cycle of $\mathrm{GL}(n,q)$. Thus it follows from Proposition 2.5.15 that any given preimage of $S_2$ in $\mathrm{SL}(n,q)$ lies in a Singer cycle of $\mathrm{GL}(n,q)$. The Singer cycles of $\mathrm{GL}(n,q)$ are all conjugate by Proposition 2.5.12, and so there exists some $g \in R$ such that $S_2 \leqslant G \cap N_R(K^g) = M_1^g \leqslant G$. In fact, since $M_1^g$ and $M_1$ both have odd order, they are conjugate in $G$ by Theorem 4.2.3. It follows from above that both $M_1$ and $M_1^g$ are adjacent in $\Delta_G$ to $G_U$, for each $U \in \Omega$. Hence $S_1 \sim M_1 \sim G_U \sim M_1^g \sim S_2$ and $d(S_1, S_2) \leqslant 4$.

**Case (d)**: $G = \mathrm{PSU}(n,q)$, with $n$ an odd prime and $q$ a prime power, and $G \notin \{\mathrm{PSU}(3,3), \mathrm{PSU}(3,5), \mathrm{PSU}(5,2)\}$. Here, $G$ acts on the set of one-dimensional subspaces of the vector space $V := \mathbb{F}_{q^2}^n$. However, this action is intransitive, as the non-degenerate and totally singular subspaces lie in separate orbits. The maximal subgroup $M_1$ is equal to $N_G(T)$, where $T$ is a Singer cycle of $G$, i.e., a cyclic subgroup of order $\frac{q^n+1}{(q+1)(q+1,n)}$ (see [78, §5]). By Proposition 2.2.10, we may assume that $V$ is equipped with a unitary form whose Gram matrix is the $n \times n$ identity matrix. It then follows from Lemma 2.2.6 that $G$ contains an element $x$ whose preimage in $\mathrm{SU}(n,q)$ is equal to $C(x^n-1)$. Furthermore, $M_1$ contains a $G$-conjugate $m$ of $x$ (see [78, p. 512]). As in Case (c), it follows from Lemma 2.5.13 that $m$ fixes some subspace $X \in \Omega$.

Let $L := G_X$. Then $S_1 \sim M_1 \sim L$, and we can calculate $|L|$ using [17, §1.6.4, Table 2.3]. In particular, $|L|$ is even. Hence if $|M_2|$ is even, then $d(L, M_2) \leqslant 2$ by Lemma 4.2.2. As $M_2 \sim S_2$, it follows that $d(S_1, S_2) \leqslant 5$. If instead $|M_2|$ is odd, then there exists an element $g \in G$ such that $M_2 = M_1^g$. Thus $L^g \sim M_2$. As $G$ is not

isomorphic to the non-simple group $\mathrm{PSU}(3,2)$, Theorem 3.5.1 shows that $L \cap L^g \neq 1$. Therefore, $S_1 \sim M_1 \sim L \sim L^g \sim M_2 \sim S_2$, and again $d(S_1, S_2) \leqslant 5$.

**Case (e)**: $G = \mathrm{M}_{23}$. In this case, $M_1$ has shape 23:11. We argue as in the proof of [126, Assertion I]. There exists a maximal subgroup $L$ of $G$ isomorphic to $\mathrm{M}_{22}$, and $|M_1|\,|L|$ and $|M_2|\,|L|$ are both greater than $|G|$ (for any choice of $M_2$). Thus $M_1 \cap L$ and $M_2 \cap L$ are both nontrivial. We conclude that $S_1 \sim M_1 \sim L \sim M_2 \sim S_2$, and so $d(S_1, S_2) \leqslant 4$.

**Case (f)**: $G = \mathrm{Th}$. Here, $M_1$ has shape 31:15. If the nontrivial proper subgroup $S_1$ of $M_1$ has order 31, then $S_1$ lies in a maximal subgroup of shape $2^5{\cdot}\mathrm{L}_5(2)$. Otherwise, $|C_G(S_1)|$ is even. Therefore, in each case, $S_1$ lies in a maximal subgroup of even order. The same is true for $S_2$, and thus $d(S_1, S_2) \leqslant 4$ by Lemma 4.2.2.

**Case (g)**: $G = \mathbb{B}$. In this case, $M_1$ has shape 47:23. Let $H$ be a subgroup of $M_1$ of order 23. Then $H$ is a Sylow 23-subgroup of $G$. Additionally, $G$ has a maximal subgroup $K \cong \mathrm{Fi}_{23}$, which has even order, and contains a conjugate of $H$. Conjugating $K$ if necessary, we may assume that $H \leqslant K$, and so $S_1 \sim M_1 \sim K$. Hence if $|M_2|$ is even, then $d(K, M_2) \leqslant 2$ by Lemma 4.2.2. As $M_2 \sim S_2$, it follows that $d(S_1, S_2) \leqslant 5$. If instead $|M_2|$ is odd, then there exists an element $g \in G$ such that $M_2 = M_1^g$, and hence $K^g \sim M_2$. As $|K|^2/|G| > 1$ (see Table 4.2.1), we conclude that $S_1 \sim M_1 \sim K \sim K^g \sim M_2 \sim S_2$ and $d(S_1, S_2) \leqslant 5$. Thus $\mathrm{diam}(\Delta_G) \leqslant 5$.

To complete the proof, we will show that $\mathrm{diam}(\Delta_G) \geqslant 5$. Each maximal subgroup of $G$ that contains $H$ is conjugate either to $M_1$, to $K$, or to a subgroup $L$ of shape $2^{1+22}{\cdot}\mathrm{Co}_2$. Conjugating $L$ if necessary, we may assume that $H \leqslant M_1 \cap K \cap L$. Additionally, $N_G(H)$ has shape $(23{:}11) \times 2$ and $N_L(H) = N_G(H)$, while $|N_G(H) : N_{M_1}(H)| = 22$. Furthermore, the 22 non-identity elements of $H$ fall into two $K$-conjugacy classes, and $C_K(H) = H$. It follows from the Orbit-Stabiliser Theorem that $N_K(H)$ has shape 23:11, and so $|N_G(H) : N_K(H)| = 2$.

Consider now the pairs $(M', H')$, where $M'$ is a $G$-conjugate of $M_1$, $H'$ is a $G$-conjugate of $H$, and $H' \leqslant M'$. Observe that there are exactly $|G : M_1|$ choices for $M'$, and for any fixed $M'$, there are exactly $|M_1 : N_{M_1}(H)|$ choices for $H'$ (since $H$ is a Sylow subgroup of $G$). Thus there are exactly $|G : N_{M_1}(H)|$ of these pairs. Additionally, $G$ contains exactly $|G : N_G(H)|$ subgroups conjugate to $H$. As any two of these conjugate subgroups appear in an equal number of pairs, we deduce that $H$ lies in exactly $|N_G(H) : N_{M_1}(H)| = 22$ $G$-conjugates of $M_1$. Similarly, $H$ lies in two $G$-conjugates of $K$ and one $G$-conjugate of $L$.

As $M_1$ has shape 47:23, it contains a subgroup $S$ of order 47. In fact, each maximal subgroup of $G$ whose order is divisible by 47 is conjugate to $M_1$, and it follows that $M_1$ is the unique maximal subgroup of $G$ that contains $S$. Hence if $J$

is a maximal subgroup of $G$ satisfying $J \cap M_1 \neq 1$, then $J$ contains a $G$-conjugate of $H$. Let $\mathcal{U}$ be the set of $G$-conjugates of $H$ that lie in at least one such maximal subgroup $J$ (with $J = M_1$ allowed). There are 47 subgroups of order 23 in $M_1$, each of which lies in two $G$-conjugates of $K$, and there are $|K : N_K(H)|$ subgroups of order 23 in $K$. Therefore, there are fewer than $47 \cdot 2|K : N_K(H)|$ subgroups in $\mathcal{U}$ that lie in at least one $G$-conjugate of $K$. By considering the $G$-conjugates of $M_1$ and $L$ similarly, we conclude that

$$|\mathcal{U}| < 47(2|K : N_K(H)| + 22 \cdot 47 + |L : N_L(H)|) < |G : M_1|/22. \tag{4.2.1}$$

Recall from above that each $G$-conjugate of $H$ lies in exactly 22 $G$-conjugates of $M_1$. Hence the number of $G$-conjugates of $M_1$ containing subgroups in $\mathcal{U}$ is less than $22|\mathcal{U}|$, which is less than $|G : M_1|$ by (4.2.1). We conclude that there exists $g \in G$ such that no subgroup of $M_1^g$ lies in $\mathcal{U}$. This means that $M_1$ and $M_1^g$ are not adjacent in $\Delta_G$ and have no common neighbours, and so $d(M_1, M_1^g) > 2$. Since $S$ is maximal in $M_1$, and no other maximal subgroup of $G$ contains $S$, we observe that $M_1$ is the unique neighbour of $S$ in $\Delta_G$. Similarly, $M_1^g$ is the unique neighbour of $S^g$, and it follows that $d(S, S^g) > 4$. Therefore, $\mathrm{diam}(\Delta_G) = 5$. □

We can in fact say more about the vertices of $\Delta_{\mathbb{B}}$ that witness the maximal distance of 5.

**Proposition 4.2.4.** *Suppose that $G = \mathbb{B}$, and let $S_1$ and $S_2$ be nontrivial proper subgroups of $G$ such that $d(S_1, S_2) = 5$. Then $S_1$ and $S_2$ are (conjugate) subgroups of order 47.*

*Proof.* By Lemma 4.2.2, we may assume that $S_1$ lies in no maximal subgroup of $G$ of even order. Then $S_1$ is either a member of the unique $G$-conjugacy class of cyclic subgroups of order 47, or a maximal subgroup of $G$ of shape 47:23. As mentioned in the proof of Theorem 4.1.4, each subgroup $T$ of $G$ of order 47 lies in a unique maximal subgroup $F$ of $G$, of shape 47:23, and $F$ is the unique neighbour in $\Delta_G$ of $T$. Hence if $S_2 \neq T$, then $d(F, S_2) < d(T, S_2)$. We may therefore assume that $|S_1| = 47$. We will write $M_1$ to denote the neighbour of $S_1$ of shape 47:23.

It remains to show that $d(S_1, S_2) < 5$ when $|S_2| \neq 47$. Note that if $S_2$ is not cyclic of prime order, then, as in the proof of Lemma 4.2.1, $d(S_1, S_2) \leqslant d(S_1, C)$ for each cyclic subgroup $C$ of $S_2$ of prime order. Hence we may assume that $S_2$ itself is cyclic of prime order, and so $|S_2| \in \{2, 3, 5, 7, 11, 13, 17, 19, 23, 31\}$.

As we stated in the proof of Theorem 4.1.4, $M_1$ contains a Sylow 23-subgroup $H$ of $G$, and $H$ lies in a maximal subgroup $L$ of $G$ of shape $2^{1+22}{\cdot}\mathrm{Co}_2$. Let $\mathcal{R}$ be the set of maximal subgroups $R$ of $G$ with $|L|\,|R| > |G|$ (up to $G$-conjugacy,

these are the first twelve subgroups in Table 4.2.1). Any subgroup $R \in \mathcal{R}$ satisfies $L \cap R \neq 1$. Hence it suffices to show that $S_2$ lies in a subgroup $R \in \mathcal{R}$, as in this case $S_1 \sim M_1 \sim L \sim R \sim S_2$ (or $S_1 \sim M_1 \sim L \sim S_2$ if $L = R$) and $d(S_1, S_2) \leqslant 4$.

If $|S_2| \geqslant 7$, then there is a unique $G$-conjugacy class of cyclic subgroups of order $|S_2|$, and $\mathcal{R}$ contains a maximal subgroup of $G$ whose order is divisible by $|S_2|$. Thus we can set $R$ to be some conjugate of this maximal subgroup. If instead $|S_2| = 2$, then $|L|\,|C_G(S_2)| > |G|$, and so we can set $R$ to be any maximal subgroup containing $C_G(S_2)$.

Suppose finally that $|S_2| \in \{3, 5\}$. Then there are four choices for $S_2$ up to $G$-conjugacy: $S_{3\mathrm{A}}$, $S_{3\mathrm{B}}$, $S_{5\mathrm{A}}$ and $S_{5\mathrm{B}}$, where the subscript is the label in the Atlas for the $G$-conjugacy class of a generator for $S_2$. If $S_2$ is conjugate to $S_{3\mathrm{A}}$, then we may set $R = N_G(S_2)$. We also observe that each cyclic subgroup of $G$ of order 9, 35 or 25 contains a $G$-conjugate of $S_{3\mathrm{B}}$, $S_{5\mathrm{A}}$ or $S_{5\mathrm{B}}$, respectively. As the simple group HN contains cyclic subgroups of order 25, while ${}^2E_6(2)$ contains cyclic subgroups of order 9 and 35, we can choose $R$ to be an appropriate maximal subgroup of $G$ of shape HN:2 or $2.{}^2E_6(2)$:2. □

We complete this chapter by proving Proposition 4.1.5.

*Proof of Proposition 4.1.5.* We split the proof into three cases.

**Case (a)**: $k = 3$. Let $G := \mathrm{PSU}(3, 3)$. Note that each maximal subgroup of $G$ has even order by Theorem 4.2.3, and so $\mathrm{diam}(\Delta_G) \leqslant 4$ by Lemma 4.2.2. In fact, if $M_1$ and $M_2$ are maximal subgroups of $G$, then $|M_1|\,|M_2| > |G|$ [42, p. 14], and so $M_1 \sim M_2$. Hence if $S_1$ and $S_2$ are nontrivial proper subgroups of $G$ that are not maximal, and if $M_1$ and $M_2$ are maximal subgroups containing $S_1$ and $S_2$, respectively, then either $S_1 \sim M_1 \sim S_2$ or $S_1 \sim M_1 \sim M_2 \sim S_2$. It follows immediately that $\mathrm{diam}(\Delta_G) \leqslant 3$. As the intersection graph of any non-abelian finite simple group has diameter at least 3 by Theorem 4.1.3, we conclude that $\mathrm{diam}(\Delta_G) = 3$.

**Case (b)**: $k = 4$. Let $G := \mathrm{PSU}(3, 7)$, and let $S_1$ and $S_2$ be nontrivial proper subgroups of $G$. To show that $\mathrm{diam}(\Delta_G) = 4$, it suffices by Lemmas 4.2.1 and 4.2.2 to show that 4 is the maximum distance between $S_1$ and $S_2$ when $S_1$ and $S_2$ are cyclic of prime order, and when $S_1$ lies in no maximal subgroup of $G$ of even order. In what follows, all information about the subgroups and elements of $G$ follows from [42, pp. 66–67], except where stated otherwise. In particular, $|S_1| = 43$, and the unique neighbour of $S_1$ in $\Delta_G$ is a maximal subgroup $M_1$ of shape 43:3. Additionally, any subgroup $H$ of $M_1$ of order 3 is a Sylow subgroup of $G$, and $H$ lies in a maximal

subgroup $L$ of $G$ of order 16464. Note that for each $M \in \{M_1, L\}$, there is a unique conjugacy class in $G$ of maximal subgroups of order $|M|$.

Next, let $M_2$ be a $G$-conjugate of $L$ containing $S_2$ if $|S_2| = 3$, and otherwise let $M_2$ be a maximal subgroup of $G$ containing $C_G(S_2)$. Note that if $|S_2| = 7$, then 49 divides $|C_G(S_2)|$, and so $M_2$ is a $G$-conjugate of $L$. In general, if $|S_2| \neq 43$, then $|M_2|\,|L| > |G|$, and so $M_2 \cap L \neq 1$. Thus in this case, $S_1 \sim M_1 \sim L \sim M_2 \sim S_2$ (or $S_1 \sim M_1 \sim L \sim S_2$ if $L = M_2$), and so $d(S_1, S_2) \leqslant 4$. Assume therefore that $|S_2| = 43$. Then there exists $x \in G$ such that $S_2 = S_1^x$ and $M_2 = M_1^x$. The Magma code in `psu37` shows that, for each $g \in G$, either $M_1 \cap M_1^g \neq 1$, or there exists a $G$-conjugate of $L$ that intersects nontrivially with both $M_1$ and $M_1^g$. Hence in either case, $d(S_1, S_1^g) \leqslant 4$.

Now, $M_1$ is not a direct product of $S_1$ and $H$, and so $N_{M_1}(H) = H$. Additionally, we observe from the aforementioned Magma code that $|N_G(H)| = 96$. Therefore, $H$ lies in $|N_G(H) : N_{M_1}(H)| = 32$ $G$-conjugates of $M_1$. As there are 43 $G$-conjugates of $H$ in $M_1$, and the index of $M_1$ in $G$ is greater than $43 \cdot 96$, it follows that there exists $g \in G$ such that $M_1 \cap M_1^g = 1$. Hence $d(S_1, S_1^g) \geqslant 4$. We therefore conclude that $\mathrm{diam}(\Delta_G) = 4$.

**Case (c)**: $k = 5$. Let $G := \mathrm{PSU}(7, 2)$. Using certain Magma computations[1] from `psu72`, we can adapt the proof of Theorem 4.1.4(ii) to show that $\mathrm{diam}(\Delta_G) = 5$, as follows. First, these computations show that each maximal subgroup of $G$ of odd order has shape 43:7, that each subgroup of $G$ of order 43 lies in no maximal subgroup of even order, and that a Sylow 7-subgroup of $G$ has order 7. Now, let $M$ be a maximal subgroup of $G$ of shape 43:7, and let $S$ and $H$ be subgroups of $M$ of order 43 and 7, respectively. Additionally, let $\mathcal{U}$ be the set of $G$-conjugates of $H$ that lie in $M$ or in a neighbour of $M$ in $\Delta_G$. We see using Magma that $|\mathcal{U}|$ is less than the ratio between $|G : M|$ and the number of $G$-conjugates of $M$ containing $H$. As in the proof of Theorem 4.1.4(ii), we deduce that there exists $g \in G$ such that $d(M, M^g) > 2$, and so $d(S, S^g) > 4$. Therefore, $\mathrm{diam}(\Delta_G) = 5$ by Theorem 4.1.4(i). □

Note that $\Delta_{\mathrm{PSU}(3,7)}$ has diameter 4 even though $\mathrm{PSU}(3, 7)$ is a unitary group of odd prime dimension that contains a maximal subgroup of odd order. In general, the following question is open.

**Question 4.2.5.** *For each $k \in \{3, 4, 5\}$, which finite simple unitary groups of odd prime dimension have an intersection graph of diameter $k$?*

[1] Note that the additional computations in this file are only used in the proof of Theorem 6.5.1, and that the notation used in this code does not in general correspond with the notation used here.

# Chapter 5

# The non-commuting, non-generating graph of a group: general results and groups with non-simple central quotients

## 5.1 Background and the main theorem

In this chapter, we introduce the non-commuting, non-generating graph of a group $G$, prove general results about this graph, and investigate in detail its connectedness and diameter in the case where $G$ is not a central extension of a non-abelian simple group. In Chapter 6, we focus on the case where $G$ is a (central extension of a) non-abelian finite simple group. In general, we do not consider infinite simple groups in this thesis, but we will be able to briefly discuss these groups in certain easy cases.

We continue to use the graph theoretic notation summarised at the beginning of Chapter 4. In addition, throughout this chapter, $G$ denotes an arbitrary group, except where specified otherwise.

First, we define a few important graphs related to groups, including the non-commuting, non-generating graph.

**Definition 5.1.1** ([98, p. 55])**.** The *generating graph* of $G$ is the graph with vertices $G \setminus \{1\}$, and with two vertices $x$ and $y$ adjacent if and only if $\langle x, y \rangle = G$.

Note that although this graph was originally defined in [98, p. 55] with vertex set $G$, it is common to delete the identity element from its vertex set (see, e.g., [24, Definition 3.13]), as this vertex would otherwise be isolated whenever $G$ is not cyclic.

We will also formally define the complement of the generating graph of $G$. In §6.5, we will prove a theorem about the diameter of this complement when $G$ is a non-abelian finite simple group.

**Definition 5.1.2.** The *non-generating graph* of $G$ is the graph with vertices $G \setminus \{1\}$, and with two vertices $x$ and $y$ adjacent if and only if $\langle x, y \rangle \neq G$.

Next, we define the graph that is the focus of the remainder of this thesis.

**Definition 5.1.3.** The *non-commuting, non-generating graph* of $G$, denoted by $\Xi(G)$, is the graph with vertices $G \setminus Z(G)$, and with two vertices $x$ and $y$ adjacent if and only if $[x, y] \neq 1$ and $\langle x, y \rangle \neq G$. We will write $\Xi^+(G)$ to denote the subgraph of $\Xi(G)$ induced by its non-isolated vertices.

Similarly to the exclusion of the identity from the vertex set of the generating graph, we do not include any central elements of $G$ in the vertex set of $\Xi(G)$, as these would always be isolated. It is also clear that $\Xi(G)$ is the empty graph if and only if $G$ is abelian. We will therefore often assume that $G$ is non-abelian.

As mentioned in §1.0.2, both the generating graph of $G$ and $\Xi(G)$ are the differences between subsequent graphs in the hierarchy of graphs defined in [34, §2.6]. In particular, with the appropriate vertices deleted in each case, the generating graph is the difference between the complete graph on $G$ and the non-generating graph of $G$, while $\Xi(G)$ is the difference between the non-generating graph of $G$ and the *commuting graph* of $G$, where two vertices are adjacent if and only if they commute. The complement of this graph will be very important when studying the structure of $\Xi(G)$.

**Definition 5.1.4** ([1])**.** The *non-commuting graph* of $G$ is the graph with vertices $G \setminus Z(G)$, and with two vertices $x$ and $y$ adjacent if and only if $[x, y] \neq 1$.

Again, central vertices are not included in the vertex set of this graph, as they would otherwise always be isolated. Notice that the edge set of $\Xi(G)$ is the intersection of the edge sets of the non-commuting graph of $G$ and the non-generating graph of $G$.

We now present a theorem summarising the main results of this chapter. Here, and throughout the chapter, we consider primitivity as an abstract group property, as in Definition 2.1.22. Recall also that a minimal non-abelian group is a non-abelian group with all proper subgroups abelian.

**Theorem 5.1.5.** *Suppose that $\overline{G} := G/Z(G)$ is not simple. Then (at least) one of the following holds.*

(i) *$\Xi(G)$ has no vertices. This occurs if and only if $G$ is abelian.*

(ii) *$\Xi(G)$ has vertices but no edges. This occurs if and only if $G$ is minimal non-abelian.*

(iii) *$\Xi(G)$ has an isolated vertex, and $\Xi^+(G)$ is connected with diameter 2. If $\overline{G}$ has a proper non-cyclic quotient, then $G$ is soluble.*

(iv) *$\Xi(\overline{G})$ has an isolated vertex, $\Xi^+(G)$ is connected with diameter at most 4, and the subgraph of $\Xi(G)$ induced by the vertices in*

$$\{g \in G \setminus Z(G) \mid Z(G)g \in \Xi^+(\overline{G})\}$$

*is connected with diameter at most $\operatorname{diam}(\Xi^+(\overline{G}))$, which is equal to 2 or 3. Additionally, $\overline{G}$ is an insoluble primitive group with every proper quotient cyclic.*

(v) *$\Xi(G)$ is connected with diameter 2 or 3.*

(vi) *$\Xi(G)$ is connected with diameter 4, $G$ is infinite, and $\overline{G}$ has a proper non-cyclic quotient.*

(vii) *$\Xi(G)$ has exactly two connected components, each of diameter 2. If $G$ is finite, then this occurs if and only if $G$ has exactly two conjugacy classes of maximal subgroups, and nontrivial Sylow subgroups $P$ and $Q$ such that $\Phi(P) = Z(P) \not\leqslant Z(G)$, $Q$ is cyclic, and the unique maximal subgroup of $Q$ is normal in $G$; in particular, $G$ is soluble.*

This theorem supports our claim in §1.0.2 that the diameter of $\Xi(G)$ is often very small. However, we will see that there exist finite groups $G$ such that $\Xi(G)$ is connected with diameter larger than 2. This is not the case for the generating graph of a finite group, which, as we mentioned in §1.0.2, was recently proved to have diameter at most 2 whenever it is connected [22, Corollary 6]. It is an open question whether there exists a group $G$ satisfying case (iv) or case (vi) of the above theorem. In particular, we do not know if the diameter of $\Xi(G)$ (or $\Xi^+(G)$) can be equal to 4 when $G/Z(G)$ is not simple. However, we will see in Chapter 6 that there exist finite simple groups $G$ such that $\operatorname{diam}(\Xi(G)) = 4$.

Note also that in §5.7–5.9, we provide a more detailed structural description of the finite groups mentioned in Theorem 5.1.5(vii). We will see that more can also be said about the structure of an infinite group $G$ such that $\Xi(G)$ has two nontrivial connected components.

The remainder of this chapter is structured as follows. In §5.2, we prove general useful results about the graph $\Xi(G)$, and we discuss the isolated vertices of the graph in detail in §5.3. Next, in §5.4, we consider groups that contain normal maximal subgroups and the non-commuting, non-generating graphs of these groups. In particular, we determine the possible diameters of $\Xi(G)$ and $\Xi^+(G)$ when every

maximal subgroup of $G$ is normal; this of course includes the case where $G$ is nilpotent. We then explore in §5.5 the non-commuting, non-generating graph of a direct product of groups. The results here allow us to prove in §5.6 a detailed relationship between the structures of $G$ and $\Xi(G)$ when $G$ is a finite nilpotent group (note that these specific details are not included in Theorem 5.1.5 above). Our study of groups $G$ with normal maximal subgroups continues in §5.7, with detailed results about distances between certain pairs of vertices of $\Xi(G)$. We then complete the proof of Theorem 5.1.5 in §5.8, where $G$ is assumed to have a non-central normal subgroup with a corresponding non-cyclic quotient, and in §5.9, where $G/Z(G)$ is assumed to be non-simple with every proper quotient cyclic. Finally, in §5.10, we consider the structure of $\Xi(G)$ for certain infinite groups $G$, namely, free products of groups.

## 5.2 General results

In this section, we prove general results about the non-commuting, non-generating graph $\Xi(G)$ of the group $G$. Many of these results will be useful throughout this chapter and the next, though a few are only stated for the purpose of general interest. We also consider briefly the non-commuting graph of $G$ and the non-generating graph of $G$. Throughout this chapter, for vertices $x$ and $y$ of $\Xi(G)$, we write $d(x, y) := d_{\Xi(G)}(x, y)$ when the underlying group is evident. Similarly, we write $x \sim y$ in place of $x \sim_{\Xi(G)} y$.

Our first two results highlight useful symmetries of $\Xi(G)$ and the non-commuting graph of $G$.

**Proposition 5.2.1.** *Let $\Gamma$ be equal to the non-commuting graph of $G$, or to $\Xi(G)$. Additionally, let $x, y \in G$, and suppose that $\langle x \rangle = \langle y \rangle$. Then $x$ and $y$ have the same set of neighbours in $\Gamma$.*

*Proof.* As $x$ and $y$ are powers of each other, we observe that $C_G(x) = C_G(y)$, and $\langle x, g \rangle = \langle y, g \rangle$ for each $g \in G$. Therefore, $\{x, g\}$ is an edge of $\Gamma$ if and only if $\{y, g\}$ is an edge. In addition, $[x, y] = 1$, and so $\{x, y\}$ is not an edge of $\Gamma$. □

**Proposition 5.2.2.** *Let $\Gamma$ be equal to the non-commuting graph of $G$, or to $\Xi(G)$. Additionally, let $x, y \in G$, and suppose that $\{x, y\}$ is an edge of $\Gamma$. Then $x$ is adjacent in $\Gamma$ to each element of the double coset $\langle x \rangle y \langle x \rangle$.*

*Proof.* Let $g \in \langle x \rangle y \langle x \rangle$, so that $g = x^i y x^j$ for some $i, j \in \mathbb{Z}$. Then $\langle x, g \rangle = \langle x, y \rangle$. Thus if $\Gamma = \Xi(G)$, then $\langle x, g \rangle$ is a proper subgroup of $G$. Additionally, since $\{x, y\}$ is an edge of $\Gamma$, we see that $y \notin C_G(x)$. As $x \in C_G(x)$, it follows that $\langle x \rangle y \langle x \rangle \cap C_G(x) = \varnothing$. Thus $\{x, g\}$ is an edge of $\Gamma$, as required. □

Now, the *spread* of a graph $\Gamma$ is the largest value $k$ such that the vertices in each $k$-subset of $\Gamma$ have a common neighbour, if such $k$ exists. It is clear that $\Gamma$ has nonzero spread if and only if it has no isolated vertices, and that if $\Gamma$ has spread at least 2, then $\mathrm{diam}(\Gamma) \leqslant 2$.

As we mentioned in §1.0.2, Burness, Guralnick and Harper [22, Corollary 6] recently proved that the generating graph of a finite group has diameter at most 2 whenever it is connected. In fact, they proved a stronger result: whenever this graph is connected (and has more than one vertex), its spread is at least 2 [22, Theorem 1]. This result was proved over several papers, using the classification of finite simple groups.

In the case of the non-commuting, non-generating graph, however, it is much easier to show that "diameter at most 2" is equivalent to "spread at least 2".

**Corollary 5.2.3.** *Suppose that $\Xi(G)$ has an edge. Then $\Xi(G)$ has spread at least 2 if and only if its diameter is at most 2.*

*Proof.* As above, the forward direction is clear. Suppose therefore that $\Xi(G)$ has diameter at most 2, and let $x, y \in G \setminus Z(G)$. If $d(x, y) = 2$, then there is a third vertex adjacent to each of $x$ and $y$. Otherwise, Proposition 5.2.2 shows that $x$ and $y$ have the common neighbour $xy$. Hence $\Xi(G)$ has spread at least 2. □

We will not address the spread of $\Xi(G)$ further in this thesis, except to point out that it can be rather large. For example, the Magma code in `psu32_spread` shows that if $G$ is the (soluble) unitary group $\mathrm{PSU}(3, 2)$ of order 72, then $\Xi(G)$ has spread 9. Further investigation of the spread of the non-commuting, non-generating graph of a group would likely be very interesting.

Proposition 5.2.2 also yields the following corollary regarding the *girth* of $\Xi(G)$, i.e., the length of its shortest cycle.

**Corollary 5.2.4.** *If $\Xi(G)$ has an edge, then it has girth 3.*

*Proof.* Let $\{x, y\}$ be an edge of $\Gamma$. Proposition 5.2.2 shows that $xy$ is adjacent in $\Gamma$ to each of $x$ and $y$. Hence $\Gamma$ contains the triangle $(x, y, xy)$. □

Note that, using similar arguments, Abdollahi, Akbari and Maimani [1, Proposition 2.1] proved a corresponding result about the girth of the non-commuting graph of $G$, as well as the following two propositions (with $\Gamma$ equal to the non-commuting graph in the former proposition).

**Proposition 5.2.5.** *Let $\Gamma$ be equal to the non-commuting graph of $G$, or to $\Xi(G)$. Then no connected component of $\Gamma$ has diameter 1.*

*Proof.* Suppose for a contradiction that $\Gamma$ has a connected component $X$ of diameter 1. Then $|X| \geqslant 2$, and so there exist distinct elements $x, y \in X$, and $x \sim y$. Proposition 5.2.2 then implies that $x \sim xy$, and so $xy \in X$.

Now, if $h \in X$ satisfies $h^{-1} \neq h$, then Proposition 5.2.1 implies that $h^{-1} \in X$. However, $[h, h^{-1}] = 1$, and so $h \not\sim h^{-1}$. As $X$ has diameter 1, we deduce that each element of $X$ is an involution. This implies that $[x, y] = (xy)^2 = 1$, and so in fact $x \not\sim y$, a contradiction. □

In the following proposition, and several times throughout this chapter, we use the elementary observation that the union of two proper subgroups of $G$ is a proper subset of $G$.

**Proposition 5.2.6.** *Suppose that $G$ is non-abelian. Then the non-commuting graph of $G$ is connected with diameter 2.*

*Proof.* By Proposition 5.2.5, it suffices to show that the non-commuting graph of $G$ is connected with diameter at most 2. Let $x, y \in G \setminus Z(G)$. Then $C_G(x)$ and $C_G(y)$ are each proper subgroups of $G$, and so there exists $g \in G \setminus (C_G(x) \cup C_G(y))$. Thus $(x, g, y)$ is a path in the non-commuting graph of $G$, and the result follows. □

Observe that if $G$ is non-abelian and not 2-generated, then $\Xi(G)$ is equal to the non-commuting graph of $G$. Hence we obtain the following.

**Corollary 5.2.7.** *Suppose that $G$ is non-abelian and not 2-generated. Then $\Xi(G)$ is connected with diameter 2.*

We note that, while each non-abelian finite simple group is 2-generated by Theorem 2.4.4, the same is not true for infinite simple groups in general. For example, consider the infinite alternating group, i.e., the group of even permutations (products of an even number of transpositions) of $\mathbb{Z}$. It is well known that this group is simple (see, e.g., [44, Lemma 2.3]), and it is easy to see that it is not finitely generated. Furthermore, the main theorem of [66] shows that there exist infinite simple groups that are finitely generated but not 2-generated. By Corollary 5.2.7, $\operatorname{diam}(\Xi(G)) = 2$ for each infinite simple group $G$ that is not 2-generated.

We can also use Proposition 5.2.6 to deduce the following corollary, which we will use many times throughout the remainder of this thesis.

**Corollary 5.2.8.** *Let $H$ be a proper non-abelian subgroup of $G$. The subgraph of $\Xi(G)$ induced by the vertices corresponding to $H \setminus Z(H)$ is connected with diameter 2.*

*Proof.* Since any two elements of $H$ generate a subgroup of $H$, which is proper in $G$, the subgraph of $\Xi(G)$ induced by the vertices corresponding to $H \setminus Z(H)$ is the non-commuting graph of $H$. Hence Proposition 5.2.6 yields the result. □

Next, we describe the structure of a finite group whose non-commuting, non-generating graph has a vertex that is adjacent to all other vertices.

**Proposition 5.2.9.** *Suppose that $G$ is finite. Then $\Xi(G)$ has a vertex that is adjacent to all other vertices if and only if $G$ is a Frobenius group $N{:}H$, where $N$ is a non-cyclic abelian group of odd order, $|H| = 2$, and the involution of $H$ acts on $N$ by inversion. Furthermore, no such Frobenius group $N{:}H$ is 2-generated, and hence $\Xi(N{:}H)$ is equal to the non-commuting graph of $N{:}H$.*

*Proof.* Assume first that $\Xi(G)$ has a vertex $x$ that is adjacent to all other vertices. Then $x \in G \setminus Z(G)$, $C_G(x) = Z(G) \cup \{x\}$, and $\langle x, y\rangle < G$ for all $y \in G \setminus C_G(x)$. In particular, the disjoint union of $Z(G)$ and $\{x\}$ is a subgroup of $G$, which means that $Z(G) = 1$ and $|x| = 2$.

Now, let $H$ be a 2-subgroup of $G$ containing $x$. Then $Z(H) > 1$. As $C_G(x) = \langle x\rangle$, we deduce that $Z(H) = \langle x\rangle$, and then that $H = \langle x\rangle$. Hence $\langle x\rangle$ is a Sylow 2-subgroup of $G$, and in particular, each involution of $G$ is conjugate to $x$. Additionally, $G$ has twice odd order.

Next, considering $G$ as a permutation group acting regularly on itself, let $N$ be the subgroup of $G$ of even permutations. Since $G$ is regular, $x$ is a product of $|G|/2$ disjoint transpositions. As $|G|/2$ is odd, $x$ is an odd permutation. Thus $N$ has index 2 in $G$, and is therefore normal of odd order.

Since $C_G(x) = \langle x\rangle$, no non-identity element of $N$ is fixed by $x$ under conjugation. Hence $G$ is equal to $N{:}H$, and is a Frobenius group by Definition 2.1.18. Moreover, [65, p. 3] shows that $N$ is abelian and that $x$ acts on $N$ by inversion. As $\langle x, N\rangle = G$, while $\langle x, n\rangle < G$ for all $n \in N$, we deduce that $N$ is not cyclic.

Conversely, assume that $G$ is a Frobenius group $N{:}H$, where $N$ is a non-cyclic abelian group of odd order, $|H| = 2$, and the involution $x$ of $H$ acts on $N$ by inversion. By Theorem 2.1.19, $C_G(x) = H$. To complete the proof, and in particular to show that $x$ is adjacent in $\Xi(G)$ to all other vertices, it suffices to prove that $G$ is not 2-generated.

Let $g, g' \in G \setminus \{1\}$. If $g, g' \in N$, then $\langle g, g'\rangle \leqslant N < G$. If instead exactly one of $g$ and $g'$, say $g$, lies in $N$, then Proposition 2.1.20 implies that $g' = x^s$ for some $s \in G$. Since $g^{s^{-1}} \in N$ and $x$ acts on $N$ by inversion, we observe that $\langle g^{s^{-1}}, x\rangle = \langle g^{s^{-1}}\rangle{:}\langle x\rangle$. This is a proper subgroup of $G$, as $N$ is not cyclic. Conjugating by $s$, we obtain $\langle g, g'\rangle < G$. Finally, if $g, g' \notin N$, then $g$ and $g'$ are involutions by Proposition 2.1.20,

and so $\langle g, g' \rangle$ is dihedral. However, in any dihedral group of twice odd order, the unique subgroup of index 2 is cyclic. Thus $G$ is not dihedral, and $\langle g, g' \rangle < G$. □

The above proposition implies that if $\Xi(G)$ has a vertex that is adjacent to all other vertices, then the set of such vertices is precisely the set of isolated vertices of the commuting graph of $G$. The finite groups whose commuting graphs have isolated vertices are classified in [58, Theorem 3.9]. As in Proposition 5.2.9, these groups are Frobenius groups $N{:}H$, where $N$ is abelian of odd order and the involution of $H \cong C_2$ acts on $N$ by inversion. However, in this more general context, the group $N$ may be cyclic; here, the generator for $H$ is not adjacent in $\Xi(G)$ to any generator for $N$.

Furthermore, several observations from the proof of Proposition 5.2.9 also apply to any infinite group $G$ such that $\Xi(G)$ has a vertex $x$ that is adjacent to all other vertices. For example, $x$ must be an involution, and any subgroup $K$ of $G$ properly containing $\langle x \rangle$ must have trivial centre. Moreover, if $K$ is finite, then $K$ is a Frobenius group $N{:}\langle x \rangle$, where $N$ is an abelian (and possibly cyclic) group of odd order, and $x$ acts on $N$ by inversion.

The following result, together with Proposition 5.2.6 will allow us to determine upper bounds for distances between vertices of $\Xi(G)$ for certain non-abelian groups $G$.

**Proposition 5.2.10.** *Let $H$ be a normal subgroup of $G$, and suppose that $G/H$ is not cyclic. Additionally, let $h \in H$ and $g \in G$. Then $\{h, g\}$ is an edge of $\Xi(G)$ if and only if $[h, g] \neq 1$, i.e., if and only if $\{h, g\}$ is an edge of the non-commuting graph of $G$.*

*Proof.* Since $G/H$ is not cyclic, we see that $\langle Hg \rangle < G/H$, and hence $\langle H, g \rangle < G$. The result now follows from the definitions of $\Xi(G)$ and the non-commuting graph of $G$. □

We now explore how information about $\Xi(G)$ can be used to deduce information about $\Xi(G/N)$, for a normal subgroup $N$ of $G$, and vice versa.

**Proposition 5.2.11.** *Let $N$ be a normal subgroup of $G$, and let $x, y \in G$. Then $\{Nx, Ny\}$ is an edge of $\Xi(G/N)$ if and only if:*

(i) $[x, y] \notin N$; *and*

(ii) $\langle x, y, N \rangle < G$.

*In particular, if $\{Nx, Ny\}$ is an edge of $\Xi(G/N)$, then $\{x, y\}$ is an edge of $\Xi(G)$.*

*Proof.* The commutator of the elements $Nx, Ny \in G/N$ is $[Nx, Ny] = N[x, y]$, which is equal to $N = 1_{G/N}$ if and only if $[x, y] \in N$. In addition, the subgroup $\langle Nx, Ny\rangle$ of $G/N$ is equal to $(N\langle x, y\rangle)/N = \langle x, y, N\rangle/N$, which is a proper subgroup of $G/N$ if and only if $\langle x, y, N\rangle$ is a proper subgroup of $G$. Thus both (i) and (ii) hold if and only if $\{Nx, Ny\}$ is an edge of $\Xi(G/N)$. It is also clear that if (i) and (ii) hold, then $\{x, y\}$ is an edge of $\Xi(G)$. □

**Corollary 5.2.12.** *Let $N$ be a normal subgroup of $G$, and suppose that $\Xi(G/N)$ has a nontrivial connected component $X$. Additionally, let $k := \mathrm{diam}(X)$. Then the subgraph of $\Xi(G)$ induced by the vertices in $\{g \in G \setminus Z(G) \mid Ng \in X\}$ is connected with diameter at most $k$. In particular, if $N = Z(G)$, $Z(G/N) = 1$, and $\Xi(G/N)$ is connected with diameter $k$, then $\Xi(G)$ is connected with diameter at most $k$.*

*Proof.* Let $x$ and $y$ be elements of $G \setminus Z(G)$ such that $Nx, Ny \in X$. As $k \geqslant 2$ by Proposition 5.2.5, there exists a path $(Nx, Ng_1, \ldots, Ng_n)$ in $\Xi(G/N)$ with $n \leqslant k$, $g_1, \ldots, g_n \in G \setminus Z(G)$, and $g_n = y$. It follows from Proposition 5.2.11 that $(x, g_1, \ldots, g_n)$ is a path in $G$. Hence $d_{\Xi(G)}(x, y) \leqslant k$. Finally, if $N = Z(G)$, $Z(G/N) = 1$ and $X = \Xi(G/N)$, then $\{g \in G \setminus Z(G) \mid Ng \in X\} = \Xi(G)$, and the result follows. □

Our next result yields additional important symmetries of the graph $\Xi(G)$.

**Proposition 5.2.13.** *Let $\alpha \in \mathrm{Aut}(G)$ and $x, y \in G$. Then $\{x, y\}$ is an edge of $\Xi(G)$ if and only if $\{x^\alpha, y^\alpha\}$ is an edge of $\Xi(G)$. Moreover, if $N$ is a normal subgroup of $G$ that is stabilised by $\alpha$, then $\{Nx, Ny\}$ is an edge of $\Xi(G/N)$ if and only $\{Nx^\alpha, Ny^\alpha\}$ is an edge of $\Xi(G/N)$.*

*Proof.* The result about the edges of $\Xi(G)$ follows from the facts that $[x^\alpha, y^\alpha] = [x, y]^\alpha$ and $\langle x^\alpha, y^\alpha\rangle = \langle x, y\rangle^\alpha$. Similarly, since $\alpha$ stabilises $N$, the commutator $[x, y]$ lies in $N$ if and only if $[x^\alpha, y^\alpha] \in N$, and $\langle x, y, N\rangle^\alpha = \langle x^\alpha, y^\alpha, N\rangle$. Thus the statement about the edges of $\Xi(G/N)$ follows from Proposition 5.2.11. □

Hence each automorphism of $G$ induces an automorphism of $\Xi(G)$, as we implied in §1.0.2. It would be very interesting to further explore the structure of $\mathrm{Aut}(\Xi(G))$, and to compare it with structure of the automorphism group of the generating graph of $G$; this latter group was investigated in detail in [37, §5] (with $G$ finite). However, this is outside the scope of this thesis.

Observe that if $\alpha$ is an inner automorphism of $G$, then the second part of Proposition 5.2.13 holds for each normal subgroup $N$. Thus we obtain the following.

**Corollary 5.2.14.** *Let $x, y \in G$ and $c \in C_G(x)$, and let $N$ be a normal subgroup of $G$. If $x$ is adjacent in $\Xi(G)$ to some element of the conjugacy class $y^G$, then each element of $x^G$ is adjacent to a corresponding element of $y^G$. In particular, if $\{x, y\}$ is an edge of $\Xi(G)$, then so is $\{x, y^c\}$. Similarly, if $Nx$ is adjacent in $\Xi(G/N)$ to some element of $Ny^G$, then each element of $Nx^G$ is adjacent to a corresponding element of $Ny^G$, and if $\{Nx, Ny\}$ is an edge of $\Xi(G/N)$, then so is $\{Nx, Ny^c\}$.*

Together with Proposition 5.2.2, the above corollary shows that if $y$ is a neighbour of $x$ in $\Xi(G)$, then so is $x_1kx_2$ for all $x_1, x_2 \in \langle x \rangle$ and all $k \in y^{C_G(x)}$.

Our final result in this section provides a link between $\Xi(G)$, the non-generating graph of $G$ and the intersection graph of $G$ (as in Definition 4.1.1), when $Z(G) = 1$. In Chapter 6, we will use this result to provide a lower bound for the diameters of the non-commuting, non-generating graphs and non-generating graphs of the baby monster group and the unitary group $\mathrm{PSU}(7, 2)$.

**Proposition 5.2.15.** *Suppose that $Z(G) = 1$, and let $\Gamma$ be equal to $\Xi(G)$ or the non-generating graph of $G$. Assume also that $\Gamma$ is connected with finite diameter. Then the intersection graph $\Delta_G$ of $G$ is also connected, and* $\mathrm{diam}(\Gamma) \geqslant \mathrm{diam}(\Delta_G) - 1$.

*Proof.* Let $S_1$ and $S_2$ be distinct nontrivial proper subgroups of $G$. Additionally, choose distinct elements $g_0 \in S_1 \setminus \{1\}$ and $g_r \in S_2 \setminus \{1\}$, where $r := d_\Gamma(g_0, g_r)$. Note that $r$ is finite, as $\Gamma$ has finite diameter. We will show that $d_{\Delta_G}(S_1, S_2) \leqslant r+1$. Since $r \leqslant k := \mathrm{diam}(\Gamma)$, it will follow that $\mathrm{diam}(\Delta_G) \leqslant k+1$, and hence $k \geqslant \mathrm{diam}(\Delta_G)-1$.

There exist elements $g_1, \ldots, g_{r-1} \in G \setminus \{1\}$ such that $(g_0, g_1, \ldots, g_r)$ is a path in $\Gamma$, and $H_i := \langle g_i, g_{i+1} \rangle$ is a proper subgroup of $G$ for each $i \in \{0, \ldots, r-1\}$. Thus deleting consecutive repeats from $(S_1, H_0, H_1, \ldots, H_{r-1}, S_2)$ yields a walk in $\Delta_G$ of length at most $r + 1$, as required. □

We note that the discussion of *dual pairs* in [34, §12] (in particular Propositions 12.1 and 12.3) uses similar ideas to show that if $G$ is a (non-cyclic) group[1] whose non-generating graph is connected with diameter $k$, then $\mathrm{diam}(\Delta_G) \in \{k-1, k, k+1\}$. Hence Proposition 5.2.15 follows from this fact, and the fact that $\Xi(G)$ is a spanning subgraph of the non-generating graph of $G$ when $Z(G) = 1$.

Additionally, [34, §12] yields similar results about other pairs $(\Gamma_1, \Gamma_2)$ of graphs, where the vertex set of $\Gamma_1$ consists of the non-identity elements of a non-cyclic group $G$, and $\Gamma_2$ is an associated induced subgraph of $\Delta_G$. Indeed, the result in [29, §4] about the soluble graph of the baby monster group $\mathbb{B}$, which we mentioned at the

[1] Although [34, Proposition 12.3] assumes that $G$ is finite, the proof also holds in the infinite case.

end of §4.1, uses the fact that this soluble graph forms a dual pair with the subgraph of $\Delta_{\mathbb{B}}$ induced by the (nontrivial) soluble subgroups of $\mathbb{B}$.

## 5.3 Isolated vertices

In this section, we focus our attention on the isolated vertices of $\Xi(G)$. First, we provide a general characterisation of these vertices.

**Proposition 5.3.1.** *A vertex $g$ of $\Xi(G)$ is isolated if and only if all of the following hold:*

(i) *$G$ is 2-generated;*

(ii) *there exists a unique maximal subgroup $M$ of $G$ containing $g$; and*

(iii) *$g \in Z(M)$.*

*Moreover, if $G$ is finitely generated and $g$ is not isolated in $\Xi(G)$, then there exists a maximal subgroup $L$ of $G$ such that $g \in L \setminus Z(L)$.*

*Proof.* We may assume that $G$ is non-abelian. If $G$ is not 2-generated, then Corollary 5.2.7 shows that $\Xi(G)$ is connected. Hence in this case $\Xi(G)$ has no isolated vertices.

Suppose now that $G$ is 2-generated, and let $g \in G \setminus Z(G)$. Then $g$ is isolated in $\Xi(G)$ if and only if $[g, x] = 1$ for each $x \in G$ with $\langle g, x\rangle < G$. By Proposition 2.1.5, each proper subgroup of $G$ lies in a maximal subgroup of $G$, and hence $g$ is isolated if and only if each maximal subgroup containing $g$ also centralises $g$. Proposition 2.1.7 shows that $g$ lies in the centre of at most one maximal subgroup, and so either (ii) and (iii) both hold (and $g$ is isolated), or $g$ is non-central in at least one maximal subgroup (and is not isolated). □

It is even easier to classify the (non-abelian) groups $G$ for which every vertex of $\Xi(G)$ is isolated. Recall that a minimal non-abelian group is a non-abelian group with all proper subgroups abelian.

**Proposition 5.3.2.** *Suppose that $G$ is non-abelian. Then all vertices of $\Xi(G)$ are isolated if and only if $G$ is minimal non-abelian.*

*Proof.* The edges of $\Xi(G)$ correspond to pairs of non-generating elements of $G$ that do not commute. Thus $\Xi(G)$ has no edges if and only if all pairs of non-generating elements are commuting pairs, i.e., if and only if all proper subgroups are abelian. □

We will use Proposition 5.3.2 throughout the remainder of this thesis without further reference.

The finite minimal non-abelian groups were first classified by Miller and Moreno [110] in 1903, and Rédei [121] provided a more detailed description of their structures in 1947. In particular, any such group is a $p$-group, or a non-nilpotent group whose order has exactly two prime divisors. Thus, by Burnside's $p^aq^b$ Theorem, each finite minimal non-abelian group is soluble (Miller and Moreno in fact proved this fact without using Burnside's theorem, which had not yet been published). See [150, Theorem 2.4] for a concise description of the finite minimal non-abelian $p$-groups.

On the other hand, not all infinite minimal non-abelian groups are known. One family of examples is the family of infinite simple Tarski monster groups, mentioned in §2.1.2, where every nontrivial proper subgroup is cyclic of fixed prime order. Hence each Tarski monster group $G$ serves as an example of an infinite simple group for which the structure of $\Xi(G)$ is easily deduced: each of its vertices is isolated.

In general, it is clear that each minimal non-abelian group $G$ is 2-generated. Otherwise, $\langle x, y\rangle$ would be abelian for all $x, y \in G$, implying that $x \in Z(G)$ for all $x \in G$, contradicting the fact that $G$ is non-abelian.

Our next proposition (together with Proposition 5.3.1) details several necessary conditions for a vertex of $\Xi(G)$ to be isolated.

**Proposition 5.3.3.** *Suppose that $G$ is finitely generated, that an element $g$ of $G$ lies in a unique maximal subgroup $M$ of $G$, and that $g \in Z(M)$.*

(i) *Suppose that $M \not\trianglelefteq G$. Then $\mathrm{Core}_G(M) = Z(G)$.*

(ii) *If $M \trianglelefteq G$, or if $G$ contains a normal subgroup $N$ satisfying $Z(G) < C_G(N) < G$, then $M$ is abelian.*

(iii) *Suppose that $M$ is non-abelian. Then $G/Z(G)$ is primitive with point stabiliser $M/Z(G)$. If, in addition, $G/Z(G)$ has a minimal normal subgroup $R/Z(G)$, then $R/Z(G)$ is non-abelian, is the unique minimal normal subgroup of $G/Z(G)$, and intersects nontrivially with $M/Z(G)$.*

*Proof.* Let $h \in G \setminus M$. Since no maximal subgroup of $G$ contains both $g$ and $h$, it follows from Proposition 2.1.5 that $\langle g, h\rangle = G$.

(i) Here, $M^h \neq M$. As $M$ is the unique maximal subgroup of $G$ containing $g$, it follows that $M^h$ is the unique maximal subgroup of $G$ containing $g^h$. Thus $\langle g, g^h\rangle = \langle M, M^h\rangle = G$, which gives $\langle g\rangle^G = G$.

Now, let $K := \mathrm{Core}_G(M)$. Proposition 2.1.6 implies that $Z(G) < M$, and hence $Z(G) \leqslant K$. In addition, $C_G(K) \trianglelefteq N_G(K) = G$. The central element $g$ of $M$ centralises $K$, and hence $C_G(K)$ contains $\langle g \rangle^G = G$. It follows that $K \leqslant Z(G)$, and therefore $K = Z(G)$.

(ii) Assume first that $M \trianglelefteq G$. Then the characteristic subgroup $Z(M)$ of $M$ is normal in $G$. As $\langle Z(M), h \rangle = G$, it follows that $G/Z(M)$ is equal to the cyclic group $\langle Z(M)h \rangle$. Hence $M/Z(M)$ is cyclic, and Proposition 2.1.2 implies that $M$ is abelian.

Next, suppose that $M \not\trianglelefteq G$ and that $G$ contains a normal subgroup $N$ whose centraliser $C := C_G(N)$ satisfies $Z(G) < C < G$. Then $N \not\leqslant Z(G)$ and $N < G$. Since $\mathrm{Core}_G(M) = Z(G)$ by (i), and since $C \trianglelefteq N_G(N) = G$, it follows that $N \not\leqslant M$ and $C \not\leqslant M$. Moreover, $NM = G = CM$. Since $N \leqslant C_G(C) \leqslant C_G(C \cap M) \leqslant N_G(C \cap M)$ and $C \cap M \trianglelefteq M$, we conclude (similarly to the proof of [52, Theorem A.15.2]) that $C \cap M \trianglelefteq NM = G$. Thus $C \cap M \leqslant Z(G)$. Furthermore, no maximal subgroup of $G$ contains both $g$ and the proper subgroup $C$, and hence $\langle C, g \rangle = G$, i.e., $\langle Cg \rangle = G/C$. The Second Isomorphism Theorem gives $G/C = CM/C \cong M/(C \cap M)$, and in fact the associated isomorphism maps $Cg$ to $(C \cap M)g$. Thus $\langle (C \cap M)g \rangle = M/(C \cap M)$, i.e., $\langle C \cap M, g \rangle = M$. As $C \cap M$ lies in $Z(G)$, it follows that $M = \langle Z(G), g \rangle$, which is abelian.

(iii) Since $M$ is non-abelian, (ii) implies that $M \not\trianglelefteq G$, and hence $\mathrm{Core}_G(M) = Z(G)$ by (i). Let $\overline{G} := G/Z(G)$, $\overline{M} := M/Z(G)$ and $\overline{g} := Z(G)g$. Then $\overline{M}$ is the unique maximal subgroup of $\overline{G}$ containing $\overline{g}$, and $\overline{M}$ is core-free in $\overline{G}$. Hence $\overline{G}$ is primitive with point stabiliser $\overline{M}$ by Definition 2.1.22.

Assume now that $\overline{G}$ contains a minimal normal subgroup $\overline{R} := R/Z(G)$, with $R$ a subgroup of $G$ containing $Z(G)$. Then no maximal subgroup of $\overline{G}$ contains both $\overline{g}$ and $\overline{R}$, and hence $\langle \overline{g}, \overline{R} \rangle = \overline{G}$. Thus $\overline{G}/\overline{R} = \langle \overline{R}\,\overline{g} \rangle$ is cyclic. Additionally, since $\overline{R} \trianglelefteq \overline{G}$, we observe that $\overline{R}\,\overline{M} = \overline{G}$.

Suppose for a contradiction that $\overline{R} \cap \overline{M} = 1$. Then $\overline{G} = \overline{R} : \overline{M}$, and hence $\overline{M} = M/Z(G)$ is isomorphic to the cyclic group $\overline{G}/\overline{R}$. As $Z(G) \leqslant Z(M)$, it follows that $M/Z(M)$ is cyclic, and thus $M$ is abelian by Proposition 2.1.2. This contradicts the assumption that $M$ is non-abelian. Hence $\overline{R} \cap \overline{M} > 1$, and so $\overline{G}$ is not a split extension of $\overline{R}$ by $\overline{M}$. Theorem 2.1.24 therefore implies that $\overline{R}$ is non-abelian and the unique minimal normal subgroup of $\overline{G}$. □

The following associated question is open.

**Question 5.3.4.** *Does there exist a group $G$, a non-abelian maximal subgroup $M$ of $G$ and an element $g \in G$, such that $g \in Z(M)$ and $M$ is the unique maximal subgroup of $G$ containing $g$?*

For further discussions of related questions (from the perspective of isolated vertices of $\Xi(G)$), see §5.9.

We can in fact say more about the possible orders of elements that are isolated in the non-commuting, non-generating graphs of certain groups. First, we require the following preliminary result, which is a generalisation of Glauberman's $Z^*$ Theorem [61, Theorem 4]. In particular, the result is a combination of [61, Corollary 1] and [69, Theorem 4.1]. Here, for a prime $p$, we write $O_{p'}(G)$ to denote the largest normal subgroup of $G$ whose order is coprime to $p$.

**Theorem 5.3.5.** *Suppose that $G$ is finite, and let $p$ be a prime. Additionally, let $x$ be an element of $G$ whose order is a power of $p$, with $|x| = p$ if $p > 2$. If $O_{p'}(G)x \notin Z(G/O_{p'}(G))$, then there exists $g \in G$ such that $x^g \neq x$ and $[x, x^g] = 1$.*

Note that the proof in [61] of the $p = 2$ case of the above theorem does not use the classification of finite simple groups. However, the proof of the odd prime case in [69] does rely on the classification.

**Lemma 5.3.6.** *Suppose that $G$ is finite, and let $M$ be a non-normal maximal subgroup of $G$. Additionally, let $x$ be an element of $M \setminus Z(G)$, such that $|x|$ is a power of a prime $p$, with $|x| = p$ if $p > 2$. Assume also that each nontrivial normal subgroup of $G$ has order divisible by $p$. Then $x$ is non-central in some maximal subgroup of $G$. Hence $x$ is a non-isolated vertex of $\Xi(G)$.*

*Proof.* Suppose for a contradiction that each maximal subgroup of $G$ containing $x$ also centralises $x$. Then $x \in Z(M)$, and Proposition 2.1.7 shows that $C_G(x) = M$, and that $M$ is the unique maximal subgroup of $G$ containing $x$. Each nontrivial normal subgroup of $G$ has order divisible by $p$, and so the subgroup $O_{p'}(G)$ from Theorem 5.3.5 is trivial. Since $x \notin Z(G)$, this same theorem shows that there exists an element $g \in G$ such that $x \neq x^g \in C_G(x) = M$. As $x \in Z(M)$, we deduce that $g \in G \setminus M$.

Now, $M^g \neq M$, since $M$ is maximal and non-normal in $G$. Since $x^g$ lies in the distinct maximal subgroups $M$ and $M^g$ of $G$, its conjugate $x$ also lies in at least two maximal subgroups, a contradiction. It now follows from Proposition 5.3.1 that $x$ is a non-isolated vertex of $\Xi(G)$. □

The following result shows that in the case $|x| = 2$, we can in fact relax several of the hypotheses of the previous lemma, including the finiteness of $G$. This result and its proof are essentially from [139].

**Lemma 5.3.7.** *Suppose that $G$ is not a dihedral group and contains a non-normal maximal subgroup $M$. Then each involution of $M \setminus Z(G)$ is a non-isolated vertex of $\Xi(G)$.*

*Proof.* Let $g \in G \setminus M$, and suppose that $M \setminus Z(G)$ contains an involution $x$. Then $\langle x, x^g \rangle$ generates a (proper) dihedral subgroup $D$ of $G$. Either $D$ lies in a maximal subgroup of $G$ distinct from $M$, or $x^g \in M$ and $x \in M^{g^{-1}} \neq M$. Hence $x$ lies in at least two maximal subgroups of $G$, and Proposition 5.3.1 yields the result. □

We conclude this section by noting that §5.5 includes a characterisation of the isolated vertices of $\Xi(G)$ when $G$ is a direct product of groups. Furthermore, in §6.2, we will show that $\Xi(G)$ has no isolated vertices when $G$ is a finite simple group, using results from [139] that classify the elements of finite groups that lie in a unique maximal subgroup.

## 5.4 Groups with normal maximal subgroups

In this section, we prove several results about groups that contain normal maximal subgroups, and about these groups' non-commuting, non-generating graphs. In particular, we characterise $\Xi(G)$ when every maximal subgroup of $G$ is normal. This includes the case where $G$ is nilpotent, and in §5.6, we will describe in more detail the relationship between the structure of a finite nilpotent group and the structure of its non-commuting, non-generating graph. In §5.7, we will explore the structure of $\Xi(G)$ in more detail in the case where $G$ has a normal maximal subgroup satisfying specific properties.

Although the following result involves normal maximal subgroups of $G$, it applies also in certain cases where $G$ contains no such subgroup.

**Proposition 5.4.1.** *Let $(x, J, K)$ be an ordered triple such that $J$ and $K$ are proper subgroups of $G$, with $x \in J \setminus Z(J)$ and $x \notin K$. In addition, suppose that $H := J \cap K$ is a maximal subgroup of $J$, or that $K$ is a normal maximal subgroup of $G$.*

(i) *There exists $h \in H$ such that $\{x, h\}$ is an edge of $\Xi(G)$, and in particular $C_H(x) < H$.*

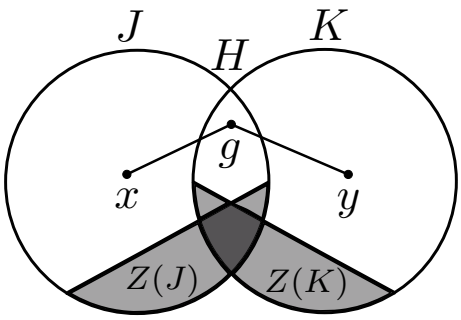



Figure 5.4.1: An illustration of Proposition 5.4.1(ii).

(ii) *Suppose that there exists $y \in K \setminus Z(K)$ with $y \notin J$, as in Figure 5.4.1. If $H$ is a maximal subgroup of $K$, or if $J$ is a normal maximal subgroup of $G$, then there exists an element $g \in H$ such that $(x, g, y)$ is a path in $\Xi(G)$.*

*Proof.* Proposition 2.1.9 shows that if $K$ is a normal maximal subgroup of $G$, then $H$ is maximal in $J$. Similarly, if $J$ is normal and maximal in $G$, then $H$ is maximal in $K$. Thus we may assume in general that $H$ is maximal in $J$, and in (ii) that $H$ is maximal in $K$.

Observe that $C_H(x) < H$, as otherwise $\langle H, x\rangle = J$ would centralise $x$. For each $h \in H \setminus C_H(x)$, the subgroup $\langle x, h\rangle$ lies in $J < G$. Hence $x \sim h$, yielding (i).

Now suppose that $H$ is maximal in $K$, and let $y$ be as in (ii). Then, similarly to above, $C_H(y) < H$. Thus there exists $g \in H \setminus (C_H(x) \cup C_H(y))$. Furthermore, $\langle x, g\rangle \leqslant J < G$ and $\langle g, y\rangle \leqslant K < G$, so that $x \sim g \sim y$, and we obtain (ii). □

In what follows, we use the fact that each nontrivial connected component of $\Xi(G)$ has diameter at least 2, by Proposition 5.2.5.

Let $L$ and $M$ be maximal subgroups of $G$, with $x \in L \setminus Z(L)$ and $y \in M \setminus Z(M)$. We split the proof of the following lemma into several cases, corresponding to where $x$ lies with respect to $M$ and $Z(M)$ and where $y$ lies with respect to $L$ and $Z(L)$. In one of these cases, we assume that either $x \in M \setminus Z(M)$ or $y \in L \setminus Z(L)$. If this does not occur, then either $x \in Z(M)$ or $x \notin M$, and either $y \in Z(L)$ or $y \notin L$. By considering the two possibilities for each of $x$ and $y$, we obtain our remaining cases.

**Lemma 5.4.2.** *Let $(x, L, y, M)$ be an ordered 4-tuple such that $L$ and $M$ are non-abelian maximal subgroups of $G$, with $L \trianglelefteq G$, $x \in L \setminus Z(L)$ and $y \in M \setminus Z(M)$. Suppose also that $C_L(x) \trianglelefteq G$ or $M \trianglelefteq G$. Then $d(x, y) \leqslant 3$. Moreover, $d(x, y) = 3$ if and only if $G$ is finitely generated and either:*

(i) *$x \in Z(M)$, $y \notin L$, and $M$ is the only maximal subgroup of $G$ containing but not centralising $y$; or*

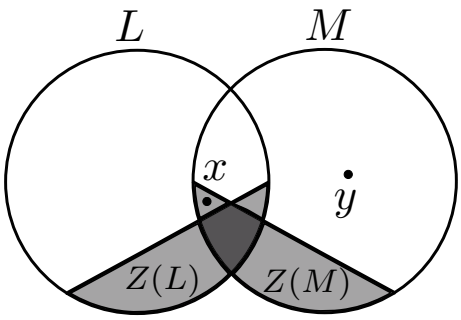



Figure 5.4.2: An illustration of case (i) of Lemma 5.4.2.

(ii) *$y \in Z(L)$, $x \notin M$, and $L$ is the only maximal subgroup of $G$ containing but not centralising $x$.*

Figure 5.4.2 illustrates the situation in (i).

*Proof.* We may assume that $G$ is finitely generated, as otherwise $d(x,y) \leqslant 2$ by Corollary 5.2.7. Let $\{(f,A),(g,B)\} = \{(x,L),(y,M)\}$. We will first show that if $f \in Z(B)$, then $G/\langle f\rangle^G$ is not cyclic. Here, if $B = L$ or $M \trianglelefteq G$, then $B$ is a non-abelian normal subgroup of $G$, and Proposition 2.1.2 implies that $G/\langle f\rangle^G$ is not cyclic. It remains to consider the case where $B = M \ntrianglelefteq G$ (so that $x \in Z(M)$) and $C_A(f) = C_L(x) \trianglelefteq G$. Observe that $M = C_G(x)$ by Proposition 2.1.7. Thus $C_L(x) = L \cap M$, and so $\langle x\rangle^G \leqslant L \cap M$. As $M \ntrianglelefteq G$, we see that $M/(L\cap M) \ntrianglelefteq G/(L\cap M)$. Hence $G/(L\cap M)$ is not cyclic, and it follows that $G/\langle x\rangle^G$ is also not cyclic, as required.

We split the remainder of the proof into the cases mentioned above the statement of the lemma.

**Case (a)**: $x \in M \setminus Z(M)$ or $y \in L \setminus Z(L)$. Here, $x$ and $y$ are non-central elements of a proper subgroup ($L$ or $M$) of $G$. Hence Corollary 5.2.8 yields $d(x,y) \leqslant 2$.

**Case (b)**: $x \notin M$ and $y \notin L$. As $L \trianglelefteq G$, applying Proposition 5.4.1 to the triple $(y,M,L)$ gives $C_{L\cap M}(y) < L \cap M$. If $M \trianglelefteq G$, then this same proposition implies that $d(x,y) \leqslant 2$.

It remains to consider the case where $C_L(x) \ntrianglelefteq G$. Since $x$ lies in $L$ and in $C_G(x)$ but not in $M$, we see that $C_G(x) \cap L \nleqslant M$. As $L$ and $L \cap C_G(x) = C_L(x)$ are normal in $G$, with $L$ and $M$ maximal, applying Proposition 2.1.10 to the triple $(C_G(x), L, M)$ gives $L \cap M \nleqslant C_G(x)$. Hence $C_{L\cap M}(x) < L \cap M$.

We have shown that $C_{L\cap M}(x)$ and $C_{L\cap M}(y)$ are proper subgroups of $L\cap M$. Thus there exists an element $h \in L \cap M$ that centralises neither $x$ nor $y$. Additionally, $\langle x,h\rangle \leqslant L < G$ and $\langle h,y\rangle \leqslant M < G$. Hence $x \sim h \sim y$, and $d(x,y) \leqslant 2$.

**Case (c)**: $x \in Z(M)$ and $y \in Z(L)$. Here, $[x, y] = 1$, since $x \in L$. As the non-commuting graph of $G$ is connected with diameter 2 by Proposition 5.2.6, this graph contains the path $(x, r, y)$ for some $r \in G \setminus Z(G)$. In addition, since $x \in Z(M)$ and $y \in Z(L)$, the quotients $G/\langle x \rangle^G$ and $G/\langle y \rangle^G$ are non-cyclic, by the first paragraph of the proof. It follows from Proposition 5.2.10 that $(x, r, y)$ is also a path in $\Xi(G)$, and hence $d(x, y)$ is at most 2 (and is in fact equal to 2 since $[x, y] = 1$).

**Case (d)**: $x \in Z(M)$ and $y \notin L$, or $y \in Z(L)$ and $x \notin M$. Here, $f \in Z(B)$ and $g \notin A$, where $\{(f, A), (g, B)\} = \{(x, L), (y, M)\}$ as above. We claim that $C_{A \cap B}(g) < A \cap B$. Indeed, if $(g, B) = (y, M)$ or if $M \trianglelefteqslant G$, then applying Proposition 5.4.1(i) to the triple $(g, B, A)$ yields the claim. Otherwise, the claim follows by applying Proposition 2.1.10 to the triple $(C_G(g), B, A)$, as in the proof of Case (b). In general, as $f$ lies in $A \cap B$ but not in $Z(A)$, we see that $Z(A) \cap B < A \cap B$. Thus there exists $k \in A \cap B$ with $k \notin Z(A)$ and $k \notin C_G(g)$. Observe that $g \sim k$, while $d(f, k) \leqslant 2$ by Corollary 5.2.8. Hence $d(f, g) \leqslant 3$.

It remains to show that $d(f, g) = 3$ if and only if $B$ is the unique maximal subgroup of $G$ that contains but does not centralise $g$. If $B$ is indeed the unique such maximal subgroup, then the neighbourhood of $g$ in $\Xi(G)$ is a subset of $B$. However, since $f \in Z(B)$, no element of $B$ is a neighbour of $f$. Thus $d(f, g) > 2$, and so $d(f, g) = 3$ by the previous paragraph.

Suppose instead that there exists a maximal subgroup $K$ of $G$ that contains but does not centralise $g$, with $K \neq B$. Then $K \cap B$ and $C_K(g)$ are proper subgroups of $K$, and so there exists $s \in K \setminus (B \cup C_K(g))$. In particular, $s \sim g$. Additionally, since $f \in Z(B)$, the quotient $G/\langle f \rangle^G$ is non-cyclic, by the first paragraph of the proof. As $s$ does not lie in $B$, which is equal to $C_G(f)$ by Proposition 2.1.7, it follows from Proposition 5.2.10 that $f \sim s$. Hence $f \sim s \sim g$, yielding $d(f, g) \leqslant 2$. □

We are now able to describe the structure of the non-commuting, non-generating graph of a group where every maximal subgroup is normal. Recall that $\Xi^+(G)$ denotes the subgraph of $\Xi(G)$ induced by its non-isolated vertices.

**Theorem 5.4.3.** *Suppose that every maximal subgroup of $G$ is normal, and that $\Xi(G)$ contains an edge. Then $\Xi^+(G)$ is connected with diameter 2 or 3. Moreover, if $G$ contains an abelian maximal subgroup, or if $\Xi(G)$ has an isolated vertex, then* $\operatorname{diam}(\Xi^+(G)) = 2$.

*Proof.* As $\Xi(G)$ contains an edge, $G$ is neither abelian nor minimal non-abelian. We may also assume that $G$ is 2-generated, as otherwise $\Xi(G)$ is connected with diameter 2 by Corollary 5.2.7.

Let $x$ and $y$ be non-isolated vertices of $\Xi(G)$. Then Proposition 5.3.1 shows that $G$ contains maximal subgroups $L$ and $M$ such that $x \in L \setminus Z(L)$ and $y \in M \setminus Z(M)$. As these maximal subgroups are normal in $G$, applying Lemma 5.4.2 to the 4-tuple $(x, L, y, M)$ yields $d(x, y) \leqslant 3$. Hence $\Xi^+(G)$ is connected with diameter 2 or 3. Moreover, if $G$ has an abelian maximal subgroup, then $Z(L)$ and $Z(M)$ are subgroups of $Z(G)$ by Lemma 2.1.12. Thus $x \notin Z(M)$ and $y \notin Z(L)$ for all choices of 4-tuples as above, and so Lemma 5.4.2 implies that $\operatorname{diam}(\Xi^+(G)) = 2$.

Suppose finally that $\Xi(G)$ has an isolated vertex $g$. Then by Proposition 5.3.1, $G$ is 2-generated, $g$ lies in a unique maximal subgroup $K$ of $G$, and $g \in Z(K)$. Furthermore, as $K \trianglelefteqslant G$, Proposition 5.3.3(ii) shows that $K$ is abelian. The previous paragraph now yields $\operatorname{diam}(\Xi^+(G)) = 2$. □

Now, each maximal subgroup of a nilpotent group is normal, and a finite group with each maximal subgroup normal is nilpotent. However, this latter statement is not true in the infinite case. For example, for each odd prime $p$, let $G_p$ be the infinite 2-generated $p$-group constructed by Gupta and Sidki in [68]. Then every maximal subgroup of $G_p$ is normal [119, Theorem 4.3]. By [8, Theorem 2.1], each finitely generated infinite nilpotent group contains an element of infinite order. Since each non-identity element of $G_p$ has order $p$, this group is not nilpotent. Groups with every maximal subgroup normal are discussed further in [114, 115].

In §5.6, we will present an example of a finite nilpotent group $G$ such that $\Xi(G)$ is connected with diameter 2; an example such that $\Xi(G)$ is connected with diameter 3; and an example such that $\Xi(G)$ has isolated vertices and a connected component of diameter 2. Hence each possibility allowed by Theorem 5.4.3 does indeed occur.

We also note that Lucchini [102, Corollary 4] proved a version of Theorem 5.4.3 for the generating graph of a finite 2-generated nilpotent group: the subgraph of this graph induced by its non-isolated vertices is always connected with diameter at most 2.

## 5.5 Direct products of groups

In this section, we consider the non-commuting, non-generating graph of a direct product of groups. Since a finite nilpotent group is the direct product of its Sylow subgroups by Theorem 2.1.15, the results of this section will play an important role in describing the structure of the non-commuting, non-generating graph of a given finite nilpotent group. Moreover, the results here are interesting in a broader context. In particular, we will see that the non-commuting, non-generating graph is relatively "well-behaved" in the context of direct products.

Throughout this section, both $G$ and $H$ will denote arbitrary groups, except where stated otherwise. The following proposition is one of the key observations towards determining the structure of $\Xi(G \times H)$.

**Proposition 5.5.1.** *Let $x_1, x_2 \in G$ and $y_1, y_2 \in H$. Suppose also that the following conditions are satisfied:*

(i) $[x_1, x_2] \neq 1$ *or* $[y_1, y_2] \neq 1$*; and*

(ii) $\langle x_1, x_2 \rangle < G$ *or* $\langle y_1, y_2 \rangle < H$.

*Then the elements $(x_1, y_1)$ and $(x_2, y_2)$ of $G \times H$ are adjacent vertices of $\Xi(G \times H)$.*

*Proof.* Since (i) holds, $(x_1, y_1)$ and $(x_2, y_2)$ do not commute. In particular, these are distinct non-central elements of $G \times H$, i.e., they are vertices of $\Xi(G \times H)$. Furthermore, (ii) implies that $\langle (x_1, y_1), (x_2, y_2) \rangle < G \times H$. Therefore, $(x_1, y_1)$ and $(x_2, y_2)$ are adjacent in $\Xi(G \times H)$. □

Using the above observation, we are able to prove the following.

**Theorem 5.5.2.** *Suppose that $G$ is non-abelian and that $H$ is not cyclic. Then $\Xi(G \times H)$ is connected with diameter 2.*

*Proof.* Let $(g_1, h_1), (g_2, h_2) \in (G \times H) \setminus (Z(G \times H))$. Note that, for each $i \in \{1, 2\}$, either $g_i \notin Z(G)$ or $h_i \notin Z(H)$. We split the proof into three (not all mutually exclusive) cases. By Proposition 5.2.5, it suffices in each case to find a path of length 2 in $\Xi(G \times H)$ between $(g_1, h_1)$ and $(g_2, h_2)$.

**Case (a)**: $g_1, g_2 \notin Z(G)$. Proposition 5.2.6 shows that there exists an element $u \in G$ that commutes with neither $g_1$ nor $g_2$. Additionally, as $H$ is not cyclic, $\langle h_1, 1 \rangle < H$ and $\langle 1, h_2 \rangle < H$. It follows from Proposition 5.5.1 that $((g_1, h_1), (u, 1), (g_2, h_2))$ is a path in $\Xi(G \times H)$.

**Case (b)**: $h_1, h_2 \notin Z(H)$. Here, $H$ is non-abelian. Thus arguing as in Case (a), there exists an element $v \in H$ such that $((g_1, h_1), (1, v), (g_2, h_2))$ is a path in $\Xi(G \times H)$.

**Case (c)**: Exactly one of $g_1$ and $g_2$ is central in $G$, and exactly one of $h_1$ and $h_2$ is central in $H$. We will assume without loss of generality that $h_1 \in Z(H)$, so that $h_2 \notin Z(H)$. Then $g_1 \notin Z(G)$ and $g_2 \in Z(G)$. Let $s \in G \setminus C_G(g_1)$ and $t \in H \setminus C_H(h_2)$. The non-abelian group $G$ properly contains the abelian group $\langle g_2, s \rangle$, and similarly, $\langle h_1, t \rangle < H$. Thus Proposition 5.5.1 implies that $((g_1, h_1), (s, t), (g_2, h_2))$ is a path in $\Xi(G \times H)$. □

The above theorem shows that there are certain trivial cases where $G$ is a central extension of an infinite simple group and $\mathrm{diam}(\Xi(G))$ is known, even if that simple group is 2-generated. Namely, if $G$ is the direct product of an infinite simple group and a non-cyclic abelian group, then $\mathrm{diam}(\Xi(G)) = 2$.

Now, let $\Gamma(G)$ denote the generating graph of $G$, and $\Gamma^+(G)$ the subgraph of $\Gamma(G)$ induced by its non-isolated vertices. Crestani and Lucchini [47, Theorem 1.1] proved that $\Gamma^+(G)$ is connected whenever $G$ is a 2-generated direct power $S^k$ of a non-abelian finite simple group $S$. However, if $S \cong \mathrm{PSL}(2, 2^p)$, with $p$ an odd prime, then $p$ and $k$ can be chosen so that $\mathrm{diam}(\Gamma^+(G)) > n$ for any given integer $n$ [47, Theorem 1.3]. On the other hand, Theorem 5.5.2 shows that $\Xi(S^m)$ is connected with diameter 2 for each non-abelian simple group $S$ and each integer $m \geqslant 2$. Thus the non-commuting, non-generating graphs of direct products of non-abelian groups are structured much more uniformly than the generating graphs of these groups.

In the next proposition and its proof, we write $d(\cdot, \cdot)$ to denote distances in both $\Xi(G)$ and $\Xi(G \times H)$. In each case, it will be clear which graph contains the relevant vertices.

**Proposition 5.5.3.** *Suppose that $G$ is non-abelian, and that $H$ is cyclic. Additionally, let $g_1$ and $g_2$ be distinct elements of $G \setminus Z(G)$, and let $h_1, h_2 \in H$. Then the following statements hold.*

(i) $d((g_1, h_1), (g_2, h_2)) \leqslant d(g_1, g_2)$.

(ii) *Suppose that $g_1$ is not isolated in $\Xi(G)$. Then $d((g_1, h_1), (g_1, h_2)) \in \{0, 2\}$.*

*Hence if $\Xi(G)$ is connected with diameter $k$, then $\Xi(G \times H)$ is connected with diameter at most $k$.*

*Proof.* Let $r := (x_1, x_2, \ldots, x_k)$ be a walk in $\Xi(G)$. No two adjacent vertices in $r$ commute or generate $G$, and so $((x_1, h_1), (x_2, h_2), \ldots, (x_k, h_2))$ is a walk in $\Xi(G \times H)$ by Proposition 5.5.1. We now use this fact to prove (i) and (ii).

(i) This is clear if $d(g_1, g_2) = \infty$. Otherwise, we obtain the result by setting $r$ to be a path in $\Xi(G)$ of minimal length under the conditions $x_1 = g_1$ and $x_k = g_2$.

(ii) If $h_1 = h_2$, then $d((g_1, h_1), (g_1, h_2)) = 0$. Otherwise, $(g_1, h_1)$ and $(g_1, h_2)$ commute, and hence are not adjacent in $\Xi(G \times H)$. Setting $r = (g_1, x_2, g_1)$, with $x_2$ some neighbour of $g_1$ in $\Xi(G)$, gives $d((g_1, h_1), (g_1, h_2)) = 2$.

Suppose finally that $\Xi(G)$ is connected with diameter $k$, and recall from Proposition 5.2.5 that $k \geqslant 2$. Since $\{(g, h) \mid g \in G \setminus Z(G), h \in H\}$ is the set of vertices of

$\Xi(G \times H)$, it follows from (i) and (ii) that $\Xi(G \times H)$ is connected with diameter at most $k$. □

The previous result suggests that, if $G$ is non-abelian and $H$ is cyclic, then $\mathrm{diam}(\Xi(G \times H))$ may be strictly less than $\mathrm{diam}(\Xi(G))$. The following two examples show that this possibility does indeed arise.

**Example 5.5.4.** For a group $K$, let $d(K)$ denote the minimum size of a generating set for $K$. It is easy to show, using Burnside's Basis Theorem, that $d(P_1 \times P_2) = d(P_1) + d(P_2)$ for all finite $p$-groups $P_1$ and $P_2$ with $p$ a fixed prime. Thus no 2-generated non-abelian finite $p$-group can be expressed as a nontrivial direct product. It will follow from Theorem 5.6.2 below that if $H$ is a finite cyclic group and $G$ is a finite nilpotent group such that $\Xi(G)$ is connected, then $\mathrm{diam}(\Xi(G \times H)) \neq \mathrm{diam}(\Xi(G))$ if and only if $\mathrm{diam}(\Xi(G)) = 3$ and $|G|$ and $|H|$ have a common prime divisor.

**Example 5.5.5.** Suppose that $G$ is the (non-nilpotent) symmetric group $S_4$. Using the Magma code in `comp_nc_ng`, we can show that the non-commuting, non-generating graphs of the 2-generated groups $S_4$, $S_4 \times C_3$ and $S_4 \times C_2$ are connected with diameter 3, 3 and 2, respectively. Hence, for a given non-nilpotent finite group $G$, there may exist nontrivial cyclic groups $H_1$ and $H_2$ such that $|G|$ is divisible by both $|H_1|$ and $|H_2|$, while $\mathrm{diam}(\Xi(G \times H_1)) < \mathrm{diam}(\Xi(G \times H_2)) = \mathrm{diam}(\Xi(G))$.

We now wish to determine the isolated vertices of $\Xi(G \times H)$. Proposition 5.3.1 suggests that a classification of the maximal subgroups of $G \times H$ will aid us in this task. The following result, which is a consequence of Goursat's Lemma [63, §11–12] (see also [7, §1–2]), gives such a classification.

**Lemma 5.5.6** ([138, p. 354])**.** *Let $K$ be a subgroup of $G \times H$. Then $K$ is maximal in $G \times H$ if and only if one of the following occurs:*

(i) *$K = M_G \times H$, for some maximal subgroup $M_G$ of $G$;*

(ii) *$K = G \times M_H$, for some maximal subgroup $M_H$ of $H$; or*

(iii) *$K = \{(g, h) \mid g \in G, h \in H, (N_1 g)\theta = N_2 h\}$, where $N_1$ and $N_2$ are maximal normal subgroups of $G$ and $H$, respectively, and $\theta$ is an isomorphism from $G/N_1$ to $H/N_2$.*

In the following two results, we assume the convention that if $H$ is an infinite group, then each positive integer divides $|H|$.

**Theorem 5.5.7.** *Suppose that $G$ and $H$ are finitely generated, with $G$ non-cyclic, and let $g \in G$ and $h \in H$. Additionally, let $\mathcal{L}$ be the set of maximal subgroups $L$ of $G$ such that $L \trianglelefteqslant G$ and $|G : L|$ is a prime dividing $|H|$. Then $(g, h)$ lies in a unique maximal subgroup of $G \times H$ if and only if all of the following hold:*

(i) $\langle h \rangle = H$;

(ii) *$g$ lies in a unique maximal subgroup $M_G$ of $G$; and*

(iii) $\mathcal{L} \subseteq \{M_G\}$.

*Proof.* As $G$ is finitely generated and $\langle g \rangle < G$, Proposition 2.1.5 implies that there exists a maximal subgroup $M_G$ of $G$ containing $g$. Similarly, there exists a maximal subgroup $M_H$ of $H$ containing $h$ if and only if $\langle h \rangle \neq H$. Notice that $(g, h)$ lies in the maximal subgroups $M_G \times H$ and $G \times M_H$ of $G \times H$ for every such $M_G$ and $M_H$. Hence if $(g, h)$ lies in a unique maximal subgroup of $G \times H$, then (i) and (ii) hold. For the remainder of the proof, we will assume that these two conditions hold.

Lemma 5.5.6 shows that $(g, h)$ lies in a maximal subgroup of $G \times H$ other than $M_G \times H$ if and only if there exist maximal normal subgroups $N_1$ of $G$ and $N_2$ of $H$, and an isomorphism $\theta : G/N_1 \to H/N_2$ with $(N_1 g)\theta = N_2 h$. If this is the case, then since $\langle h \rangle = H$, we see that $\langle N_2 h \rangle = H/N_2$, and hence $\langle N_1 g \rangle = G/N_1$. Furthermore, $N_2$ is a maximal subgroup of the cyclic group $H$, and so $N_1$ is maximal in $G$.

Now, the quotients of the cyclic group $H$ by its maximal subgroups are precisely the cyclic groups of order a prime dividing $|H|$. Hence $G$ contains a normal subgroup $N_1$ as in the previous paragraph if and only if $N_1 \in \mathcal{L}$ and $g \notin N_1$, i.e., if and only if $\mathcal{L}$ contains a subgroup not equal to $M_G$. Therefore, $M_G \times H$ is the unique maximal subgroup of $G \times H$ containing $(g, h)$ if and only if (iii) holds, as required. □

We are now able to describe the isolated vertices of $\Xi(G \times H)$.

**Corollary 5.5.8.** *Suppose that $G$ is non-abelian, and let $g \in G$ and $h \in H$. Additionally, let $\mathcal{L}$ be the set of maximal subgroups $L$ of $G$ such that $L \trianglelefteqslant G$ and $|G : L|$ divides $|H|$. Then $(g, h)$ is an isolated vertex of $\Xi(G \times H)$ if and only if all of the following hold:*

(i) $\langle h \rangle = H$;

(ii) *$g$ is an isolated vertex of $\Xi(G)$; and*

(iii) $|\mathcal{L}| \leqslant 1$, *and if* $\mathcal{L} = \{L\}$, *then* $g \in L$.

*Proof.* Note that if $G$ is not 2-generated, then neither is $G \times H$. Hence in this case Corollary 5.2.7 implies that $\Xi(G)$ and $\Xi(G \times H)$ are connected, and so have no isolated vertices. In particular, (ii) is not satisfied. If instead $H$ is not 2-generated, then again neither is $G \times H$, and $\Xi(G \times H)$ has no isolated vertices. Furthermore, (i) does not hold in this case. We may therefore assume that $G$ and $H$ are 2-generated. Note also that if (i) holds, then $g$ is a vertex of $\Xi(G)$ if and only if $(g, h)$ is a vertex of $\Xi(G \times H)$.

Suppose first that $(g, h)$ is an isolated vertex of $\Xi(G \times H)$. Then Proposition 5.3.1 implies that $G \times H$ has a unique maximal subgroup $K$ containing $(g, h)$, and $(g, h) \in Z(K)$. Hence by Theorem 5.5.7, (i) and (iii) hold, and $g$ lies in a unique maximal subgroup $M_G$ of $G$. Since $(g, h)$ lies in the maximal subgroup $M_G \times H$ of $G \times H$, we conclude that $K = M_G \times H$. In addition, as $(g, h) \in Z(K) = Z(M_G) \times H$, we see that $g \in Z(M_G)$. Proposition 5.3.1 therefore yields (ii).

Conversely, suppose that (i), (ii) and (iii) all hold. Then it follows from Proposition 5.3.1 that $g$ lies in a unique maximal subgroup $M_G$ of $G$, and $g \in Z(M_G)$. Hence Theorem 5.5.7 implies that $M_G \times H$ is the unique maximal subgroup of $G \times H$ containing $(g, h)$. Since $(g, h) \in Z(M_G) \times H = Z(M_G \times H)$, the vertex $(g, h)$ is isolated in $\Xi(G)$ by Proposition 5.3.1. □

The fact that $\Xi(G \times H)$ contains no isolated vertices if $G$ is non-abelian and $H$ is not cyclic also follows directly from Theorem 5.5.2.

## 5.6 Finite nilpotent groups

Recall Theorem 5.4.3, which describes the possible structures of the graph $\Xi(G)$ when $G$ is a group with every maximal subgroup normal. In this section, we will investigate in more detail the relationship between the structures of $\Xi(G)$ and $G$ when $G$ is also finite, and hence nilpotent. In particular, we will prove the following two stronger versions of Theorem 5.4.3. Here, $p$ denotes a prime, and as in Definition 5.1.3, $\Xi^+(G)$ denotes the subgraph of $\Xi(G)$ induced by its non-isolated vertices.

**Theorem 5.6.1.** *Suppose that $G$ is a finite $p$-group. Then one of the following occurs.*

(i) *$G$ is either abelian or minimal non-abelian. In this case, $\Xi(G)$ has no edges.*

(ii) *$G$ is non-abelian and not 2-generated. In this case, $\Xi(G)$ is connected with diameter 2.*

(iii) *$G$ is non-abelian, 2-generated and not minimal non-abelian, and contains at most one abelian maximal subgroup. Furthermore, each maximal subgroup contains $Z(G)$.*

  (a) *If $G$ has an abelian maximal subgroup $M$, then $\Xi^+(G)$ is connected with diameter 2, and the isolated vertices of $\Xi(G)$ are precisely the elements of $M \setminus \Phi(G) \neq \varnothing$.*

  (b) *If the centre of each maximal subgroup of $G$ is equal to $Z(G)$, then $\Xi(G)$ is connected with diameter 2.*

  (c) *If all maximal subgroups of $G$ are non-abelian, and at least one has a centre properly containing $Z(G)$, then $\Xi(G)$ is connected with diameter 3.*

**Theorem 5.6.2.** *Suppose that $G$ is finite and nilpotent, and that $|G|$ is divisible by at least two primes. Then one of the following occurs.*

(i) *$G$ is abelian. In this case, $\Xi(G)$ is the empty graph.*

(ii) *$G$ is non-abelian and contains at least two non-cyclic Sylow subgroups. In this case, $\Xi(G)$ is connected with diameter 2.*

(iii) *$G = P \times H$, with $P$ a non-abelian Sylow subgroup of $G$ and $H$ cyclic.*

  (a) *If $\Xi(P)$ has no isolated vertex, then $\Xi(G)$ is connected, and $\operatorname{diam}(\Xi(G)) = \operatorname{diam}(\Xi(P)) \in \{2, 3\}$.*

  (b) *If $\Xi(P)$ has an isolated vertex, then $\Xi^+(G)$ is connected with diameter 2, and $(g, h) \in G$ is an isolated vertex of $\Xi(G)$ if and only if $g$ is an isolated vertex of $\Xi(P)$ and $\langle h \rangle = H$.*

As mentioned in §5.3, each finite nilpotent minimal non-abelian group is a $p$-group [110]. Thus the group $G$ from Theorem 5.6.2 is never minimal non-abelian. However, the group $P$ in case (iii)(b) of this theorem may be minimal non-abelian.

We will first focus on proving Theorem 5.6.1. It is clear that $\Xi(G)$ has no edges if $G$ is abelian or minimal non-abelian, and we recall from Corollary 5.2.7 that $\Xi(G)$ is connected with diameter 2 if $G$ is non-abelian and not 2-generated. We therefore begin by proving the following useful lemma about non-abelian, finite, 2-generated $p$-groups. The "equality" statement in part (iii) of this lemma is well known (for example, see [150, Lemma 2.3]). Additionally, while part (v) of the lemma is not required to prove Theorem 5.6.1, we include it for general interest.

**Lemma 5.6.3.** *Suppose that $G$ is a non-abelian, finite, 2-generated $p$-group. Then the following statements hold.*

(i) *$\Phi(G)$ is a maximal subgroup of each maximal subgroup of $G$.*

(ii) *Each element of $G \setminus \Phi(G)$ lies in a unique maximal subgroup of $G$.*

(iii) *$Z(G) \leqslant \Phi(G)$, with equality if and only if $G$ is minimal non-abelian.*

(iv) *If $G$ is not minimal non-abelian, then $G$ contains at most one abelian maximal subgroup.*

(v) *Let $M$ be a non-abelian maximal subgroup of $G$. Then $Z(M) < \Phi(G)$.*

*Proof.*

(i) As $G$ is 2-generated, Burnside's Basis Theorem implies that $\Phi(G)$ has index $p^2$ in $G$. Since $\Phi(G)$ lies in each maximal subgroup of $G$ by definition, and since each maximal subgroup of a $p$-group has index $p$, the result follows.

(ii) We will prove the contrapositive of the result. Let $x$ be an element of $G$ that lies in two distinct maximal subgroups $L$ and $M$. Then $x \in L \cap M$, which is equal to $\Phi(G)$ by (i).

(iii)–(iv) Let $M$ be a maximal subgroup of $G$. By (i), $M$ contains an element $x$ that does not lie in $\Phi(G)$. Moreover, (ii) shows that $M$ is the unique maximal subgroup of $G$ containing $x$. As the abelian group $\langle x, Z(G)\rangle$ is a proper subgroup of $G$, it follows that $M$ contains $Z(G)$. This holds for every maximal subgroup of $G$, and so $Z(G) \leqslant \Phi(G)$.

Now, if $Z(G) = \Phi(G)$, then $\langle \Phi(G), x\rangle$ is abelian, and is equal to $M$ by (i). This again holds for every maximal subgroup, and so $G$ is minimal non-abelian.

If instead there exists $y \in \Phi(G) \setminus Z(G)$, then by Proposition 2.1.7, $y$ lies in the centre of at most one maximal subgroup of $G$. As $y$ lies in each maximal subgroup of $G$, it follows that at most one of these maximal subgroups is abelian, and in particular $G$ is not minimal non-abelian.

(v) As $M \trianglelefteq G$, Proposition 5.3.3(ii) implies that each central element of $M$ lies in a maximal subgroup of $G$ distinct from $M$. Thus (ii) implies that no element of $M \setminus \Phi(G)$ is central in $M$, and hence $Z(M) \leqslant \Phi(G)$. Since $\Phi(G)$ is maximal in $M$ by (i), while $Z(M)$ is not maximal in $M$ by Proposition 2.1.2, we deduce that $Z(M) < \Phi(G)$. □

*Proof of Theorem 5.6.1.* Lemma 5.6.3 shows that if $G$ is non-abelian, 2-generated and not minimal non-abelian, then $G$ contains at most one abelian maximal subgroup, and $Z(G) < \Phi(G)$. Hence, in this case, each maximal subgroup of $G$ contains $Z(G)$. Therefore, exactly one of (i), (ii) and (iii) holds, and we may consider each case separately.

(i) This is clear.

(ii) This is an immediate consequence of Corollary 5.2.7.

(iii)(a) By Lemma 5.6.3(ii), the abelian maximal subgroup $M$ of $G$ is the unique maximal subgroup containing each element of $M \setminus \Phi(G)$. As each other maximal subgroup of $G$ is non-abelian, it follows from Propositions 5.3.1 and 5.3.3(ii) that a vertex $g$ of $\Xi(G)$ is isolated if and only if $g$ lies in the set $M \setminus \Phi(G)$, which is non-empty as $G$ is not cyclic. As each element of $G \setminus M$ is a vertex of $\Xi(G)$ by Lemma 5.6.3(iii), we see that $\Xi(G)$ has an edge. It now follows from Theorem 5.4.3 that $\Xi^+(G)$ is connected with diameter 2.

(iii)(b) Let $x, y \in G \setminus Z(G)$, and let $L$ and $M$ be maximal subgroups of $G$ that contain $x$ and $y$, respectively. As $Z(L) = Z(G) = Z(M)$, applying Lemma 5.4.2 to the 4-tuple $(x, L, y, M)$ gives $d(x, y) \leqslant 2$. It follows from Proposition 5.2.5 that $\Xi(G)$ is connected with diameter 2.

(iii)(c) Let $M$ be a (non-abelian) maximal subgroup of $G$ that satisfies $Z(G) < Z(M)$. In addition, let $y \in M \setminus \Phi(G)$, and let $x \in Z(M) \setminus Z(G)$. Proposition 5.3.3(ii) implies that each element of $Z(M)$ lies in a maximal subgroup of $G$ distinct from $M$. In particular, $x$ lies in such a maximal subgroup $L$, and $x \notin Z(L)$ by Proposition 2.1.7. On the other hand, Lemma 5.6.3(ii) shows that $M$ is the unique maximal subgroup of $G$ containing $y$, and thus $y \notin Z(M)$. Hence applying Lemma 5.4.2 to the 4-tuple $(x, L, y, M)$ yields $d(x, y) = 3$. Theorem 5.4.3 therefore implies that $\Xi(G)$ is connected with diameter 3. □

Using the Magma code in `p_groups_small`, we can show that the groups numbered[2] $(16, 7)$, $(243, 3)$ and $(32, 6)$ in the Small Groups Library [11] are groups of the smallest order satisfying properties (iii)(a), (b) and (c) of Theorem 5.6.1, respectively.

We can now prove Theorem 5.6.2 using Theorems 5.4.3 and 5.6.1, together with the results of §5.5.

[2]The first integer in each ordered pair is the order of the group.

*Proof of Theorem 5.6.2.* Recall from Theorem 2.1.15 that $G$ is the direct product of its Sylow subgroups. Hence exactly one of (i), (ii) and (iii) holds. We may therefore consider each case separately.

(i) This is clear.

(ii) We may express $G$ as $A \times B$, where $A$ is a non-abelian direct product of Sylow subgroups of $G$, and $B$ is a non-cyclic direct product of Sylow subgroups of $G$. Thus Lemma 5.5.2 shows that $\Xi(G)$ is connected with diameter 2.

(iii)(a) As $\Xi(P)$ is not the empty graph, Theorem 5.4.3 implies that $\Xi(P)$ is connected with diameter 2 or 3. Hence Propositions 5.2.5 and 5.5.3 show that $\Xi(G)$ is connected, with $1 < \operatorname{diam}(\Xi(G)) \leqslant \operatorname{diam}(\Xi(P))$. It therefore suffices to find a pair of vertices of $\Xi(G)$ of distance 3 in the case $\operatorname{diam}(\Xi(P)) = 3$. Here, Theorem 5.6.1 shows that $P$ is 2-generated, and that there exists a non-abelian maximal subgroup $M$ of $P$ with $Z(P) < Z(M)$. As $P$ is a Sylow subgroup of $G$, the direct factors $P$ and $H$ have coprime orders, and so $G$ is also 2-generated.

Now, $Z(M)$ is a proper subgroup of the non-abelian group $M$, as is $\Phi(P)$ since $P$ is not cyclic. Thus there exists $a \in M \setminus (\Phi(P) \cup Z(M))$. Let $x$ be a generator for $H$, and $b \in Z(M) \setminus Z(P)$. By Lemma 5.6.3(ii), $M$ is the unique maximal subgroup of $P$ containing $a$. As $|P|$ is coprime to $|H|$, the set $\mathcal{L}$ in Theorem 5.5.7 (applied to the direct product $P \times H$) is empty, and so that theorem shows that $M \times H$ is the unique maximal subgroup of $G$ containing $(a, x)$. Additionally, $(b, x)$ lies in $Z(M) \times H = Z(M \times H)$, while $(a, x)$ does not. Since $\Xi(P)$ contains no isolated vertices, we conclude from Proposition 5.3.1 that there exists a maximal subgroup $L$ of $P$ with $b \in L \setminus Z(L)$, and hence $(b, x) \in (L \times H) \setminus Z(L \times H)$. Applying Lemma 5.4.2 to the 4-tuple $((b, x), L \times H, (a, x), M \times H)$ therefore yields $d((a, x), (b, x)) = 3$.

(iii)(b) Since $|P|$ is coprime to $|H|$, the set $\mathcal{L}$ in Corollary 5.5.8 (again applied to the direct product $P \times H$) is empty. Hence this corollary implies that the set of isolated vertices of $\Xi(G)$ is as required. In particular, $\Xi(G) \neq \Xi^+(G)$. Additionally, Proposition 5.5.1 shows that for any choice of $x \in P \setminus Z(P)$ and $y \in P \setminus C_P(x)$, the vertices $(x, 1)$ and $(y, 1)$ are adjacent in $\Xi(G)$. Thus $\Xi(G)$ has both isolated and non-isolated vertices, and we conclude from Theorem 5.4.3 that $\Xi^+(G)$ is connected with diameter 2. □

Theorem 5.6.2 includes a description of the non-commuting, non-generating graph of the direct product of a finite non-abelian nilpotent group and a finite

cyclic group. We can also describe the graph of such a direct product where the cyclic group is infinite.

**Proposition 5.6.4.** *Suppose that $G$ is non-abelian, finite and nilpotent. Then $G \times \mathbb{Z}$ is not 2-generated, and hence $\Xi(G \times \mathbb{Z})$ is connected with diameter 2.*

*Proof.* As above, it follows from Theorem 2.1.15 that $G$ contains a non-abelian (and hence non-cyclic) Sylow subgroup $P$. Let $k$ be the smallest size of a generating set for $P$. Then $k > 1$, and Burnside's Basis Theorem implies that $P/\Phi(P)$ is isomorphic to the elementary abelian group $C_p^k$ for some prime $p$. Thus $C_p^{k+1}$ is a quotient of $P/\Phi(P) \times \mathbb{Z}$, which is a quotient of $G \times \mathbb{Z}$. Hence the smallest size of a generating set for $G \times \mathbb{Z}$ is at least the smallest size of a generating set for $C_p^{k+1}$, which is $k + 1 > 2$. Therefore, Corollary 5.2.7 shows that $\Xi(G \times \mathbb{Z})$ is connected with diameter 2. □

## 5.7 Distances involving certain normal maximal subgroups

In this section, we continue the study of groups containing normal maximal subgroups that we began in §5.4. The focus here is on the case where $G$ has a normal, non-abelian maximal subgroup $M$ satisfying $Z(G) < Z(M)$. In particular, we determine upper bounds for the distance in $\Xi(G)$ between an element of $M \setminus Z(M)$ and an element of $(G \setminus M) \cup (Z(M) \setminus Z(G))$. The results here will be useful in §5.8 when we determine the structures of the non-commuting, non-generating graphs for a certain family of groups.

We begin with two necessary results that apply even when $G$ does not contain a maximal subgroup $M$ with all of the above properties. Note that, since the union of two proper subgroups of a group is a proper subset of that group, it follows from Proposition 2.1.5 that each finitely generated non-cyclic group has at least three maximal subgroups.

**Lemma 5.7.1.** *Suppose that $G$ is finitely generated and non-cyclic. Moreover, assume that $G$ contains a normal maximal subgroup $M$, and that $K \cap M = L \cap M$ for all maximal subgroups $K$ and $L$ of $G$ distinct from $M$. Then $K \cap M = K \cap L = \Phi(G)$. Moreover, if $G$ is finite, then $G$ is soluble. If, in addition, $M$ is the unique normal maximal subgroup of $G$, then $G$ contains exactly two conjugacy classes of maximal subgroups.*

*Proof.* Let $K$ and $L$ be distinct maximal subgroups of $G$ that are not equal to $M$. As $K \cap M = L \cap M$, we observe that $K \cap M \leqslant K \cap L < K$. Moreover, $K \cap M$ is a maximal subgroup of $K$ by Proposition 2.1.9, and thus $K \cap M = K \cap L$. Hence

$K \cap M$ is the intersection of each pair of distinct maximal subgroups of $G$, and so $K \cap M = \Phi(G)$.

We assume from now on that $G$ is finite. As $|K \cap M| = |L \cap M|$, it follows that $|K| = |L|$, and so the set $S$ of orders of maximal subgroups of $G$ has size at most 2.

Suppose first that $G$ is insoluble. Since $|S| \leqslant 2$, the quotient $G/\Phi(G)$ is isomorphic to $H := (C_2^{3i}{:}\mathrm{PSL}(2,7)) \times C_7^j$, where $i$ and $j$ are non-negative integers [127]. The group $\mathrm{PSL}(2,7)$ contains a maximal subgroup $A$ of index 7 and a maximal subgroup $B$ of index 8 [42, p. 3]. It follows that $(C_2^{3i}{:}A) \times C_7^j$ and $(C_2^{3i}{:}B) \times C_7^j$ are maximal subgroups of $H$ of index 7 and 8, respectively. Each of these maximal subgroups intersects the simple group $\mathrm{PSL}(2,7)$ in its corresponding maximal subgroup, which is not normal, and hence these maximal subgroups of $H$ are not normal. Therefore, $G$ contains non-normal maximal subgroups $K$ and $L$ of index 7 and 8, respectively. However, this contradicts the fact $|K| = |L|$ from the previous paragraph.

Hence $G$ is soluble. Assume now that $M$ is the unique normal maximal subgroup of $G$. Then $K \not\trianglelefteq G$, and the normal subgroup $\Phi(G)$ of $G$ is maximal in $K$ by the first paragraph of this proof. Hence $\mathrm{Core}_G(K) = \Phi(G)$. This holds for each maximal subgroup of $G$ distinct from $M$, and so Theorem 2.1.17 shows that these maximal subgroups are all conjugate in $G$. Therefore, $G$ has exactly two conjugacy classes of maximal subgroups, one of which contains only the normal subgroup $M$. □

In the following theorem, which is a more detailed version of a theorem of Adnan [2], we classify the finite groups that satisfy the final conclusion of the previous lemma, and determine some of their properties. Recall from Burnside's Basis Theorem that if $P$ is a finite $p$-group, then we may consider $P/\Phi(P)$ as a vector space over $\mathbb{F}_p$.

**Theorem 5.7.2.** *Suppose that $G$ is finite. Then the following statements hold.*

(i) *$G$ contains exactly two conjugacy classes of maximal subgroups if and only if:*

  (a) *$G = P{:}Q$, where $P$ and $Q$ are nontrivial Sylow subgroups of coprime order; and*

  (b) *$Q$ is cyclic and acts irreducibly on $P/\Phi(P)$.*

  *In particular, $G$ is soluble.*

(ii) *Suppose that* (i)(a) *and* (b) *hold, and let $R$ be the unique maximal subgroup of $Q$. Then:*

(a) *the maximal subgroups of* $G$ *are the normal subgroup* $M := PR$ *and the conjugates of* $\Phi(P)Q$*;*

(b) $R \trianglelefteqslant G$ *if and only if* $\Phi(G) = M \cap \Phi(P)Q$*;*

(c) *if* $R \trianglelefteqslant G$*, then* $M = P \times R$*, and* $\Phi(G) = \Phi(P) \times R$ *is the intersection of each pair of distinct maximal subgroups of* $G$*; and*

(d) *if* $R \trianglelefteqslant G$*,* $C_M(\Phi(G)) \not\leqslant \Phi(G)$*, and* $M$ *is non-abelian, then* $\Phi(G) = Z(M)$*, i.e.,* $\Phi(P) = Z(P)$*.*

*Proof.* We will begin by proving (i) and (ii)(a). Note that $\Phi(P)$ is a characteristic subgroup of the normal subgroup $P$ of $G$, and hence $\Phi(P)Q$ is a subgroup of $G$ (and the action of $Q$ on $P/\Phi(P)$ is well-defined). Adnan [2] proved that if $G$ contains exactly two conjugacy classes of maximal subgroups, then $G$ satisfies (i)(a) and (b). We will therefore assume that (i)(a) and (b) hold. Then Burnside's $p^aq^b$ Theorem implies that $G$ is soluble.

The irreducibility of the action of $Q$ on $P/\Phi(P)$ implies that $\langle \Phi(P), Q, x\rangle = G$ for each $x \in P \setminus \Phi(P)$, and so $\Phi(P)Q$ is a maximal subgroup of $G$. Since $R$ is maximal in $Q$ and $P \trianglelefteqslant G$, we deduce that $M := PR$ is also a maximal subgroup of $G$. As $G/P$ is cyclic, its subgroup $M/P$ is normal, and hence $M \trianglelefteqslant G$.

To complete the proofs of (i) and (ii)(a), it suffices to show that we have described all maximal subgroups of $G$. Suppose, for a contradiction, that $G$ contains a maximal subgroup $T$ that is not equal to $M$ and not conjugate to $\Phi(P)Q$. Then $T$ contains an element $xy$, where $x \in P$ and (without loss of generality) $y$ is a generator for $Q$. For each integer $k$, the projection of $(xy)^k$ onto $Q$ is equal to $y^k$. Thus $|Q|$ divides $|xy|$, and it follows that $T$ contains an element of order $|Q|$. Hence $T$ contains a Sylow subgroup of $G$ of order $|Q|$, and we may assume that $Q \leqslant T$.

Let $S$ be the projection of $T$ onto $P$, i.e., the set of elements $x \in P$ such that there exists $y \in Q$ with $xy \in T$. By the previous paragraph, $S = T \cap P$. Moreover, Theorem 2.1.17 implies that $G = T\Phi(P)Q = TQ\Phi(P) = (T\cap P)Q\Phi(P) = S\Phi(P)Q$. As $G = P{:}Q$, we deduce that $\langle S, \Phi(P)\rangle = P$. Hence $S = P$ (since each maximal subgroup of $P$ contains $\Phi(P)$), and so $P \leqslant T$. Thus $T$ contains $\langle P, Q\rangle = G$. This contradicts the maximality of $T$, and so we obtain (i) and (ii)(a).

We now prove (ii)(b)–(c). Assume first that $\Phi(G) = M \cap \Phi(P)Q$. Then this intersection, which is equal to $\Phi(P)R$, is normal in $G$. Since $R$ is a Sylow $q$-subgroup of $\Phi(P)R$, the Frattini Argument yields $G = \Phi(P)RN_G(R) = \Phi(P)N_G(R)$. Thus $P = \Phi(P)N_G(R) \cap P$, which is equal to $\Phi(P)(N_G(R) \cap P)$ by Lemma 2.1.1. As each maximal subgroup of $P$ contains $\Phi(P)$, it follows that $P = N_G(R) \cap P$, i.e., $P \leqslant N_G(R)$. Additionally, $Q \leqslant N_G(R)$. Therefore, $R \trianglelefteqslant P{:}Q = G$.

Conversely, assume that $R \trianglelefteqslant G$. Since $P \cap R = 1$, it is clear that $M = P \times R$. Additionally, as $G = P{:}Q^g$ for each $g \in G$, we see that

$$M \cap (\Phi(P)Q)^g = (P \times R) \cap \Phi(P)Q^g = (P \cap \Phi(P))(R \cap Q^g) = \Phi(P) \times R.$$

Similarly, $\Phi(P) \times R$ is the intersection of each pair of distinct $G$-conjugates of $\Phi(P)Q$, and in particular $\Phi(G) = \Phi(P) \times R$. Thus (ii)(b)–(c) hold.

To prove (ii)(d), we will again assume that $R \trianglelefteqslant G$. Observe that $C_M(\Phi(G)) = C_{P\times R}(\Phi(P) \times R) = C_P(\Phi(P)) \times R$. As $\Phi(P)$ is a characteristic subgroup of $P$, so is $C_P(\Phi(P))$. Hence $C_P(\Phi(P)) \trianglelefteqslant G$, and thus $C_P(\Phi(P))Q$ is a subgroup of $G$. As $\Phi(P)Q$ is the unique maximal subgroup of $G$ containing $Q$, and $P \cap Q = 1$, it follows that either $C_P(\Phi(P)) \leqslant \Phi(P)$ or $C_P(\Phi(P)) = P$. In the former case, $C_M(\Phi(G)) \leqslant \Phi(P) \times R = \Phi(G)$.

Suppose therefore that $M$ is non-abelian, and that $C_M(\Phi(G)) \not\leqslant \Phi(G)$, so that $C_P(\Phi(P)) = P$. Then $C_M(\Phi(G)) = P \times R = M$, and hence $\Phi(G) \leqslant Z(M)$. Assume for a contradiction that $\Phi(G) \neq Z(M)$, so that $Z(M) \not\leqslant \Phi(G) = M \cap \Phi(P)Q$. Then $Z(M) \not\leqslant \Phi(P)Q$, and applying Corollary 2.1.11 to the pair $(M, \Phi(P)Q)$ yields $\Phi(G) = M \cap \Phi(P)Q \not\leqslant Z(M)$, a contradiction. Thus $\Phi(G) = Z(M)$. As $\Phi(G) = \Phi(P) \times R$ and $Z(M) = Z(P) \times R$, we obtain (ii)(d). □

We will see at the end of this section, and in subsequent sections, that finite groups satisfying a certain set of properties related to the above theorem are very interesting, in terms of the structures of their non-commuting, non-generating graphs. For convenience, we will collect these properties in the following assumption, which utilises Theorem 5.7.2(i).

**Assumption 5.7.3.** Assume that $G$ is finite and contains exactly two conjugacy classes of maximal subgroups, i.e., that $G = P{:}Q$, where $P$ and $Q$ are nontrivial Sylow subgroups of coprime order such that $Q$ is cyclic and acts irreducibly on $P/\Phi(P)$. In addition, assume that $\Phi(P) = Z(P) \not\leqslant Z(G)$, and that the unique maximal subgroup of $Q$ is normal in $G$.

Observe that if a group $G$ satisfies this assumption, then Theorem 5.7.2(ii)(c) shows that $\Phi(G)$ is the intersection of each pair of distinct maximal subgroups of $G$.

We now focus on the case where $G$ is a group containing a normal, non-abelian maximal subgroup $M$ with $Z(G) < Z(M)$. By Proposition 2.1.7, this last condition is equivalent to the condition $Z(M) \not\leqslant Z(G)$.

The following three results will be key tools when bounding the distance in $\Xi(G)$ between an element of $M \setminus Z(M)$ and an element of $Z(M) \setminus Z(G)$.

**Lemma 5.7.4.** *Suppose that $G$ contains a normal, non-abelian maximal subgroup $M$ with $Z(G) < Z(M)$, and let $z \in Z(M) \setminus Z(G)$. Then $G \setminus M$ is the set of neighbours of $z$ in $\Xi(G)$.*

*Proof.* As $M$ is non-abelian, Proposition 2.1.2 shows that $G/Z(M)$ is not cyclic. Furthermore, $M = C_G(z)$ by Proposition 2.1.7. Thus we deduce the result from Proposition 5.2.10. □

**Lemma 5.7.5.** *Suppose that $G$ contains a normal, non-abelian maximal subgroup $M$ with $Z(G) < Z(M)$. In addition, let $x \in M \setminus Z(M)$ and $z \in Z(M) \setminus Z(G)$, and let $\mathcal{J}_M$ be the set of maximal subgroups of $G$ distinct from $M$. If $\langle I \cap M \mid I \in \mathcal{I} \rangle = M$ for some $\mathcal{I} \subseteq \mathcal{J}_M$, then there exists $I \in \mathcal{J}_M$ such that $x \notin C_M(I \cap M)$. More generally, if such $I$ exists, then $d(x, z) \leqslant 3$.*

*Proof.* First, if $\langle I \cap M \mid I \in \mathcal{I} \rangle = M$ for some $\mathcal{I} \subseteq \mathcal{J}_M$, then $\bigcap_{I \in \mathcal{I}} C_M(I \cap M) = Z(M)$, and so there exists $I \in \mathcal{I}$ such that $x \notin C_M(I \cap M)$.

We now assume, more generally, that there exists $I \in \mathcal{J}_M$ such that $x \notin C_M(I \cap M)$. Then $C_{I \cap M}(x) < I \cap M$. By Lemma 2.1.12, $I$ is non-abelian, and so there exists $s \in I \setminus (Z(I) \cup M)$. Applying Proposition 5.4.1(i) to the triple $(s, I, M)$ yields $C_{I \cap M}(s) < I \cap M$. Therefore, there exists an element $t \in I \cap M$ that centralises neither $x$ nor $s$. In addition, $s \sim z$ by Lemma 5.7.4. Thus $(x, t, s, z)$ is a path in $\Xi(G)$, and $d(x, z) \leqslant 3$. □

**Lemma 5.7.6.** *Suppose that $G$ contains a normal, non-abelian maximal subgroup $M$ with $Z(G) < Z(M)$, and a maximal subgroup $K \neq M$ that satisfies at least one of the following:*

(i) *$K \trianglelefteqslant G$;*

(ii) *$K \cap M$ is a maximal subgroup of $M$;*

(iii) *$Z(M) \not\leqslant K$; or*

(iv) *$Z(K) \neq Z(G)$.*

*Then $C_M(K \cap M) \subseteq K \cup Z(M)$.*

*Proof.* If each element of $M \setminus Z(M)$ lies in $K$, then the result is clear. Assume therefore that there exists an element $x \in M \setminus Z(M)$ that does not lie in $K$. It suffices to show that if any of (i)–(iv) hold, then $x \notin C_M(K \cap M)$. If (i) or (ii) holds, then applying Proposition 5.4.1(i) to the triple $(x, M, K)$ yields $C_{K \cap M}(x) < K \cap M$. Hence $x \notin C_M(K \cap M)$.

Suppose next that (iii) holds. As $Z(M) \trianglelefteqslant G$, we deduce that $G = Z(M)K$. Lemma 2.1.1 therefore gives $Z(M)(K \cap M) = Z(M)K \cap M = G \cap M = M$. Since $C_G(x)$ contains $Z(M)$ but not $M$, we see that $K \cap M \not\leqslant C_G(x)$, and therefore $x \notin C_M(K \cap M)$.

Finally, suppose that (iv) holds. By the previous paragraphs, we may assume that (i) and (iii) do not hold, so that $Z(M) \leqslant K \not\trianglelefteqslant G$. Since $Z(K) \neq Z(G)$ by assumption, it follows from Proposition 2.1.6 that $Z(G) < Z(K)$, and Proposition 2.1.7 implies that $C_G(Z(K)) = K$. Additionally, applying Corollary 2.1.8 to the pair $(M, K)$ shows that $Z(K) \leqslant K \cap M$. Thus $C_M(K \cap M) \leqslant C_M(Z(K)) = K \cap M$, which is indeed a subset of $K \cup Z(M)$. □

We can now state our first main result that bounds distances in $\Xi(G)$ involving elements of $M \setminus Z(M)$. Recall from Corollary 5.2.7 that if $G$ is non-abelian and not 2-generated, then $\operatorname{diam}(\Xi(G)) = 2$.

**Lemma 5.7.7.** *Suppose that $G$ is finitely generated and contains a normal, non-abelian maximal subgroup $M$ with $Z(G) < Z(M)$. In addition, let $x \in M \setminus Z(M)$ and $z \in Z(M) \setminus Z(G)$. Then the following statements hold.*

(i) *$x$ and $z$ lie in distinct connected components of $\Xi(G)$ if and only if $K \cap M = Z(M)$ for every maximal subgroup $K$ of $G$ distinct from $M$. Otherwise, $d(x, z) \leqslant 4$.*

(ii) *Suppose that $d(x, z) < \infty$. Then $d(x, z) = 4$ if and only if, for each maximal subgroup $K$ of $G$ distinct from $M$:*

  (a) *$x \notin K$; and*

  (b) *$x \in C_M(K \cap M)$.*

(iii) *Suppose that* (ii)(a)–(b) *hold for each maximal subgroup $K$ of $G$ distinct from $M$. Then $K \cap M = \Phi(G)$ for all such $K$.*

(iv) *Suppose that $d(x, z) < \infty$, and that $G$ is finite. Then $d(x, z) \leqslant 3$.*

*Proof.* Lemma 2.1.12 implies that $G$ contains no abelian maximal subgroups, while Proposition 2.1.5 shows that each proper subgroup of $G$ lies in a maximal subgroup. Additionally, $M = C_G(z)$ by Proposition 2.1.7, and Lemma 5.7.4 shows that $G \setminus M$ is the set of neighbours of $z$ in $\Xi(G)$.

(i) Suppose first that $K \cap M = Z(M)$ for every maximal subgroup $K$ of $G$ distinct from $M$, and let $y \in (G \setminus M) \cup Z(M)$. Then $M$ is the unique maximal subgroup

of $G$ containing $x$, and so if $\langle x, y\rangle < G$, then $y \in Z(M)$, and hence $[x, y] = 1$. Thus there is no edge in $\Xi(G)$ between any element of $M \setminus Z(M)$ and any element of $(G \setminus M) \cup Z(M) = G \setminus (M \setminus Z(M))$. In particular, the connected component of $\Xi(G)$ containing $x$ consists only of elements of $M \setminus Z(M)$, and so this component does not contain $z \in Z(M)$.

Conversely, suppose that there exists a maximal subgroup $L$ of $G$ distinct from $M$ that satisfies $L \cap M \neq Z(M)$. We claim that $L \cap M \not\leqslant Z(M)$. Indeed, either $Z(M) \not\leqslant L \cap M$ or $L \cap M \not\leqslant Z(M)$, and if the former holds, then applying Corollary 2.1.11 to the pair $(M, L)$ yields $L \cap M \not\leqslant Z(M)$. Additionally, as $L$ is non-abelian, there exists $r \in L \setminus (Z(L) \cup M)$. Applying Proposition 5.4.1(i) to the triple $(r, L, M)$ yields $C_{L\cap M}(r) < L \cap M$, and so $Z(L) \cap M < L \cap M$. We also see, since $L \cap M \not\leqslant Z(M)$, that $L \cap Z(M) < L \cap M$. Thus there exists an element $s \in (L \cap M) \setminus (Z(L) \cup Z(M))$, and an element $t \in L \setminus (C_L(s) \cup M)$. Corollary 5.2.8 gives $d(x, s) \leqslant 2$, and as $G \setminus M$ is the neighbourhood of $z$ in $\Xi(G)$, we observe that $s \sim t \sim z$. Therefore, $d(x, z) \leqslant d(x, s) + d(s, z) \leqslant 4$.

(ii) Assume first that (a) and (b) hold for each maximal subgroup $K$ of $G$ distinct from $M$. We will show that $d(x, z) = 4$. As $G \setminus M$ is the set of neighbours of $z$ in $\Xi(G)$, it suffices by (i) to show that $d(x, t) \geqslant 3$ for all $t \in G \setminus M$. Suppose for a contradiction that $d(x, t) \leqslant 2$ for some $t$. By (a), $\langle x, t\rangle = G$, and so $d(x, t) = 2$. This implies that there exists an element $s \in M$ such that $x \sim s \sim t$, and so $\langle s, t\rangle$ lies in a maximal subgroup $R$ of $G$. However, $x$ centralises $s \in R \cap M$ by (b), a contradiction. Thus $d(x, z) = 4$.

Conversely, suppose that some maximal subgroup $K$ of $G$ distinct from $M$ fails to satisfy either (a) or (b). We will prove that $d(x, z) \leqslant 3$. If $K$ does not satisfy (b), i.e., if $x \notin C_M(K \cap M)$, then this is an immediate consequence of Lemma 5.7.5, with $I = K$.

Assume therefore that $K$ does not satisfy (a), i.e., that $x \in K$. If $x \notin Z(K)$, then $C_K(x)$ and $C_K(z) = K \cap M$ are proper subgroups of $K$. Hence there exists an element $r \in K \setminus M$ that does not centralise $x$. As $G \setminus M$ is the neighbourhood of $z$ in $\Xi(G)$, it follows that $x \sim r \sim z$ and $d(x, z) = 2$.

Suppose now that $x \in Z(K)$. Then $K = C_G(x)$ by Proposition 2.1.7, and since $x$ also lies in $M \setminus Z(G)$, applying Corollary 2.1.8 to the pair $(K, M)$ implies that $Z(M) \leqslant K \cap M$. As $C_G(z) = M$, we deduce that $z \in K \setminus Z(K)$. If $K \trianglelefteq G$, then applying Lemma 5.4.2 to the 4-tuple $(x, M, z, K)$ gives $d(x, z) \leqslant 3$ (and in fact $d(x, z) = 2$ since $x \in K$ and $z \in M$).

If instead $C_G(x) = K$ is not normal in $G$, then there exists $g \in G$ such that $K^g \neq K$. If $x \in K^g$, then since $x \notin Z(K^g)$, applying the second last paragraph with $K^g$ in place of $K$ yields $d(x, z) = 2$. Otherwise, $x \notin K^g = C_G(x)^g = C_G(x^g)$, and since $x^g \in K^g \cap M^g = K^g \cap M$, we obtain $d(x, z) \leqslant 3$ by setting $I = K^g$ in Lemma 5.7.5.

(iii) Let $\mathcal{J}_M$ be the set of maximal subgroups of $G$ distinct from $M$, and suppose for a contradiction that $K \cap M \neq \Phi(G)$ for some $K \in \mathcal{J}_M$. We will show that there exists a subset $\mathcal{I}$ of $\mathcal{J}_M$ such that $\langle I \cap M \mid I \in \mathcal{I}\rangle = M$. It will follow from Lemma 5.7.5 that (ii)(b) does not hold for some $I \in \mathcal{J}_M$, a contradiction. Note that, since $x \in C_M(R \cap M) \setminus R$ for all $R \in \mathcal{J}_M$ by (ii)(a)–(b), while $x \notin Z(M)$, Lemma 5.7.6 implies that no such $R$ is normal in $G$, i.e., $M$ is the unique normal maximal subgroup of $G$.

Suppose first that there exists $R \in \mathcal{J}_M$ such that $R \cap M \not\trianglelefteqslant G$. Proposition 2.1.9 shows that $R \cap M$ is a maximal subgroup of $R$, which is not normal in $G$, and thus $\langle R \cap M\rangle^G \not\leqslant R$. However, $\langle R \cap M\rangle^G \leqslant M$, since $M \trianglelefteqslant G$. If $\langle R \cap M\rangle^G \neq M$, then we can apply Proposition 2.1.10 to the triple $(\langle R \cap M\rangle^G, M, R)$ of distinct subgroups, and this yields $R \cap M \not\leqslant \langle R \cap M\rangle^G$, a contradiction. Therefore, $\langle R \cap M\rangle^G = M$. Since $M \trianglelefteqslant G$, the subgroup $\langle R \cap M\rangle^G$ is equal to $\langle R^g \cap M \mid g \in G\rangle$, and so we can set $\mathcal{I} = \{R^g \mid g \in G\}$.

Assume finally that $R \cap M \trianglelefteqslant G$ for all $R \in \mathcal{J}_M$. Since $K \cap M \neq \Phi(G)$, Lemma 5.7.1 implies that there exists a maximal subgroup $L \in \mathcal{J}_M$ such that $L \cap M \neq K \cap M$. Either $K \cap M \not\leqslant L$ or $L \cap M \not\leqslant K$, and if the former holds, then since $K \cap M \trianglelefteqslant G$, applying Proposition 2.1.10 to the triple $(K, M, L)$ shows that the latter holds too. Thus, in general, $L \cap M \not\leqslant K$. As $L \cap M \trianglelefteqslant G$, it follows that $(L \cap M)K = G$, and so applying Lemma 2.1.1 to the subgroups $L \cap M$, $K$ and $M$ gives $(L \cap M)(K \cap M) = ((L \cap M)K) \cap M = G \cap M = M$. We can therefore set $\mathcal{I} = \{K, L\}$.

(iv) By (i), $d(x, z) \leqslant 4$, and there exists a maximal subgroup $K$ of $G$ distinct from $M$ with $K \cap M \neq Z(M)$. Suppose for a contradiction that $d(x, z) = 4$. Then (ii) shows that each maximal subgroup $L$ of $G$ distinct from $M$ satisfies $x \in C_M(L \cap M) \setminus L$. As $x \notin Z(M)$, Lemma 5.7.6 yields $L \not\trianglelefteqslant G$. Additionally, (iii) implies that $\Phi(G) = L \cap M$ for each $L$, and that $C_M(\Phi(G))$ is not a subgroup of $\Phi(G)$. Thus Lemma 5.7.1 implies that the finite group $G$ contains exactly two conjugacy classes of maximal subgroups. Since $M$ is the unique normal maximal subgroup of $G$, and since $\Phi(G) = K \cap M$, the equivalent conditions of part (b) of Theorem 5.7.2(ii) hold. In addition, $M$ is non-abelian

and $\Phi(G) = K \cap M \neq Z(M)$, and so part (d) of that theorem shows that $C_M(\Phi(G)) \leqslant \Phi(G)$, a contradiction. Thus $d(x, z) \leqslant 3$. □

The previous result leads to the following open question.

**Question 5.7.8.** *Consider the family $\mathcal{G}$ of finitely generated infinite groups $G$ that contain a normal, non-abelian maximal subgroup $M$ with $Z(G) < Z(M)$. Is there a group $G \in \mathcal{G}$ such that each maximal subgroup $K$ of $G$ distinct from $M$ satisfies properties (a) and (b) from Lemma 5.7.7(ii), and such that some maximal subgroup $L$ satisfies $L \cap M \neq Z(M)$? Equivalently, does there exist $G \in \mathcal{G}$, $x \in M \setminus Z(M)$ and $z \in Z(M) \setminus Z(G)$ such that $d(x, z) = 4$?*

Note that, for any such $G \in \mathcal{G}$, no maximal subgroup $K$ of $G$ distinct from $M$ can satisfy any of the properties listed in Lemma 5.7.6; otherwise, $G$ would not satisfy properties (a) and (b) from Lemma 5.7.7(ii).

The next few results will allow us to determine upper bounds for distances in $\Xi(G)$ between elements of $M \setminus Z(M)$ and elements of $G \setminus M$. In the first two of these results, we relax the condition that $Z(G) < Z(M)$, and if $H$ is a subgroup of $G$ containing $Z(M)$, then we write $\overline{H} := H/Z(M)$. Recall also Definition 2.1.22, of an abstract primitive group.

**Proposition 5.7.9.** *Suppose that $G$ contains a normal, non-abelian maximal subgroup $M$, and a maximal subgroup $K$ with $K \cap M = Z(M)$. Then the following statements hold.*

(i) *$\overline{G}$ is primitive, and is the semidirect product of its unique minimal normal subgroup $\overline{M}$ by its point stabiliser $\overline{K}$, which has prime order.*

(ii) *$\overline{G}$ is finite if and only if it is soluble. Hence $G$ is soluble if and only if $\overline{G}$ is finite.*

(iii) *If $\overline{G}$ is infinite, then $\overline{M}$ is an infinite simple group, and $|\overline{K}|$ is odd.*

(iv) *If $G$ contains a maximal subgroup $L$ such that $L \neq M$ and $Z(M) < L \cap M$, then $\overline{G}$ is infinite.*

*Proof.* The subgroup $K$ of $G$ is not normal, as otherwise $Z(M)$ would be a maximal subgroup of $M$ by Proposition 2.1.9, contradicting Proposition 2.1.2. Additionally, Proposition 2.1.9 implies that $Z(M)$ is a maximal subgroup of $K$. As $Z(M) \trianglelefteq G$, it follows that $\mathrm{Core}_G(K) = Z(M)$.

We now observe that $\overline{K}$ is a core-free maximal subgroup of $\overline{G}$, and hence $\overline{G}$ is primitive with point stabiliser $\overline{K}$. Additionally, $\overline{M}$ is a normal subgroup of $\overline{G}$ that

intersects $\overline{K}$ trivially, and hence $\overline{G} = \overline{M}{:}\overline{K}$. It is also clear that each nontrivial normal subgroup $\overline{N}$ of $\overline{G}$ contained in $\overline{M}$ intersects $\overline{K}$ trivially. Since $\overline{N}\,\overline{K} = \overline{G}$ by the maximality of $\overline{K}$, we deduce that $\overline{N} = \overline{M}$, and so $\overline{M}$ is a minimal normal subgroup of $\overline{G}$. In addition, as $Z(M)$ is a maximal subgroup of $K$, the maximal subgroup $\overline{K}$ of $\overline{G}$ is cyclic of prime order.

Now, if $\overline{G}$ is finite, then since its subgroup $\overline{K}$ is maximal and abelian, Theorem 2.1.16 implies that $\overline{G} = G/Z(M)$ is soluble. As the abelian group $Z(M)$ is also soluble, it follows that $G$ is soluble. In this case, Theorem 2.1.24 shows that $\overline{M}$ is the unique minimal normal subgroup of $\overline{G}$. If instead $\overline{G}$ is infinite, then since $\overline{K}$ is finite, [132, Theorem 1.1] shows that $\overline{M}$ is a direct product of isomorphic infinite simple groups, and is again the unique minimal normal subgroup of $\overline{G}$. Thus in this case, the quotient $\overline{G}$ of $G$ is not soluble, and so neither is $G$ itself. In fact, arguing as in the proof of [77, Theorem 4.1], we deduce that the infinite group $\overline{M}$ is simple, and that $|\overline{K}|$ is odd. Thus we have proved (i), (ii) and (iii).

Finally, suppose that $G$ contains a maximal subgroup $L$ as in (iv). Since the unique minimal normal subgroup of $\overline{G}$ is its maximal subgroup $\overline{M}$, the maximal subgroup $\overline{L}$ of $\overline{G}$ is core-free. Additionally, $\overline{K} \cap \overline{M} = 1 \neq \overline{L} \cap \overline{M}$, and thus the core-free maximal subgroup $\overline{K}$ of $G$ is not conjugate to $\overline{L}$. Theorem 2.1.17 therefore implies that $\overline{G}$ is not a finite soluble group. Hence by (ii), $\overline{G}$ is infinite, and we obtain (iv). □

**Lemma 5.7.10.** *Suppose that $G$ contains a normal, non-abelian maximal subgroup $M$. In addition, let $x \in M \setminus Z(M)$ and $y \in G \setminus M$. Finally, suppose that $R$ is a maximal subgroup of $G$ containing $y$, with $C_{R\cap M}(y) < R \cap M \neq Z(M)$. Then $d(x, y) \leqslant 3$.*

*Proof.* Either $Z(M) \not\leqslant R$ or $R \cap M \not\leqslant Z(M)$, and if the former holds, then applying Corollary 2.1.11 to the pair $(M, R)$ shows that the latter also holds. Thus, in general, $R \cap M \not\leqslant Z(M)$, and so $R \cap Z(M) < R \cap M$. Since $C_{R\cap M}(y) < R \cap M$, there exists $h \in R \cap M$ with $h \notin C_{R\cap M}(y) \cup Z(M)$. We see that $h \sim y$, while $d(x, h) \leqslant 2$ by Corollary 5.2.8. Therefore, $d(x, y) \leqslant d(x, h) + d(h, y) \leqslant 3$. □

**Lemma 5.7.11.** *Suppose that $G$ contains a normal, non-abelian maximal subgroup $M$, with $Z(G) < Z(M)$. In addition, suppose that $G$ contains maximal subgroups $K$ and $L$, with $K \cap M = Z(M) \not\leqslant L$ and $L \not\trianglelefteq G$. Then the following statements hold.*

(i) *$U := L \cap M$ is a normal subgroup of $G$.*

(ii) *$C_M(U) = Z(M)$.*

(iii) *Let* $s \in L \cap (K \setminus Z(M))$. *Then* $S := \{[s,r] \mid r \in Z(M)\}$ *is a normal subgroup of* $G$, *and* $SU = M$.

(iv) *Each element of* $K \setminus Z(M)$ *lies in some* $G$*-conjugate of* $L$.

*Proof.* We first note that $G = Z(M)L$, since the maximal subgroup $L$ of $G$ does not contain $Z(M) \trianglelefteq G$.

(i) Observe that $U \trianglelefteq L$. Additionally, $U \leqslant M$, and hence $U$ is centralised by $Z(M)$. Therefore, $U \trianglelefteq Z(M)L = G$.

(ii) Let $c \in C_M(U)$. Then $c$ is centralised by $Z(M)U = Z(M)(L \cap M)$, which Lemma 2.1.1 shows is equal to $Z(M)L \cap M = G \cap M = M$. Hence $c \in Z(M)$. It is clear that $Z(M) \leqslant C_M(U)$, and the result follows.

(iii) Let $x, y \in Z(M)$. As $Z(M) \trianglelefteq G$, it follows that $[s,y] \in Z(M)$. Therefore,

$$\begin{aligned}[s,x][s,y] &= s^{-1}x^{-1}sx[s,y] = s^{-1}x^{-1}s[s,y]x = s^{-1}x^{-1}ss^{-1}y^{-1}syx \\ &= s^{-1}x^{-1}y^{-1}syx = [s,yx].\end{aligned}$$

In particular, $[s,x][s,x^{-1}] = [s,1] = 1$. Hence $S$ is a subgroup of $G$.

Next, since $S \leqslant Z(M)$, we deduce that $S \trianglelefteq M$. Additionally, $x^s \in Z(M)$, and hence $[s,x]^s = [s^s, x^s] = [s,x^s] \in S$. Thus $S^s = S$. As $s \in K \setminus Z(M)$, we see that $s \notin M$ and $\langle M, s\rangle = G$. Therefore, $S \trianglelefteq G$.

Now, by (i), $U \trianglelefteq G$. For a subgroup $T$ of $G$, let $\overline{T} := TU/U$, and for an element $g \in G$, let $\overline{g} := Ug$. Proposition 2.1.9 implies that $U$ is a maximal subgroup of $L$. Since $L \ntrianglelefteq G$, it follows that $\overline{L}$ is a core-free maximal subgroup of $\overline{G}$, and so $\overline{G}$ is primitive. Note also that $\overline{G}$ is not cyclic of prime order, as $U$ is not maximal in $G$. Thus Proposition 2.1.23 gives $Z(\overline{G}) = 1$.

Let $r \in Z(M) \setminus L$. Then $\overline{r} \in Z(\overline{M}) \setminus Z(\overline{G})$, and it follows from Proposition 2.1.7 that $C_{\overline{G}}(\overline{r}) = \overline{M}$. As $s \notin M$, we deduce that $\overline{[s,r]} = [\overline{s},\overline{r}] \neq 1$, and thus $[s,r] \notin U = L \cap M$. Since $S \leqslant M$, it follows that $S \not\leqslant L$. Additionally, as $S \trianglelefteq G$ and $L$ is maximal in $G$, we obtain $SL = G$. Moreover, $SU = S(L \cap M)$ is a subgroup of $G$. Using Lemma 2.1.1, we conclude that $S(L \cap M) = SL \cap M = G \cap M = M$, as required.

(iv) Let $k \in K \setminus Z(M)$. As $G = Z(M)L$, it follows that $k = zf$ for some $z \in Z(M)$ and some $f \in L$, with $f \notin Z(M)$. In fact, since $Z(M) \leqslant K$, we see that $f = z^{-1}k \in K \setminus Z(M)$. Hence $f^{-1} \in L \cap (K \setminus Z(M))$.

Let $S := \{[f^{-1}, r] \mid r \in Z(M)\}$. Then $SU = M$ by (iii). As $U \trianglelefteq G$ by (i), we deduce that $Z(M)U/U \leqslant M/U = SU/U$. Thus there exists $r \in Z(M)$ such that $z^{-1}U = Uz^{-1} = U[f^{-1}, r]$, and hence $z[f^{-1}, r] \in U$. As $U = U^r \leqslant L^r$, it follows that $L^r$ contains the element $z[f^{-1}, r]f^r = zf = k$. □

We are now ready to state our main result bounding distances in $\Xi(G)$ between elements of $M \setminus Z(M)$ and elements of $G \setminus M$. As above, we will assume that $G$ is finitely generated, as otherwise $\operatorname{diam}(\Xi(G)) = 2$ by Corollary 5.2.7.

**Lemma 5.7.12.** *Suppose that $G$ is finitely generated and contains a normal, non-abelian maximal subgroup $M$, with $Z(G) < Z(M)$. In addition, let $x \in M \setminus Z(M)$ and $y \in G \setminus M$.*

(i) *$x$ and $y$ lie in distinct connected components of $\Xi(G)$ if and only if $K \cap M = Z(M)$ for every maximal subgroup $K$ of $G$ distinct from $M$.*

(ii) *If $x$ and $y$ lie in the same connected component of $\Xi(G)$, then $d(x, y) \leqslant 4$.*

(iii) *If $d(x, y) = 4$, then $\Phi(G) = Z(M)$, and $G/Z(M)$ is primitive with unique minimal normal subgroup $M/Z(M)$, which is infinite and simple. Moreover, each maximal subgroup $K$ of $G$ containing $y$ satisfies $K \cap M = Z(M)$, and $K/Z(M)$ is a point stabiliser of $G/Z(M) = (M/Z(M)) : (K/Z(M))$ of odd prime order.*

*Proof.* We first observe from Lemma 2.1.12 that $G$ contains no abelian maximal subgroup, and from Proposition 2.1.5 that each proper subgroup of $G$ lies in a maximal subgroup. Let $z \in Z(M) \setminus Z(G)$. Then $y \sim z$ by Lemma 5.7.4, and so $x$ and $y$ lie in the same connected component of $\Xi(G)$ if and only if $x$ and $z$ lie in the same component. Thus (i) follows from Lemma 5.7.7(i).

Assume now that $x$ and $y$ lie in the same connected component of $\Xi(G)$. We split the rest of the proof into two cases.

**Case (a)**: $\Phi(G) = Z(M)$. Let $K$ be a maximal subgroup of $G$ containing $y$, so that $K \neq M$, and suppose that $d(x, y) > 3$. Since $K \cap M$ contains $\Phi(G) = Z(M) > Z(G)$, we deduce from Corollary 2.1.8, applied to the pair $(M, K)$, that $Z(K) \leqslant K \cap M$. As $y \notin M$, it follows that $y \notin Z(K)$. Thus applying Proposition 5.4.1(i) to the triple $(y, K, M)$ yields $C_{K\cap M}(y) < K \cap M$. Since $d(x, y) > 3$, Lemma 5.7.10 shows that $K \cap M = Z(M)$. On the other hand, as $x$ and $y$ lie in the same component of $\Xi(G)$, we see from (i) that there exists a maximal subgroup $L$ of $G$ with $L \neq M$ and $L \cap M \neq Z(M)$. This means that $\Phi(G) = Z(M) < L \cap M$, and so Lemma 5.7.7 gives $d(x, z) \leqslant 3$. Thus $d(x, y) = d(x, z) + d(y, z) = 4$.

Finally, as $K \cap M = Z(M) < L \cap M$, Proposition 5.7.9(iv) shows that $G/Z(M)$ is infinite, and hence the claims about $G/Z(M)$, $M/Z(M)$ and $K/Z(M)$ in (iii) follow from Proposition 5.7.9(i)–(iii).

**Case (b)**: $\Phi(G) \neq Z(M)$. To complete the proof of (ii) and (iii), it suffices to show that $d(x, y) \leqslant 3$. Since $y \sim z$, there exists a (non-abelian) maximal subgroup $K$ of $G$ containing $y$ and $z$. Note that $z \in (K \cap M) \setminus C_G(y)$, and so $C_{K\cap M}(y) < K \cap M$. Thus by Lemma 5.7.10, we may assume that $K \cap M = Z(M)$, and so $\Phi(G) < Z(M)$. Some maximal subgroup $L$ of $G$ therefore satisfies $Z(M) \not\leqslant L$. We will show that $Z(L) \leqslant Z(G)$.

As $Z(M) \trianglelefteqslant G$, we see that $G = Z(M)L$, and hence $G/Z(M) = Z(M)L/Z(M) \cong L/(L \cap Z(M))$. Since $G/Z(M)$ is primitive by Proposition 5.7.9 (and $Z(M)$ is not maximal in $G$), we deduce from Proposition 2.1.23 that $L/(L \cap Z(M))$ has trivial centre. Hence $Z(L) \leqslant L \cap Z(M) \leqslant M$. As $Z(M) \not\leqslant L \cap M$, the contrapositive of Corollary 2.1.8, applied to the pair $(L, M)$, shows that $Z(L) = Z(L) \cap M \leqslant Z(G)$.

We divide the remainder of Case (b) into three (not all mutually exclusive) sub-cases.

**Case (b)($\alpha$)**: $y \in L^g$ for some $g \in G$. Since $y \notin Z(G)$ and $Z(L^g) \leqslant Z(G)$, applying Proposition 5.4.1(i) to the triple $(y, L^g, M)$ yields $C_{L^g\cap M}(y) < L^g \cap M \neq Z(M)$. Thus $d(x, y) \leqslant 3$ by Lemma 5.7.10.

**Case (b)($\beta$)**: $L \not\trianglelefteqslant G$. Since $y \in K \setminus Z(M)$, it follows from Lemma 5.7.11(iv) that $y \in L^g$ for some $g \in G$. Thus by the previous sub-case, $d(x, y) \leqslant 3$.

**Case (b)($\gamma$)**: $L \trianglelefteqslant G$ and $y \notin L$. Applying Proposition 5.4.1(i) to the triple $(y, K, L)$ shows that $r \sim y$ for some $r \in K \cap L$, and that $C_{K\cap L}(y) < K \cap L$. If $x \in L$, then (since $Z(L) \leqslant Z(G)$) Corollary 5.2.8 yields $d(x, r) \leqslant 2$, and so $d(x, y) \leqslant 3$.

If instead $x \notin L$, then since $K \cap M = Z(M) \not\leqslant L$, applying Proposition 2.1.10 to the triple $(K, M, L)$ shows that $L \cap M \not\leqslant K$. Therefore, applying the same proposition to the triple $(M, L, K)$ yields $K \cap L \not\leqslant M$. Thus there exists $t \in (K\cap L)\setminus M$, and in particular $t \notin Z(G) = Z(L)$. It follows from Proposition 5.4.1(ii), applied to the triple $(x, M, L)$ and the element $t$, that $x \sim s \sim t$ for some $s \in L \cap M$. As $s \sim t \in K \cap L$, we see that $C_{K\cap L}(s) < K \cap L$. Additionally, $C_{K\cap L}(y) < K \cap L$ by the previous paragraph. Hence there exists an element $f \in K \cap L$ that centralises neither $s$ nor $y$. Since $y \in K$, we see that $x \sim s \sim f \sim y$ and $d(x, y) \leqslant 3$. □

The above lemma is again associated with open questions.

**Question 5.7.13.** *Consider the family $\mathcal{G}$ of finitely generated infinite groups $G$ that contain a normal, non-abelian maximal subgroup $M$ with $Z(G) < Z(M)$. Is there*

*a group $G \in \mathcal{G}$ and an element $y \in G$ for which all of the necessary conditions given in Lemma 5.7.12(iii) are satisfied? If yes, for such $G$ and $y$, does there exist $x \in M \setminus Z(M)$ such that $d(x, y) = 4$?*

We note that Questions 5.7.8 and 5.7.13 can be partially addressed, as follows.

**Remark 5.7.14.** Let $x \in M \setminus Z(M)$, $z \in Z(M) \setminus Z(G)$ and $y \in G \setminus M$. Observe from Lemmas 5.7.7 and 5.7.12 that if $d(x, z) = 4$, then $K \cap M = \Phi(G) \neq Z(M)$ for each maximal subgroup $K$ of $G$ distinct from $M$, while if $d(x, y) = 4$, then there exists a maximal subgroup $L \neq M$ of $G$ such that $Z(M) = \Phi(G) < L \cap M$. Hence the distances $d(x, z)$ and $d(x, y)$ cannot both be equal to 4.

Our next result specifies exactly when $\Xi(G)$ is connected (assuming that $G$ contains a maximal subgroup $M$ as above). In the next section, we will consider in more detail the diameters of the connected components of this graph, and discuss several concrete examples.

**Lemma 5.7.15.** *Suppose that $G$ is finitely generated and contains a normal, non-abelian maximal subgroup $M$, with $Z(G) < Z(M)$. If $K \cap M = Z(M)$ for every maximal subgroup $K$ of $G$ distinct from $M$, then the elements of $M \setminus Z(M)$ form a connected component of $\Xi(G)$, and Proposition 5.7.9 applies to $G$, for any choice of $K$. Otherwise, $\Xi(G)$ is connected. In particular, if $G$ is finite, then $\Xi(G)$ is not connected if and only if $G$ satisfies Assumption 5.7.3.*

*Proof.* Suppose first that $K \cap M = Z(M)$ for every maximal subgroup $K$ of $G$ distinct from $M$. Then Proposition 5.7.9 applies to $G$, for any choice of $K$, and in particular $\mathrm{Core}_G(K) = Z(M)$. Thus $M$ is the unique normal maximal subgroup of $G$. It follows from Lemma 5.7.1 that if $G$ is finite, then it is soluble and contains exactly two conjugacy classes of maximal subgroups, and $Z(M) = \Phi(G)$ is the intersection of each pair of distinct maximal subgroups. Hence in this case $G$ satisfies all conditions of Theorem 5.7.2(i). In particular, $G$ has exactly two conjugacy classes of maximal subgroups, and a unique non-cyclic Sylow subgroup $P$. Furthermore, Theorem 5.7.2(ii) shows that $G$ has a nontrivial cyclic Sylow subgroup whose maximal subgroup is normal in $G$, and that $\Phi(P) = Z(P)$. As $Z(G) < Z(M) = \Phi(G)$, we also observe from this theorem that $\Phi(P) \not\leqslant Z(G)$. Thus $G$ satisfies Assumption 5.7.3.

Whether or not $G$ is finite, Lemmas 5.7.7 and 5.7.12 show that there is no path in $\Xi(G)$ between any element of $M \setminus Z(M)$ and any element of $(G \setminus M) \cup (Z(M) \setminus Z(G))$. However, Corollary 5.2.8 implies that any two vertices of $M \setminus Z(M)$ are joined by a path in $\Xi(G)$. Hence the elements of $M \setminus Z(M)$ form a connected component of $\Xi(G)$. As each element of $G \setminus M$ is a vertex of $\Xi(G)$, this graph is not connected.

If instead there exists a maximal subgroup $L$ of $G$ such that $L \neq M$ and $L \cap M \neq Z(M)$, then by Lemmas 5.7.7 and 5.7.12, there exists a path in $\Xi(G)$ between any element of $M \setminus Z(M)$ and any element of $(G \setminus M) \cup (Z(M) \setminus Z(G))$. Thus $\Xi(G)$ is connected. Suppose finally that $G$ is finite in this case. To show that Assumption 5.7.3 does not hold for $G$, we may assume that $G$ has exactly two conjugacy classes of maximal subgroups, and a nontrivial cyclic Sylow subgroup whose maximal subgroup is normal in $G$. Then parts (c) and (d) of Theorem 5.7.2(ii) imply that $\Phi(G) = L \cap M \neq Z(M)$, and hence that the unique non-cyclic Sylow subgroup $P$ of $G$ does not satisfy $\Phi(P) = Z(P)$. Since $\Phi(S) < S = Z(S)$ for each nontrivial Sylow subgroup $S \neq P$, we conclude that $G$ does not satisfy Assumption 5.7.3 □

In particular, Proposition 5.7.9 and Lemma 5.7.15 show that if $G$ is infinite and $\Xi(G)$ is not connected, then $G/Z(M)$ is primitive with a unique minimal normal subgroup, which is infinite and simple, and each point stabiliser of $G/Z(M)$ has odd prime order.

## 5.8 Non-central by non-cyclic groups

In this section, we consider in detail the non-commuting, non-generating graph of a group $G$ that satisfies the following assumption, i.e., that contains a non-central normal subgroup whose corresponding quotient is non-cyclic.

**Assumption 5.8.1.** Assume that $G$ contains a normal subgroup $N$, such that $G/N$ is not cyclic and $N \not\leqslant Z(G)$. Additionally, let $C := C_G(N)$.

In particular, we will determine upper bounds (or exact values in some cases) for the diameters of the connected components of $\Xi(G)$ whenever $G$ satisfies this assumption. Throughout this section, we will implicitly use Proposition 5.2.5, which states that each nontrivial connected component of $\Xi(G)$ has diameter at least 2.

The following proposition will be useful when investigating the structure of $\Xi(G)$. Here, and throughout this section, it will be useful to observe that $Z(G) \leqslant C < G$ and $C \trianglelefteqslant N_G(N) = G$. Furthermore, the characteristic subgroup $Z(C)$ of $C$ is normal in $G$.

**Proposition 5.8.2.** *Let $G$, $N$ and $C$ be as in Assumption 5.8.1.*

(i) *Let $h, h' \in G \setminus C$. Then $d(h, h') \leqslant 2$. In particular, there exists $n \in N \setminus Z(G)$ such that $h \sim n \sim h'$ is a path in $\Xi(G)$.*

(ii) *Let $c \in C \setminus Z(G)$ and $g \in G \setminus Z(G)$. If $d(c, g) > 2$, then either $G/\langle c \rangle^G$ and $G/\langle g \rangle^G$ are both cyclic, or one of these quotients is cyclic and $[c, g] = 1$.*

*Proof.*

(i) Since $h, h' \notin C$, each of $C_N(h)$ and $C_N(h')$ is a proper subgroup of $N$. Thus there exists $n \in N \setminus (C_N(h) \cup C_N(h'))$. As $G/N$ is not cyclic, Proposition 5.2.10 implies that $h \sim n \sim h'$, and hence $d(h, h') \leqslant 2$.

(ii) We prove the contrapositive of the given statement. Suppose first that $[c, g] \neq 1$, and that either $G/\langle c \rangle^G$ or $G/\langle g \rangle^G$ is not cyclic. Then Proposition 5.2.10 implies that $c \sim g$, i.e., $d(c, g) = 1$.

It remains to show that $d(c, g) \leqslant 2$ when $[c, g] = 1$ and when $G/\langle c \rangle^G$ and $G/\langle g \rangle^G$ are both non-cyclic. Since the non-commuting graph of $G$ is connected with diameter 2 by Proposition 5.2.6, there exists $k \in G \setminus Z(G)$ such that $(c, k, g)$ is a path in this graph. As $G/\langle c \rangle^G$ and $G/\langle g \rangle^G$ are non-cyclic, Proposition 5.2.10 shows that $(c, k, g)$ is also a path in $\Xi(G)$, and hence $d(c, g) \leqslant 2$. □

We now split the investigation of the structure of $\Xi(G)$ into three cases: $G/C$ non-cyclic; $G/C$ cyclic and $C$ abelian; and $G/C$ cyclic and $C$ non-abelian. In the second and third cases, we will see that more can be said if we know whether or not $C$ is a maximal subgroup of $G$.

**Lemma 5.8.3.** *Let $G$, $N$ and $C$ be as in Assumption 5.8.1, and suppose that $G/C$ is not cyclic. Then $\Xi(G)$ is connected with diameter 2 or 3. Moreover, if $d(x, y) = 3$ for $x, y \in G \setminus Z(G)$, then one of these elements lies in $C$, the other lies in $G \setminus (N \cup C)$, and $[x, y] = 1$. Hence $\operatorname{diam}(\Xi(G)) = 2$ if $C_G(x) \subseteq N \cup C$ for all $x \in C \setminus Z(G)$, and in particular if $C = Z(G)$.*

*Proof.* By Proposition 5.8.2(i), any two elements of $G \setminus C$ are joined in $\Xi(G)$ by a path of length at most two. Thus it suffices to consider distances in $\Xi(G)$ involving elements of $C \setminus Z(G)$.

Suppose that $x \in C \setminus Z(G)$ and $y \in G \setminus Z(G)$ satisfy $d(x, y) > 2$. As $G/N$ and $G/C$ are not cyclic, neither is $G/\langle r \rangle^G$ for any $r \in N \cup C$. In particular, $G/\langle x \rangle^G$ is not cyclic. Therefore, Proposition 5.8.2(ii) implies that $y \in G \setminus (N \cup C)$ and $[x, y] = 1$.

Now, Proposition 5.8.2(i) shows that $n \sim y$ for some $n \in N \setminus Z(G)$. By the previous paragraph, $d(x, n) \leqslant 2$, and so $d(x, y) \leqslant d(x, n) + d(n, y) \leqslant 3$. □

We will see later in this section that if $G$ has an abelian maximal subgroup, if the non-cyclic group $G/C$ is finite, and if either $N$ is abelian or $G/C_G(C)$ is finite, then $\operatorname{diam}(\Xi(G)) = 2$.

Using Magma, and in particular the code in `comp_nc_ng`, we see that the groups numbered $(24, 12)$ and $(24, 14)$ in the Small Groups Library [11] satisfy the hypotheses of Lemma 5.8.3, and have non-commuting, non-generating graphs of diameter 3 and 2, respectively. In fact, in the latter case, $C = Z(G)$, and $G$ has an abelian maximal subgroup. On the other hand, if $G = \text{SmallGroup}(36, 10)$, then $G$ satisfies the hypotheses of Lemma 5.8.3 and $\text{diam}(\Xi(G)) = 2$, even though $G$ has no abelian maximal subgroup and there exists $x \in C \setminus Z(G)$ such that $C_G(x) \not\subseteq N \cup C$.

We can also use Lemma 5.8.3 to determine the diameter of the non-commuting, non-generating graph of a certain 2-generated infinite group.

**Example 5.8.4.** Consider *Thompson's group* $F$, which is the 2-generated infinite group given by[3] the presentation $\langle a, b \mid [ab^{-1}, a^{-1}ba] = [ab^{-1}, a^{-2}ba^2] = 1\rangle$ [101, Example 2.2.21]. The derived subgroup $F'$ of $F$ is an infinite simple group, $F/F' \cong \mathbb{Z}^2$, and every proper quotient of $F$ is abelian [9, §1.4]. It follows from this last fact that $F'$ is the unique minimal normal subgroup of $F$.

Now, $C_F(F') \trianglelefteq F$. Since the simple group $F'$ is non-abelian, $C_F(F')$ cannot contain the minimal normal subgroup $F'$, and so $C_F(F') = 1$. As $F/F'$ is not cyclic, we can apply Lemma 5.8.3 with $G = F$ and $N = F'$ to deduce that $\Xi(F)$ is connected with diameter 2.

Next, we prove useful properties of $N$ and $C$ in the case where $G/C$ is cyclic.

**Proposition 5.8.5.** *Let $G$, $N$ and $C$ be as in Assumption 5.8.1, and suppose that $G/C$ is cyclic. Then the following statements hold.*

(i) *$N$ is abelian, and $N < C$.*

(ii) *Let $H$ be a subgroup of $G$ properly containing $C$. Then $H$ is non-abelian, $Z(H) < Z(C)$, and $H \trianglelefteq G$. In particular, $Z(G) < Z(C)$.*

(iii) *If $G$ contains an abelian maximal subgroup and $C$ is non-abelian, then $G/C \cong \mathbb{Z}$, and in particular, $C$ is not maximal in $G$.*

*Proof.*

(i) Since $G/C$ is cyclic, its subgroup $NC/C$ is also cyclic. This subgroup is isomorphic to $N/(N \cap C) = N/Z(N)$. Thus $N$ is abelian by Proposition 2.1.2, and so $N \leqslant C$. As $G/C$ is cyclic while $G/N$ is not, we conclude that $N < C$.

[3] Note also that $F$ can be defined as a certain set of piecewise linear homeomorphisms from the unit interval $[0, 1]$ to itself; see [9, §1.1].

(ii) By (i), $H$ contains $N$. Hence each of $N$ and $C$ is centralised by $Z(H)$, and so $Z(H) \leqslant C \cap C_G(C) = Z(C)$. However, $H$ does not centralise $N$. Thus $N \not\leqslant Z(H)$, and so $H$ is non-abelian. On the other hand, $N \leqslant Z(C)$ by (i), and it follows that $Z(H)$ is a proper subgroup of $Z(C)$. Additionally, $H/C$ is a normal subgroup of the cyclic group $G/C$, and hence $H \trianglelefteqslant G$.

(iii) By (ii), $Z(C) \not\leqslant Z(G)$. Thus Lemma 2.1.12 yields the result. □

Now, if $G$ is not finitely generated, then Corollary 5.2.7 shows that $\Xi(G)$ is connected with diameter 2. Hence in the following two results, we will assume that $G$ is finitely generated, so that, by Proposition 2.1.5, each proper subgroup of $G$ lies in a maximal subgroup.

Our next lemma explores the case where $G/C$ is cyclic and $C$ is abelian. Recall that $\Xi^+(G)$ denotes the subgraph of $\Xi(G)$ induced by its non-isolated vertices.

**Lemma 5.8.6.** *Let $G$, $N$ and $C$ be as in Assumption 5.8.1. Suppose also that $G$ is finitely generated, $G/C$ is cyclic, and $C$ is abelian. Then the following statements hold.*

(i) *$G$ is soluble.*

(ii) *Each isolated vertex of $\Xi(G)$ lies in $C \setminus N$.*

(iii) *Suppose that $C$ is maximal in $G$. Then $\Xi^+(G)$ is connected with diameter 2.*

(iv) *Suppose that $C$ is not maximal in $G$, and let $M$ be a maximal subgroup of $G$ containing $C$. Then Table 5.8.1 lists upper bounds for distances between vertices of $\Xi(G)$, depending on the subsets of $G \setminus Z(G)$ that contain them. In particular, $\operatorname{diam}(\Xi(G)) \leqslant 3$. Moreover, if $G$ contains an abelian maximal subgroup, then $\operatorname{diam}(\Xi(G)) = 2$.*

*Proof.*

(i) This is clear, since $G$ is an extension of the abelian group $C$ by the cyclic group $G/C$.

(ii) Observe from Proposition 5.8.2(i) that any two elements of $G \setminus C$ have distance at most two in $\Xi(G)$. In particular, no element of $G \setminus C$ is an isolated vertex. Additionally, as $G/N$ is not cyclic, and as the non-commuting graph of $G$ is connected by Proposition 5.2.6, it follows from Proposition 5.2.10 that no element of $N$ is an isolated vertex. Hence any isolated vertex lies in $C \setminus N$.

Table 5.8.1: Upper bounds for distances between vertices $x \in A$ and $y \in B$ of $\Xi(G)$, where $A$ and $B$ are specified subsets of $G \setminus Z(G)$, and $C$ and $M$ are as in Lemma 5.8.6(iv). Additionally, $\mathcal{A}$ denotes the family of groups that contain an abelian maximal subgroup.

| $A$ \ $B$ | $Z(M) \setminus Z(G)$ | $C \setminus Z(M)$ | $M \setminus C$ | $G \setminus M$ |
|---|---|---|---|---|
| $G \setminus M$ | 1 | 3<br>2, if $[x,y] \neq 1$<br>2, if $G \in \mathcal{A}$ | 2 | 2 |
| $M \setminus C$ | 3 | 2 | 2 | |
| $C \setminus Z(M)$ | 3 | 2 | | |
| $Z(M) \setminus Z(G)$ | 2 | | | |

(iii) By Proposition 5.8.2(i), it suffices to show that $d(x,y) \leqslant 2$ whenever $x \in C \setminus Z(G)$ and $y \in G \setminus Z(G)$ are distinct non-isolated vertices. Since $C$ is abelian, Proposition 2.1.7 yields $C_G(x) = C$. If $G/\langle x \rangle^G$ is not cyclic, then Proposition 5.2.10 shows that $G \setminus C_G(x) = G \setminus C$ is the neighbourhood of $x$ in $\Xi(G)$. In particular, if $y \in G \setminus C$, then $d(x,y) = 1$. If instead the non-isolated vertex $y$ lies in the abelian group $C$, then $k \sim y$ for some $k \in G \setminus C$. Hence $x \sim k \sim y$ and $d(x,y) = 2$.

Suppose now that $G/\langle x \rangle^G$ is cyclic. As $x$ and $y$ are non-isolated vertices, Proposition 5.3.1 implies that there exist maximal subgroups $L$ and $K$ of $G$ with $x \in L \setminus Z(L)$ and $y \in K \setminus Z(K)$. Then $x \in Z(C) \cap L$, and thus applying Corollary 2.1.8 to the pair $(C, L)$ gives $Z(L) \leqslant Z(G)$. Note also that $G = C_G(x)L$, since $C_G(x) = C$ is a normal maximal subgroup of $G$. Hence applying Proposition 2.1.4 to $x$ and $L$ yields $L \trianglelefteq G$, and it follows that $C_L(x) = C \cap L \trianglelefteq G$. We therefore see that $d(x,y) \leqslant 3$ by applying Lemma 5.4.2 to the 4-tuple $(x, L, y, K)$. In fact, this lemma shows that $d(x,y) \leqslant 2$ if $x \notin Z(K)$ and $y \notin Z(L)$. This is indeed the case, as $K \not\leqslant C = C_G(x)$ and $Z(L) \leqslant Z(G)$.

(iv) Since $Z(G) \leqslant C < M$, it follows that $Z(G) \leqslant Z(M)$. Additionally, Proposition 5.8.5(ii) shows that $M$ is non-abelian and normal in $G$, with $Z(M) < Z(C) = C$. Note that if $G$ contains an abelian maximal subgroup, then Lemma 2.1.12 implies that $Z(M) = Z(G)$, and so the first column of Table 5.8.1 can be ignored. In general, we observe from Corollary 5.2.8 that any two vertices of $\Xi(G)$ in $M \setminus Z(M) = (M \setminus C) \cup (C \setminus Z(M))$ have distance at most two. This yields the $(2,2)$, $(2,3)$ and $(3,2)$ entries of Table 5.8.1. Additionally, Proposition 5.8.2(i) implies that any two elements of $G \setminus C = (G \setminus M) \cup (M \setminus C)$

have distance at most two. Thus we obtain the $(1,3)$ and $(1,4)$ entries of the table.

Now, suppose that $Z(G) < Z(M)$, and let $z \in Z(M) \setminus Z(G)$. Since $M$ is a non-abelian, normal subgroup of $G$ and $\langle z \rangle^G \leqslant Z(M)$, Proposition 2.1.2 shows that $G/\langle z \rangle^G$ is not cyclic. As $C_G(z) = M$ by Proposition 2.1.7, Proposition 5.2.10 gives $z \sim r$ for each $r \in G \setminus M$, hence the $(1,1)$ entry of Table 5.8.1. Thus if $z' \in Z(M) \setminus Z(G)$ is not equal to $z$, then $z \sim r \sim z'$ and $d(z,z') = 2$, yielding the $(4,1)$ entry of the table. Moreover, if $m \in M \setminus C$, then $d(r,m) \leqslant 2$ by the (1,3) entry of the table, and so $d(z,m) \leqslant d(z,r) + d(r,m) \leqslant 1 + 2 = 3$. This gives the $(2,1)$ entry of the table.

It remains to determine upper bounds for $d(c,g)$, where $c \in C \setminus Z(M)$ and $g \in G \setminus M$, and for $d(c,z)$ when the element $z$ exists. As $g$ does not lie in $C$, it is a non-isolated vertex by (ii). It follows from Proposition 5.3.1 that $g \in K \setminus Z(K)$ for some (non-abelian) maximal subgroup $K$ of $G$. Additionally, since $C$ is abelian, it lies in $C_G(c)$, and the cyclic group $G/C$ normalises $C_G(c)/C$. Thus $C_G(c) \trianglelefteqslant G$. Since $M$ is also normal in $G$, it follows that $C_M(c) = C_G(c) \cap M \trianglelefteqslant G$. Therefore, applying Lemma 5.4.2 to the 4-tuple $(c, M, g, K)$ gives $d(c,g) \leqslant 3$. Moreover, since $g \notin Z(M)$, that lemma shows that if $d(c,g) = 3$, then $c \in Z(K)$, and in particular, $[c,g] = 1$. In this case, Proposition 2.1.7 shows that the non-abelian maximal subgroup $K$ of $G$ is equal to the normal subgroup $C_G(c)$, and so Lemma 2.1.12 implies that $G$ contains no abelian maximal subgroup. Thus we obtain the $(1,2)$ entry of Table 5.8.1.

Finally, since $C_G(c)$ and $M$ are proper subgroups of $G$, there exists $h \in G \setminus (M \cup C_G(c))$. The $(1,1)$ and $(1,2)$ entries of Table 5.8.1 yield $h \sim z$ and $d(c,h) \leqslant 2$. Hence $d(c,z) \leqslant d(c,h) + d(h,z) \leqslant 3$. This gives the $(3,1)$ entry of the table. We have now accounted for distances between all elements of $\Xi(G)$. In particular, we have shown that $\Xi(G)$ is connected with diameter at most 3. Furthermore, as stated above, if $G$ contains an abelian maximal subgroup, then $Z(M) \setminus Z(G) = \varnothing$, and hence $\operatorname{diam}(\Xi(G)) = 2$. □

Using the Magma code in `comp_nc_ng`, together with additional straightforward calculations, we observe that if $G$ is equal to SmallGroup$(12,4)$ or SmallGroup$(18,4)$, then $G$ satisfies the hypotheses of Lemma 5.8.6(iii), and that $\Xi(G)$ is connected only in the latter case (in both cases, $\Xi^+(G)$ is connected with diameter 2). If instead $G$ is equal to SmallGroup$(40,12)$, SmallGroup$(60,7)$ or SmallGroup$(100,3)$, then $G$ satisfies the hypotheses of Lemma 5.8.6(iv), and $\Xi(G)$ has diameter 2, 3 or 2, respec-

tively. Note that the first of these three groups has an abelian maximal subgroup, while the third does not.

The following result is a more detailed version of Lemma 5.7.15, with a weaker hypothesis (cf. Proposition 5.8.5(ii)).

**Lemma 5.8.7.** *Let $G$ and $C$ be as in Assumption 5.8.1. Suppose also that $G$ is finitely generated, $G/C$ is cyclic, and $C$ is non-abelian. Then the following statements hold.*

(i) *$\Xi(G)$ is not connected if and only if $C$ is maximal in $G$ and $K \cap C = Z(C)$ for every maximal subgroup $K$ of $G$ distinct from $C$. In this case, $\Xi(G)$ has exactly two connected components, each of diameter 2, and one component consists of the elements of $C \setminus Z(C)$. In particular, if $G$ is finite, then $\Xi(G)$ is not connected if and only if $G$ satisfies Assumption 5.7.3.*

(ii) *Suppose that $C$ is not maximal in $G$, and let $M$ be a maximal subgroup of $G$ containing $C$. Then Table 5.8.2 lists upper bounds for distances between vertices of $\Xi(G)$, depending on the subsets of $G \setminus Z(G)$ that contain them. In particular, $\operatorname{diam}(\Xi(G)) \leqslant 4$, and $\operatorname{diam}(\Xi(G)) \leqslant 3$ if $G$ is finite or if $Z(M) = Z(G)$.*

(iii) *Suppose that $C$ is maximal in $G$, and that $\Xi(G)$ is connected. Then $G$ contains no abelian maximal subgroup. Additionally, Table 5.8.3 lists upper bounds for distances between vertices of $\Xi(G)$, depending on the subsets of $G \setminus Z(G)$ that contain them. In particular, $\operatorname{diam}(\Xi(G)) \leqslant 4$, and $\operatorname{diam}(\Xi(G)) \leqslant 3$ if $G$ is finite.*

*Proof.* We first present several simple arguments that apply in each case. Proposition 5.8.2(i) shows that any two elements of $G \setminus C$ are joined in $\Xi(G)$ by a path of length at most two. We therefore obtain the $(1,4)$, $(1,5)$ and $(2,4)$ entries of Table 5.8.2, and the $(1,3)$ entry of Table 5.8.3. It also follows from Corollary 5.2.8 that any two elements of $C \setminus Z(C)$ are joined by a path of length at most two. This gives the $(3,3)$ entry of Table 5.8.2 and the $(2,2)$ entry of Table 5.8.3.

Next, Proposition 5.8.5(ii) implies that $Z(G) < Z(C)$. Let $z \in Z(C) \setminus Z(G)$. Since $C$ is non-abelian and normal in $G$ and $\langle z \rangle^G \leqslant Z(C)$, we deduce from Proposition 2.1.2 that $G/\langle z \rangle^G$ is not cyclic.

We split the remainder of the proof into two cases, depending on whether or not $C$ is maximal in $G$.

Table 5.8.2: Upper bounds for distances between vertices $x \in A$ and $y \in B$ of $\Xi(G)$, where $A$ and $B$ are specified subsets of $G \setminus Z(G)$, and $C$ and $M$ are as in Lemma 5.8.7(ii). Additionally, $\mathcal{A}$ denotes the family of groups that contain an abelian maximal subgroup, and $\mathcal{M}$ denotes the family of groups for which any two distinct maximal subgroups intersect in the Frattini subgroup.

| $A$ \ $B$ | $Z(M) \setminus Z(G)$ | $Z(C) \setminus Z(M)$ | $C \setminus Z(C)$ | $M \setminus C$ | $G \setminus M$ |
|---|---|---|---|---|---|
| $G \setminus M$ | 1 | 3<br>2, if $G \in \mathcal{A}$ | 3 | 2 | 2 |
| $M \setminus C$ | 3 | 2 | 2 | 2 | |
| $C \setminus Z(C)$ | 4<br>3, if $\lvert G\rvert < \infty$<br>3, if $G \notin \mathcal{M}$ | 2 | 2 | | |
| $Z(C) \setminus Z(M)$ | 2 | 2 | | | |
| $Z(M) \setminus Z(G)$ | 2 | | | | |

Table 5.8.3: Upper bounds for distances between vertices $x \in A$ and $y \in B$ of $\Xi(G)$, where $A$ and $B$ are specified subsets of $G \setminus Z(G)$, and $C$ is as in Lemma 5.8.7(iii). Additionally, $\mathcal{M}$ denotes the family of groups for which any two distinct maximal subgroups intersect in the Frattini subgroup.

| $A$ \ $B$ | $Z(C) \setminus Z(G)$ | $C \setminus Z(C)$ | $G \setminus C$ |
|---|---|---|---|
| $G \setminus C$ | 1 | 4<br>3, if $\lvert G/Z(C)\rvert < \infty$<br>3, if $G \in \mathcal{M}$ | 2 |
| $C \setminus Z(C)$ | 4<br>3, if $\lvert G\rvert < \infty$<br>3, if $G \notin \mathcal{M}$ | 2 | |
| $Z(C) \setminus Z(G)$ | 2 | | |

**Case (a)**: $C$ is maximal in $G$. Here, Proposition 5.8.5(iii) shows that $G$ has no abelian maximal subgroup. In addition, $C = C_G(z)$ by Proposition 2.1.7. Since $G/\langle z\rangle^G$ is not cyclic, it follows from Proposition 5.2.10 that $z \sim k$ for all $k \in G \setminus C$. Thus we obtain the $(1,1)$ entry of Table 5.8.3. If $z'$ is another element of $Z(C) \setminus Z(G)$, then $z \sim k \sim z'$, yielding the $(3,1)$ entry of Table 5.8.3. Furthermore, since $Z(G) < Z(C)$, Lemma 5.7.15 shows that if $G$ is finite, then $\Xi(G)$ is not connected if and only $G$ satisfies Assumption 5.7.3, and in general, $\Xi(G)$ is not connected if and only if $K \cap C = Z(C)$ for every maximal subgroup $K \neq C$ of $G$.

Suppose first that $\Xi(G)$ is connected, and let $x \in C \setminus Z(C)$ and $y \in G \setminus C$.

Then Lemma 5.7.7 shows that $d(x,z) \leqslant 4$, and that if $d(x,z) = 4$, then $|G| = \infty$ and $K \cap C = \Phi(G)$ for each maximal subgroup $K$ of $G$ distinct from $C$. It follows from Lemma 5.7.1 that if $d(x,z) = 4$, then any two distinct maximal subgroups of $G$ intersect in $\Phi(G)$, and we obtain the $(2,1)$ entry of Table 5.8.3. Additionally, Lemma 5.7.12 shows that $d(x,y) \leqslant 4$, and that if $d(x,y) = 4$, then $|G/Z(C)| = \infty$ and $G$ contains maximal subgroups $K$ and $L \neq C$ such that $K \cap C = Z(C) \neq L \cap C$. This yields the $(1,2)$ entry of Table 5.8.3. We have therefore proved (iii).

Next, suppose that $\Xi(G)$ is not connected. We have shown that if $g, h \in G \setminus Z(G)$ satisfy $g, h \in C \setminus Z(C)$ or $g, h \in (G \setminus C) \cup (Z(C) \setminus Z(G))$, then $d(g,h) \leqslant 2$. Hence the connected components of $\Xi(G)$ and their diameters are as specified in (i). To complete the proof of (i), it remains to show that if $C$ is not maximal in $G$, then $\Xi(G)$ is connected, and if $G$ is also finite, then it does not satisfy Assumption 5.7.3.

**Case (b)**: $C$ is not maximal in $G$. Let $M$ be a maximal subgroup of $G$ containing $C$. Then $M$ is non-abelian, and Proposition 5.8.5(ii) implies that $M$ is normal in $G$, with $Z(M) < Z(C)$. Additionally, as $Z(G) < C$, it follows that $Z(G) \leqslant Z(M)$. Corollary 5.2.8 shows that there is a path of length at most two in $\Xi(G)$ between any two elements of $M \setminus Z(M)$, hence the $(2,2)$, $(2,3)$, $(3,2)$ and $(4,2)$ entries of Table 5.8.2. Let $z'$ be an element of $Z(C) \setminus Z(G)$ distinct from $z$. Since $[z,z'] = 1$, and since $G/\langle z \rangle^G$ and $G/\langle z' \rangle^G$ are not cyclic, Proposition 5.8.2(ii) implies that $d(z,z') = 2$. This gives the $(4,1)$ and $(5,1)$ entries of Table 5.8.2. Note also that as $z \in Z(C) \setminus Z(G)$, there exists $h \in G \setminus C$ with $[z,h] \neq 1$. As $G/\langle z \rangle^G$ is not cyclic, it follows from Proposition 5.2.10 that $z \sim h$. Letting $g \in G \setminus C$, the known entries of Table 5.8.2 show that $d(h,g) \leqslant 2$, and so $d(z,g) \leqslant d(z,h) + d(h,g) \leqslant 3$. This gives the $(2,1)$ entry of Table 5.8.2, as well as the general upper bound of 3 in the $(1,2)$ entry.

Now, let $x \in C \setminus Z(C)$. Then $x \notin Z(M)$, and so $C_M(x) < M$. Thus there exists $k \in M \setminus (C \cup C_M(x))$, and we observe that $x \sim k$. The $(1,4)$ entry of Table 5.8.2 gives $d(k,g) \leqslant 2$ for each $g \in G \setminus M$, and hence $d(x,g) \leqslant d(x,k) + d(k,g) \leqslant 3$, yielding the $(1,3)$ entry of the table.

Next, we will consider the remaining entries in the first column of Table 5.8.2, which apply only when $Z(G) < Z(M)$. Let $r \in Z(M) \setminus Z(G)$. Then the $(2,1)$ entry of Table 5.8.2 shows that $d(r,m) < \infty$ for each $m \in M \setminus C$. The $(3,1)$ entry of Table 5.8.2 therefore follows from Lemmas 5.7.7 and 5.7.1. In addition, $M = C_G(r)$ by Proposition 2.1.7, and so Proposition 5.2.10 gives the $(1,1)$ entry of the table.

We have now justified the general upper bound given in each entry of Table 5.8.2. In particular, $\Xi(G)$ is connected, which partially proves (i). To complete the proof of (i), suppose for a contradiction that $G$ is finite and satisfies Assumption 5.7.3. Then

the unique non-cyclic Sylow subgroup $G$ of $P$ satisfies $Z(P) \not\leqslant Z(G)$; the unique maximal subgroup of each nontrivial cyclic Sylow subgroup of $G$ is normal in $G$; and $M$ is precisely the maximal subgroup $M$ specified in Theorem 5.7.2(ii) (by part (a) of that theorem). Part (c) of that theorem therefore implies that $Z(M)$ contains $Z(P) \not\leqslant Z(G)$, and so $Z(G) < Z(M)$ by Proposition 2.1.7. Hence Lemma 5.7.15 applies, and shows that $G$ does not in fact satisfy Assumption 5.7.3. Thus (i) holds.

To prove (ii), it remains to assume that $G$ has an abelian maximal subgroup, and to deduce the $(1,2)$ entry of Table 5.8.2, i.e., to show that $d(y,z) \leqslant 2$ when $y \in G \setminus M$ and $z \in Z(C) \setminus Z(M)$. Let $K$ be a maximal subgroup of $G$ containing $C_G(z)$, so that $C < K$. Then $K$ is non-abelian, and $K \trianglelefteq G$ by Proposition 5.8.5(ii). Thus Lemma 2.1.12 yields $Z(K) \leqslant Z(G)$ (in fact, it is easy to see that $Z(K) = Z(G)$). Hence if $y \in K$, then $d(y,z) \leqslant 2$ by Corollary 5.2.8. If instead $y \notin K$, then $[y,z] \neq 1$. As $G/\langle z \rangle^G$ is not cyclic (by the start of the proof), Proposition 5.2.10 gives $y \sim z$, and we obtain (ii). □

Notice from Lemmas 5.7.7 and 5.7.12 that the conditions $G \notin \mathcal{M}$ and $G \in \mathcal{M}$ in the $(2,1)$ and $(1,2)$ entries of Table 5.8.3, respectively, are stronger than those necessary to ensure that the specified distances cannot be equal to 4 (and similarly for the $(3,1)$ entry of Table 5.8.2). However, the chosen conditions highlight the fact that there is no group for which these two entries of Table 5.8.3 are simultaneously equal to 4, as discussed in Remark 5.7.14.

The Magma code in `comp_nc_ng` (together with additional basic calculations) shows that SmallGroup$(120,36)$ and SmallGroup$(192,30)$ satisfy the hypotheses of Lemma 5.8.7(ii), and have non-commuting, non-generating graphs of diameter 2 and 3, respectively. Additionally, SmallGroup$(36,10)$ and SmallGroup$(48,15)$ satisfy the hypotheses of Lemma 5.8.7(iii), and the associated graphs have diameter 2 and 3, respectively. As we mentioned earlier in this section, SmallGroup$(36,10)$ also satisfies the hypotheses of Lemma 5.8.3.

Before presenting examples of groups that satisfy Lemma 5.8.7(i), we further clarify how Assumption 5.7.3 relates to this lemma (and to Assumption 5.8.1).

**Proposition 5.8.8.** *Suppose that $G$ satisfies Assumption 5.7.3. Then $G$ contains a normal subgroup $N$, such that $G/N$ is not cyclic, $G/C_G(N)$ is cyclic, and $C_G(N)$ is non-abelian. Thus $G$ satisfies the hypotheses of Lemma 5.8.7, and so $\Xi(G)$ has exactly two connected components, each of diameter 2.*

*Proof.* Let $P$ and $Q$ be as in Assumption 5.7.3, and let $R$ be the unique maximal subgroup of $Q$. Theorem 5.7.2 shows that $G$ contains a normal maximal subgroup $M = P \times R$. Additionally, $N := Z(M)$ is equal to $Z(P) \times R$, which is not a subgroup

of $Z(G)$ by assumption. Since $Z(P) = \Phi(P) < P$, we deduce that $P$ is non-abelian, and hence so is $M$. Thus Proposition 2.1.2 shows that $G/N = G/Z(M)$ is not cyclic, and so $G$ and $N$ are as in Assumption 5.8.1. Moreover, Proposition 2.1.7 shows that $C := C_G(N)$ is the non-abelian maximal subgroup $M$ of $G$, and hence $G/C$ is cyclic. Therefore, $G$ satisfies the hypotheses of Lemma 5.8.7, and the final part of the result follows from Lemma 5.8.7(i). □

We will now discuss, with several examples, finite groups $G$ such that $\Xi(G)$ has two connected components, each of diameter 2. For brevity, we will call such a group a $[2, 2]$-group.

**Example 5.8.9.** Except where stated otherwise, all information in this example can be verified using the Magma code in `nc_ng_22_groups`. First, the unique smallest finite $[2, 2]$-group is the group $G$ numbered $(96, 3)$ in the Small Groups Library. Interestingly, the derived subgroup $G'$ contains elements that are not commutators of elements of $G$, and as observed in [18, Example 2.3-7], no smaller finite group satisfies this property. However, there is no correlation between these two properties in general. For example, $H :=$ SmallGroup$(96, 203)$ contains elements that lie in $H'$ and are not commutators. On the other hand, $\Xi(H)$ is connected with diameter 2. Conversely, SmallGroup$(448, 179)$ is a $[2, 2]$-group, and every element in its derived subgroup is a commutator.

The Magma code in `nc_ng_22_groups` also shows that the final group discussed in the previous example is (isomorphic to) the normaliser in the simple group Sz(8) of one of its Sylow 2-subgroups. We now generalise this observation with an infinite family of $[2, 2]$-groups.

**Example 5.8.10.** Let $i$ be an odd integer at least 3, $q := 2^i$, and $G := \mathrm{Sz}(q)$. Additionally, let $S$ be a Sylow 2-subgroup of $G$, and let $N := N_G(S)$. Then $|S| = q^2$, and $N$ is a maximal subgroup of $G$ isomorphic to the Frobenius group $S{:}C_{q-1}$ [136, §4, p. 133, Theorem 9].

By Zsigmondy's Theorem, there exists an odd primitive prime divisor $r$ of $q-1$, i.e., a prime divisor that does not divide $2^j - 1$ for any positive integer $j < i$. For any such $r$, let $N_r$ be the subgroup of $N$ isomorphic to $S{:}C_r$. It follows from Theorem 2.1.19 that $N_r$ is also a Frobenius group, and that $Z(N_r) = 1$. Moreover, each cyclic subgroup of $N_r$ of order $r$ acts irreducibly on the vector space $S/\Phi(S)$ [75, Theorem 3.5]. Hence $N_r$ satisfies all conditions of Theorem 5.7.2(i).

We claim that $N_r$ is a $[2, 2]$-group. By Proposition 5.8.8, it suffices to show that $G$ satisfies Assumption 5.7.3. As the unique maximal subgroup of $C_r$ is the

trivial group, which is of course normal in $N_r$, it remains only to prove that $\Phi(S) = Z(S) \not\leqslant Z(N_r) = 1$. Let $\theta$ be the automorphism $\alpha \mapsto \alpha^{\sqrt{2q}}$ of $\mathbb{F}_q$. Then [136, pp. 111-112, Theorem 7] shows that (up to isomorphism) $S$ can be considered as the set $\{(\alpha, \beta) \mid \alpha, \beta \in \mathbb{F}_q\}$, equipped with the multiplication defined by $(\alpha, \beta)(\gamma, \delta) := (\alpha + \gamma, \alpha\gamma^\theta + \beta + \delta)$ for all $(\alpha, \beta), (\gamma, \delta) \in S$.

Now, $Z(S) = \{(0, \beta) \mid \beta \in \mathbb{F}_q\}$ [136, Lemma 1], which is clearly not a subgroup of $Z(N_r) = 1$. For $(\alpha, \beta), (\gamma, \delta) \in S$, we calculate that $(\alpha, \beta)^2 = (0, \alpha\alpha^\theta)$, and that the first coordinate of $[(\alpha, \beta), (\gamma, \delta)]$ is equal to 0. Thus the subgroup $K$ of $S$ generated by all squares in $S$ lies in $Z(S)$, as does $S'$. In fact, the endomorphism $\alpha \mapsto \alpha\alpha^\theta$ of the set $\mathbb{F}_q^\times$ is a monomorphism [136, p. 111], and is therefore an automorphism. This implies that $K = Z(S)$. Since $\Phi(S) = KS'$ (see, e.g., [88, p. 60]), it follows that $\Phi(S) = Z(S)$. Hence $N_r$ is a $[2, 2]$-group.

**Example 5.8.11.** Observe that each $[2, 2]$-group from Examples 5.8.9 and 5.8.10 has even order and contains a Sylow subgroup of prime order. However, these are not necessary conditions for a group to be a $[2, 2]$-group. For example, the Magma code in `nc_ng_22_groups` shows that SmallGroup$(9477, 4035)$ and SmallGroup$(288, 3)$ are $[2, 2]$-groups (note that $288 = 2^5 \cdot 3^2$).

We now state this section's main theorem.

**Theorem 5.8.12.** *Suppose that $G$ contains a normal subgroup $N$, such that $G/N$ is not cyclic and $N \not\leqslant Z(G)$, and let $C := C_G(N)$. Then one of the following holds.*

(i) *$\Xi(G)$ has an isolated vertex, and $\Xi^+(G)$ is connected with diameter 2. Additionally, each isolated vertex of $\Xi(G)$ lies in $C \setminus N$. In this case, $C$ is abelian and maximal in $G$, and $G$ is soluble.*

(ii) *$\Xi(G)$ is connected with diameter 2 or 3. In this case, if $G/C$ is cyclic and $C$ is abelian, and if $G$ contains an abelian maximal subgroup, then* $\operatorname{diam}(\Xi(G)) = 2$.

(iii) *$\Xi(G)$ is connected with diameter 4. In this case, $G$ is infinite, $G/C$ is cyclic, and $C$ is non-abelian.*

(iv) *$\Xi(G)$ has exactly two connected components, each of diameter 2, with one component consisting of the elements of $C \setminus Z(C)$. In this case, $C$ is non-abelian and maximal in $G$.*

*Moreover, if $G$ is finite, then (iv) holds if and only if $G$ satisfies Assumption 5.7.3.*

*Proof.* We may assume that $G$ is finitely generated, as otherwise $\operatorname{diam}(\Xi(G)) = 2$ by Corollary 5.2.7. If $G/C$ is not cyclic, then Lemma 5.8.3 applies, and (ii) holds.

Otherwise, either Lemma 5.8.6 or Lemma 5.8.7 applies, depending on whether or not $C$ is abelian. Specifically, if $C$ is abelian, then (i) or (ii) holds, and otherwise, (ii), (iii) or (iv) holds. We therefore observe from Lemma 5.8.7 and Proposition 5.8.8 that if $G$ is finite, then (iv) holds if and only if $G$ satisfies Assumption 5.7.3. □

Note that if $\Xi(G)$ has two nontrivial components, then Lemma 5.8.7(i) applies, and states that $K \cap C = Z(C)$ for each maximal subgroup $K$ of $G$ distinct from the normal, non-abelian maximal subgroup $C$. As $Z(G) < Z(C)$ by Proposition 5.8.5(ii), we can use Lemma 5.7.15 and Proposition 5.7.9 to deduce additional information about the structures of infinite groups in this case.

There are extra restrictions on the above conclusions if $G$ contains two distinct subgroups satisfying the properties of $C$.

**Corollary 5.8.13.** *For each $i \in \{1, 2\}$, suppose that $G$ contains a normal subgroup $N_i$ such that $G/N_i$ is not cyclic and $N_i \not\leqslant Z(G)$. Additionally, let $C_i := C_G(N_i)$, and suppose that $C_1 \neq C_2$. Then $\Xi(G)$ is connected.*

*Proof.* Suppose for a contradiction that $\Xi(G)$ is not connected. If $\Xi(G)$ has two nontrivial connected components, then it follows from Theorem 5.8.12 that $C_1$ and $C_2$ are both non-abelian and maximal in $G$. Moreover, one of the components of $\Xi(G)$ consists of the elements of $C_1 \setminus Z(C_1)$, and either the second component consists of the elements of $C_2 \setminus Z(C_2)$, or $C_1 \setminus Z(C_1) = C_2 \setminus Z(C_2)$. Observe that there exists an element $x \in C_1 \setminus (Z(C_1) \cup C_2)$, and so $C_1 \setminus Z(C_1) \neq C_2 \setminus Z(C_2)$. Thus these subsets are the two connected components of $G \setminus Z(G)$, and hence $G \setminus Z(G)$ is their union. However, there exists an element $y \in G \setminus (C_1 \cup C_2)$, and since $Z(G) \leqslant C_1$, we see that $y \notin Z(G)$. Thus $G \setminus Z(G)$ is not in fact a union of the connected components, a contradiction.

Theorem 5.8.12 now implies that $\Xi(G)$ has exactly one nontrivial connected component, that $C_1$ and $C_2$ are abelian and maximal in $G$, and that each isolated vertex of $\Xi(G)$ lies in $C_1 \cap C_2$. However, Corollary 2.1.8, applied to the pair $(C_1, C_2)$ of abelian maximal subgroups, implies that $C_1 \cap C_2 = Z(G)$. Hence $\Xi(G)$ has no isolated vertices and is in fact connected, another contradiction. □

To conclude this section, we will show that the structure of $\Xi(G)$ is also restricted if $G$ contains an abelian maximal subgroup, and if certain finiteness conditions hold.

**Proposition 5.8.14.** *Suppose that $G$ contains a normal subgroup $N$, such that $G/N$ is not cyclic and $N \not\leqslant Z(G)$, and let $C := C_G(N)$. In addition, suppose that $G$ contains an abelian maximal subgroup, and that $G/C$ is finite. If $N$ is non-abelian*

*and $G/C$ is not cyclic, then assume also that $G/C_G(C)$ is finite. Then $\Xi^+(G)$ is connected with diameter 2.*

*Proof.* By Corollary 5.2.7, we may suppose that $G$ is finitely generated, as otherwise $\operatorname{diam}(\Xi(G)) = 2$. Assume first that $G/C$ is cyclic. Since this quotient is also finite, Proposition 5.8.5(iii) shows that $C$ is abelian, and Lemma 5.8.6 yields the result. If instead $G/C$ is not cyclic and $N$ is non-abelian, then Proposition 2.1.13 gives $C = Z(G)$, and the result follows from Lemma 5.8.3.

Suppose finally that $G/C$ is not cyclic and $N$ is abelian. Then $C$ is not maximal in $G$, and is abelian by Proposition 2.1.13. Let $L$ be an abelian maximal subgroup of $G$. Observe that $N \leqslant C$, and so $C_G(C) \leqslant C_G(N) = C$ (in fact, $C_G(C) = C$). Hence $C \not\leqslant L$, and $LC = G$. Thus $G/C$ is isomorphic to the abelian group $L/(L \cap C)$.

By Lemma 5.8.3, $\Xi(G)$ is connected, and it suffices to show that $d(x, y) \leqslant 2$ for each $x \in C \setminus Z(G)$ and $y \in G \setminus (N \cup C)$. Let $M$ be a maximal subgroup of $G$ containing $C$. Then $M$ is non-abelian, as $C_G(C) = C < M$. Moreover, as $G/C$ is abelian, we observe from the Correspondence Theorem that $M \trianglelefteqslant G$. Hence Lemma 2.1.12 yields $Z(M) = Z(G)$. Thus if $y \in M$, then Corollary 5.2.8 yields $d(x, y) \leqslant 2$.

We may therefore assume that $y$ lies in no maximal subgroup of $G$ containing $C$. Since $\Xi(G)$ is connected, Proposition 5.3.1 shows that $y$ is a non-central element of a maximal subgroup $R$ of $G$. As the abelian group $C$ does not lie in $R$, it follows that $C_G(x) \not\leqslant R$, and so $x \notin Z(R)$ by Proposition 2.1.7. In addition, since $G/C$ is abelian and $C \leqslant C_M(x)$, we see that $C_M(x) \trianglelefteqslant G$. As $y \notin Z(M) = Z(G)$, applying Lemma 5.4.2 to the 4-tuple $(x, M, y, R)$ gives $d(x, y) \leqslant 2$. □

## 5.9 Groups with non-simple central quotients

In this section, we complete the proof of Theorem 5.1.5, which describes $\Xi(G)$ when the quotient of the group $G$ by its centre is not simple. Observe that Theorem 5.8.12 accounts for all such groups where $G/Z(G)$ has a proper non-cyclic quotient. It therefore remains to consider the case where every proper quotient of $G/Z(G)$ is cyclic. As above, we will implicitly use Proposition 5.2.5, which states that any nontrivial connected component of $\Xi(G)$ has diameter at least 2.

Recall Definition 2.1.22, of an abstract primitive group. A classification of finite groups where every proper quotient is cyclic is given in [103, §3]. In the following lemma, we present a similar classification that does not assume finiteness.

**Lemma 5.9.1.** *Suppose that every proper quotient of $G$ is cyclic. Then one of the following occurs:*

(i) *for each central extension $H$ of $G$ (including $G$ itself), every maximal subgroup of $H$ is normal in $H$, and hence $G$ is not primitive;*

(ii) *$G$ is a soluble primitive group with a (unique) minimal normal subgroup and a cyclic point stabiliser; or*

(iii) *$G$ is an insoluble primitive group, and $C_G(N) = 1$ for each nontrivial normal subgroup $N$ of $G$.*

*Proof.* We split the proof into three cases, which together account for all possibilities.

**Case (a)**: $G$ is not primitive. Suppose that $G$ contains a maximal subgroup $M$, and let $J := \mathrm{Core}_G(M)$. By Definition 2.1.22, $J \neq 1$, and hence $G/J$ is cyclic. Thus $M/J \trianglelefteqslant G/J$, and so $M \trianglelefteqslant G$. Thus each maximal subgroup of $G$ is normal, and it follows from Proposition 2.1.6 that the same is true for each maximal subgroup of each central extension of $G$. Hence (i) holds.

**Case (b)**: $G$ is primitive, and $C_G(J) \neq 1$ for some nontrivial normal subgroup $J$ of $G$. By [5, Lemma 2.2], $N := C_G(J)$ is a minimal normal subgroup of $G$. If $G$ contains a distinct minimal normal subgroup $K$, then it follows from Theorem 2.1.24 that $K$ is non-abelian and equal to $K/(K \cap N) \cong NK/N$. In particular, $NK/N$ is not cyclic, and so neither is $G/N$, a contradiction.

Hence $N$ is the unique minimal normal subgroup of $G$. Moreover, since $C_G(N)$ contains the nontrivial subgroup $J$ (which is now clearly equal to $N$), Theorem 2.1.24 implies that $N$ is abelian, and that each point stabiliser of $G$ is isomorphic to the cyclic group $G/N$. In particular, $G$ is a cyclic extension of an abelian group, and is therefore soluble. Consequently, (ii) holds.

**Case (c)**: $G$ is primitive, and $C_G(N) = 1$ for each nontrivial normal subgroup $N$ of $G$. If $G$ is soluble, then the penultimate subgroup $R$ in the derived series of $G$ is nontrivial and abelian, and hence $C_G(R) \neq 1$. However, $R \trianglelefteqslant G$, a contradiction. Thus $G$ is insoluble, and (iii) holds. □

Observe that if case (i) of the previous lemma holds, then Theorem 5.4.3 applies. Hence it remains to consider cases (ii) and (iii). In what follows, for a subgroup $H$ of $G$ that contains $Z(G)$, we write $\overline{H} := H/Z(G)$.

**Proposition 5.9.2.** *Suppose that $\overline{G}$ is a soluble primitive group with every proper quotient cyclic, and let $L$ be a non-abelian maximal subgroup of $G$. Then $L \trianglelefteqslant G$ and $Z(L) \leqslant Z(G)$.*

*Proof.* We observe from Lemma 5.9.1 and Theorem 2.1.24 that $\overline{G}$ contains a unique minimal normal subgroup $\overline{N}$, and a cyclic point stabiliser $\overline{M}$ such that $\overline{G} = \overline{N}{:}\overline{M}$.

Suppose first that $Z(G) \not\leqslant L$. Then $L \trianglelefteqslant G$ by Proposition 2.1.6. Additionally, there is no $x \in G$ satisfying $L = C_G(x)$, and thus Proposition 2.1.7 gives $Z(L) < Z(G)$.

Assume from now on that $Z(G) \leqslant L$, and note that $\overline{L}$ is a maximal subgroup of $\overline{G}$. Since $L$ is non-abelian, Proposition 2.1.2 (with $L$ in place of $G$ and $Z(G)$ in place of $N$ and $K$) shows that $\overline{L}$ is not cyclic. Therefore, $\overline{L}$ is not a complement of $\overline{N}$ in $\overline{G}$, and so Theorem 2.1.24 implies that $\overline{L}$ is not core-free in $\overline{G}$. Hence $\overline{N} \leqslant \overline{L}$. Moreover, as $\overline{G}/\overline{N}$ is cyclic, we see that $\overline{L}/\overline{N} \trianglelefteqslant \overline{G}/\overline{N}$, and it follows that $L \trianglelefteqslant G$.

It remains to show that $Z(L) = Z(G)$. Observe that $\overline{Z(L)} \trianglelefteqslant \overline{G}$, and that $\overline{G}/\overline{Z(L)}$ is isomorphic to $G/Z(L)$, which is non-cyclic by Proposition 2.1.2. Since $\overline{G}/\overline{N}$ is cyclic, it follows that $\overline{N} \not\leqslant \overline{Z(L)}$. As $\overline{N}$ lies in each nontrivial normal subgroup of $\overline{G}$, we conclude that $\overline{Z(L)} = 1$, and so $Z(L) = Z(G)$. □

We can now prove the following. Recall that $\Xi^+(G)$ is the subgraph of $\Xi(G)$ induced by its non-isolated vertices.

**Lemma 5.9.3.** *Suppose that $\overline{G}$ is a soluble primitive group with every proper quotient cyclic, and that $\Xi(G)$ has an edge. Then $\Xi(\overline{G})$ has isolated vertices, and $\Xi^+(G)$ is connected with diameter 2.*

*Proof.* Since $\overline{G}$ has a minimal normal subgroup by Lemma 5.9.1, we observe from Theorem 2.1.24 that each point stabiliser $\overline{K}$ of $\overline{G}$ is cyclic. As $Z(\overline{G}) = 1$ by Proposition 2.1.23, and since $\overline{G} = \langle k, g \rangle$ whenever $k$ is a generator for $\overline{K}$ and $g \in \overline{G} \setminus \overline{K}$, it is clear that any such $k$ is an isolated vertex of $\Xi(\overline{G})$.

Now, we may assume that $G$ is 2-generated, as otherwise $\Xi(G)$ is connected with diameter 2 by Corollary 5.2.7. Let $x$ and $y$ be non-isolated vertices of $\Xi(G)$. Proposition 5.3.1 implies that there exist maximal subgroups $L$ and $M$ of $G$ with $x \in L \setminus Z(L)$ and $y \in M \setminus Z(M)$. Moreover, Proposition 5.9.2 shows that $L$ and $M$ are normal subgroups of $G$ whose centres lie in $Z(G)$. Thus $x \notin Z(M)$ and $y \notin Z(L)$, and so applying Lemma 5.4.2 to the 4-tuple $(x, L, y, M)$ yields $d(x, y) \leqslant 2$. □

We can show, using the Magma code in `comp_nc_ng` together with some additional basic calculations, that the affine general linear group $G := \mathrm{AGL}(1,5) = \mathbb{F}_5{:}\mathrm{GL}(1,5) = \overline{G}$ satisfies the hypotheses of Lemma 5.9.3, and $\Xi(G)$ contains an edge (and hence $\Xi(G)$ consists of a connected component of diameter 2 and isolated vertices). On the other hand, the group $H$ numbered $(80, 28)$ in the Small Groups Library [11] is a non-split extension of $Z(H)$ by $G$, and $\Xi(H)$ is connected with diameter 2.

The example above shows that there exists a finite group $G$ with every proper quotient cyclic, such that $\Xi(G)$ is not connected. On the other hand, the finite groups

with every proper quotient cyclic are precisely the finite groups with connected generating graphs [22, Theorem 1, Corollary 2].

In the following theorem, we assume that $G$ itself is primitive, so that $Z(G) = 1$ (as shown by Proposition 2.1.23).

**Lemma 5.9.4.** *Suppose that $G$ is an insoluble, non-simple primitive group with every proper quotient cyclic. Then $\Xi^+(G)$ is connected with diameter 2 or 3. Moreover, if $r$ is an isolated vertex of $\Xi(G)$, then $|r| > 2$, and each proper subgroup of $G$ containing $r$ is core-free. Finally, if $G$ is 2-generated, then it contains a normal maximal subgroup with trivial centre.*

*Proof.* We may assume that $G$ is 2-generated, as otherwise $\Xi(G)$ is connected with diameter 2 by Corollary 5.2.7. Let $N$ be a nontrivial proper normal subgroup of $G$. Then for each overgroup $H$ of $N$ in $G$, the quotient $H/N$ is a normal subgroup of the cyclic group $G/N$, and hence $H \trianglelefteqslant G$. Thus each subgroup of $G$ is either normal or core-free. Furthermore, Proposition 2.1.5 shows that $N$ lies in a maximal subgroup $M$ of $G$, which must be normal, and the characteristic subgroup $Z(M)$ of $M$ is trivial by Lemma 5.9.1. Proposition 5.3.1 therefore implies that no vertex of $\Xi(G)$ that lies in $M$ is isolated. Hence each proper subgroup of $G$ containing an isolated vertex is core-free. Moreover, as $G$ is not a dihedral group, Lemma 5.3.7 shows that no involution of $G$ is isolated.

Now, let $x$ and $y$ be non-isolated vertices of $\Xi(G)$. Then Proposition 5.3.1 shows that $x \in K \setminus Z(K)$ and $y \in L \setminus Z(L)$ for some maximal subgroups $K$ and $L$ of $G$. We may assume that $K \neq L$, as otherwise $d(x, y) \leqslant 2$ by Corollary 5.2.8. Observe from Proposition 2.1.9 that $K \cap M$ and $L \cap M$ are maximal subgroups of $K$ and $L$, respectively. Furthermore, $K$ and $L$ are non-abelian, and therefore non-cyclic, and so $K \cap M$ and $L \cap M$ are nontrivial.

Suppose first that $K$ is normal in $G$, so that $Z(K) = 1$ by the first paragraph of this proof. We may assume that $y \notin K$, as otherwise we could set $L = K$. Then applying Proposition 5.4.1(i) to the triple $(y, L, K)$ shows that $y \sim h$ for some $h \in K \cap L \setminus C_{K\cap L}(y)$. As $d(x, h) \leqslant 2$ by Corollary 5.2.8, we deduce that $d(x, y) \leqslant 3$. Note that if $L$ is also normal in $G$, then we may similarly assume that $x \notin L$, and applying Proposition 5.4.1(ii) to the triple $(x, K, L)$ and the element $y$ yields $d(x, y) \leqslant 2$.

We may assume from now on that neither $K$ nor $L$ is normal in $G$, i.e., that both are core-free in $G$, and that $x, y \notin M$. Then the nontrivial subgroups $K \cap M$ and $L \cap M$ are not normal in $G$. Since $K \cap M \trianglelefteqslant K$ and $\langle K, L\rangle = G$, it follows that $L$ does not centralise $K \cap M$. Additionally, applying Proposition 5.4.1(i) to the triple $(x, K, M)$ gives $C_{K\cap M}(x) < K \cap M$. Thus if $K \cap M \leqslant L$, then there

exists an element $a \in K \cap M$ that centralises neither $x$ nor $L$. Hence $x \sim a$, and Corollary 5.2.8 yields $d(a, y) \leqslant 2$. Therefore, $d(x, y) \leqslant 3$.

If instead $K \cap M \not\leqslant L$, then $\langle K \cap M, L \rangle = G$. As $L \cap M$ is normalised by $L$ but not $G$, we deduce that $K \cap M$ does not centralise $L \cap M$. Since $C_{K\cap M}(x) < K \cap M$, and similarly $C_{L\cap M}(y) < L \cap M$, it follows that there exists an element $b \in K \cap M$ that centralises neither $L \cap M$ nor $x$, and an element $c \in L \cap M$ that centralises neither $b$ nor $y$. Thus $x \sim b \sim c \sim y$ and $d(x, y) \leqslant 3$. □

The Magma code in `diam_nc_ng` (not to be confused with the aforementioned file `comp_nc_ng`), with the aid of some auxiliary calculations, shows that the groups numbered $(25, 23)$ and $(25, 25)$ in the Primitive Groups Library [43] satisfy the hypotheses of Lemma 5.9.4 and have non-commuting, non-generating graphs that are connected with diameter 2 and 3, respectively. Both of these groups have socle $A_5 \times A_5$, and so are not almost simple. Although the focus of Chapter 6 is on the non-commuting, non-generating graphs of non-abelian finite simple groups, in §6.2 and §6.4 we will determine bounds on $\mathrm{diam}(\Xi(G))$ for certain non-simple almost simple groups $G$, and computationally determine exact values in a few small cases.

We now consider the larger family of groups consisting of central extensions of insoluble, non-simple primitive groups with every proper quotient cyclic.

**Lemma 5.9.5.** *Suppose that $\overline{G}$ is an insoluble, non-simple primitive group with every proper quotient cyclic.*

(i) *The subgraph $X$ of $\Xi(G)$ induced by the vertices in*

$$\{g \in G \setminus Z(G) \mid Z(G)g \in \Xi^+(\overline{G})\}$$

*has diameter at most $k := \mathrm{diam}(\Xi^+(\overline{G})) \in \{2, 3\}$. In particular, if $\Xi(\overline{G})$ has no isolated vertices, then $\mathrm{diam}(\Xi(G)) \leqslant k$.*

(ii) *If $X \neq \Xi^+(G)$, then $\Xi^+(G)$ is connected with diameter at most 4.*

*Proof.* By Proposition 2.1.23, $Z(\overline{G}) = 1$. Hence (i) is an immediate consequence of Lemma 5.9.4 and Corollary 5.2.12, with $N = Z(G)$.

To prove (ii), we will assume that $X \neq \Xi^+(G)$. If $G$ is not 2-generated, then $\mathrm{diam}(\Xi(G)) = 2$ by Corollary 5.2.7. Thus we will suppose that $G$ is 2-generated. Then $\overline{G}$ is also 2-generated, and we deduce from Lemma 5.9.4 that $G$ contains a normal maximal subgroup $M$ with $Z(M) = Z(G)$, and that each element of $M \setminus Z(G)$ lies in $X$.

Let $y, y' \in \Xi^+(G) \setminus X$, so that $y, y' \notin M$. Then Proposition 5.3.1 shows that $y \in K \setminus Z(K)$ for some maximal subgroup $K$ of $G$, and applying Proposition 5.4.1 to

the triple $(y, K, M)$ yields $y \sim m$ for some $m \in K \cap M$. Similarly, $y' \sim m'$ for some $m' \in M$. Corollary 5.2.8 gives $d(m, m') \leqslant 2$, and so $d(y, y') \leqslant d(y, m) + d(m, m') + d(m', y) \leqslant 4$.

By (i), it remains to consider $d(y, x)$, with $x \in X$. We also observe from (i) that $d(m, x) \leqslant 3$. Hence $d(y, x) \leqslant d(y, m) + d(m, x) \leqslant 4$, and we conclude that $\mathrm{diam}(\Xi^+(G)) \leqslant 4$. □

Recall from above that if $G = \overline{G}$ is the group numbered $(25, 25)$ in the Primitive Groups Library, then $\mathrm{diam}(\Xi(G)) = 3$. We can use the Magma code in `diam_nc_ng` to show that the non-commuting, non-generating graphs of the central extensions $G \times C_2$ and $G \times C_3$ of $G$ are connected with diameter 2 and 3, respectively (see also Proposition 5.5.3).

The following is a collection of open problems related to Lemma 5.9.5.

**Question 5.9.6.** *For which insoluble primitive groups $G$ with every proper quotient cyclic does $\Xi(G)$ contain isolated vertices? Are any such groups finite? When $G$ is infinite, can an isolated vertex lie in a non-abelian maximal subgroup? Is there an example where $\mathrm{diam}(\Xi^+(H)) = 4$, or where $\mathrm{diam}(\Xi^+(H)) = 3$ and $\Xi^+(H) \neq \Xi(H)$, for some central extension $H$ of $G$?*

The third question here is relevant as Theorem 2.1.16 does not apply to infinite groups, i.e., there are insoluble infinite groups that contain abelian maximal subgroups. For example, each Tarski monster group $T$ mentioned in §2.1.2 is an infinite insoluble (and simple) group with each maximal subgroup abelian, and hence each vertex in $\Xi(T)$ is isolated. On the other hand, we will prove in §6.2 that the non-commuting, non-generating graph of a finite simple group has no isolated vertices. Note also that if $H \cong G \times Z(H)$, where $G$ is as in Question 5.9.6 and $Z(H)$ is not cyclic, then Theorem 5.5.2 yields $\mathrm{diam}(\Xi(H)) = 2$.

In general, Proposition 5.3.1 shows that the isolated vertices of $\Xi(G)$ are precisely the elements of $G$ that lie in a unique maximal subgroup and are centralised by that subgroup. Indeed, Question 5.9.6 is closely related to Question 5.3.4. Moreover, by Lemma 5.9.4, any such maximal subgroup must be core-free in $G$, and no involution of $G$ is isolated (Lemma 5.3.7 shows that this is true even when $G$ is simple).

Theorem 5.3.3 also shows that only certain types of insoluble primitive groups with all maximal subgroups non-abelian may have non-commuting, non-generating graphs with isolated vertices. In particular, to answer Question 5.9.6 in the finite case, it suffices to consider the insoluble primitive groups $G$ of type AS (almost simple), PA (product action), SD (simple diagonal) and CD (compound diagonal), as in the O'Nan-Scott Theorem (see [120, §3]). Moreover, since every proper quotient

of $G$ is cyclic, the structure of $G$ is as described in [103, §3]. For the remaining O'Nan-Scott types, the minimal normal subgroups of $G$ intersect trivially with its point stabilisers, and so it follows from Theorem 5.3.3(iii) (and the fact that no maximal subgroup of $G$ is abelian) that $\Xi(G)$ has no isolated vertices.

Further exploration of Question 5.9.6 in the finite case may benefit from the results in [139], which provide a classification of elements of finite groups that lie in a unique maximal subgroup, in the case where the maximal subgroup is core-free. Additionally, Lemma 5.3.6 can be used in certain cases to show that non-involutory elements of particular orders are not isolated.

In the following example, we prove the connectedness of $\Xi(G)$ for a certain infinite family of infinite groups $G$ that satisfy the hypotheses of Lemma 5.9.4. Note that for a permutation group $G$ acting on a set $\Omega$, the *support* of an element $g \in G$ is the set $\{\alpha \in \Omega \mid \alpha^g \neq \alpha\}$. As in the finite case, an even permutation of an infinite permutation group is a product of an even number of transpositions. In particular, any such permutation has finite support.

**Example 5.9.7.** Let $\mathrm{Alt}(\mathbb{Z})$ be the (infinite) group of even permutations of $\mathbb{Z}$. Additionally, for each positive integer $k$, let $G_k$ be the group of permutations of $\mathbb{Z}$ generated by $\mathrm{Alt}(\mathbb{Z})$ and the translation $t_k$ that maps $x$ to $x + k$ for all $x \in \mathbb{Z}$. The groups $G_k$ were first introduced in [21, p. 292], but our formulation is from [45, p. 215]. Each $G_k$ is a finite index subgroup of the *Houghton group* $H_2$, which is generated by $t_1$ and all permutations of $\mathbb{Z}$ with finite support [21, Lemma 3.1(ii)] (see also [45, Definition 2.2]).

Now, $\mathrm{Alt}(\mathbb{Z})$ is a simple group and is the unique minimal normal subgroup of $G_k$ [44, Lemma 2.3, Proposition 2.5]. In particular, this means that $G_k$ is insoluble. Moreover, $G_k$ is 2-generated, and every proper quotient of $G_k$ is cyclic [45, Theorem 4.1]. It follows from Proposition 2.1.5 that $\langle t_k \rangle$ lies in a maximal subgroup $M$ of $G_k$. As $G_k = \langle \mathrm{Alt}(\mathbb{Z}), t_k \rangle$, the maximal subgroup $M$ does not contain the minimal normal subgroup $\mathrm{Alt}(\mathbb{Z})$. Hence $M$ is core-free in $G_k$, and so $G_k$ is primitive.

Finally, assume that $k \geqslant 3$, and let $g \in G_k \setminus \{1\}$. Since $\mathrm{Alt}(\mathbb{Z})$ is the union of its finite alternating subgroups, it is generated by its 3-cycles. Additionally, $C_{G_k}(\mathrm{Alt}(\mathbb{Z})) = 1$ by Theorem 2.1.24. It follows that there exists a 3-cycle $\alpha \in \mathrm{Alt}(\mathbb{Z})$ such that $[g, \alpha] \neq 1$. Furthermore, the proofs of [45, Lemmas 4.2–4.3] show that no 3-cycle in $\mathrm{Alt}(\mathbb{Z})$ lies in a generating set for $G_k$ of size two. Hence $\{g, \alpha\}$ is an edge of $\Xi(G_k)$. In particular, $\Xi(G_k)$ has no isolated vertices. Using Lemmas 5.9.4 and 5.9.5(i), we conclude that $\Xi(G_k)$ is connected with diameter 2 or 3, as is $\Xi(H)$ for each central extension $H$ of $G_k$.

It would be interesting to determine the exact diameter of $\Xi(G_k)$ for each $k \geqslant 3$, and to determine the diameters of $\Xi(G_k)$ and $\Xi^+(G_k)$ for each $k \in \{1, 2\}$. We note that the above argument does not apply when $k \leqslant 2$, as here every non-identity element of $G_k$ lies in a generating set for the group of size two [45, Theorem 6.1]. As we mentioned earlier in this section, this is also true for each non-identity element of any finite group with every proper quotient cyclic, as proved in [22, Theorem 1].

We now state this section's main theorem, which summarises the possible structures of $\Xi(G)$ when $\overline{G}$ is not simple. This theorem is nearly identical to Theorem 5.1.5, the main theorem of this chapter. However, we assume here that $\Xi(G)$ contains an edge, and we give a slightly more detailed description of the finite groups $G$ for which $\Xi(G)$ has two nontrivial connected components.

**Theorem 5.9.8.** *Suppose that $\overline{G} = G/Z(G)$ is not simple, and that $\Xi(G)$ contains an edge. Then (at least) one of the following holds.*

(i) *$\Xi(G)$ has an isolated vertex, and $\Xi^+(G)$ is connected with diameter 2. If $\overline{G}$ has a proper non-cyclic quotient, then $G$ is soluble.*

(ii) *$\Xi(\overline{G})$ has an isolated vertex, $\Xi^+(G)$ is connected with diameter at most 4, and the subgraph of $\Xi(G)$ induced by the vertices in*

$$\{g \in G \setminus Z(G) \mid Z(G)g \in \Xi^+(\overline{G})\}$$

*is connected with diameter at most $\operatorname{diam}(\Xi^+(\overline{G}))$, which is equal to 2 or 3. Additionally, $\overline{G}$ is an insoluble primitive group with every proper quotient cyclic.*

(iii) *$\Xi(G)$ is connected with diameter 2 or 3.*

(iv) *$\Xi(G)$ is connected with diameter 4, $G$ is infinite, and $\overline{G}$ has a proper non-cyclic quotient.*

(v) *$\Xi(G)$ has exactly two connected components, each of diameter 2.*

*Furthermore, if $G$ is finite, then (v) holds if and only if $G$ satisfies Assumption 5.7.3.*

*Proof.* If $\overline{G}$ has a proper non-cyclic quotient, then $G$ contains a normal subgroup $N$ such that $Z(G) < N$ and $G/N$ is not cyclic. Thus in this case Theorem 5.8.12 applies, and (i), (iii), (iv) or (v) holds. Otherwise, one of the three cases in Lemma 5.9.1 holds, with $\overline{G}$ in place of $G$. If every maximal subgroup of $G$ is normal, or if $\overline{G}$ is soluble and primitive, then we can use Theorem 5.4.3 or Lemma 5.9.3, respectively, to show that (i) or (iii) holds. If instead $\overline{G}$ is insoluble and primitive, then Lemma 5.9.5 shows that (ii) or (iii) holds. It now follows from Theorem 5.8.12

and Proposition 5.8.8 that if $G$ is finite, then (v) holds if and only if $G$ satisfies Assumption 5.7.3. □

We see from the above proof that if $\Xi(G)$ has two nontrivial connected components, then Theorem 5.8.12 applies. Hence, as discussed below the statement of that theorem, Lemma 5.7.15 and Proposition 5.7.9 yield further information about the structure of infinite groups in this case.

It is an open problem to determine whether cases (ii) and (iv) above can occur; see Questions 5.7.8, 5.7.13 and 5.9.6, and Remark 5.7.14. In Chapter 6, we will see that $\Xi(G)$ is connected whenever $G$ is a central extension of a non-abelian finite simple group. Hence Theorem 5.9.8 gives a precise description of all finite groups $G$ such that $\Xi(G)$ has more than one nontrivial connected component.

Note that Lucchini [102, Theorem 1] proved that if $G$ is a finite 2-generated soluble group, then the subgraph of the generating graph of $G$ induced by its non-isolated vertices is connected with diameter at most 3. By Theorem 5.9.8, this also holds for the non-commuting, non-generating graph of such a group, except in the cases where $\Xi(G)$ has two connected components of diameter 2. As mentioned in §5.5, it follows from [47, Theorem 1.3] that there is no bound on the diameter of a connected component of the generating graph of a non-simple finite insoluble group.

The possibilities for the structure of $\Xi(G)$ are much more limited when $\overline{G}$ is finite and $G$ contains an abelian maximal subgroup.

**Proposition 5.9.9.** *Suppose that $\overline{G} = G/Z(G)$ is finite, that $G$ contains an abelian maximal subgroup, and that $\Xi(G)$ has an edge. Then* $\operatorname{diam}(\Xi^+(G)) = 2$.

*Proof.* Let $L$ be an abelian maximal subgroup of $G$. Then Proposition 2.1.7 yields $Z(G) \leqslant L$. Hence $\overline{L}$ is an abelian maximal subgroup of the finite group $\overline{G}$. Thus Theorem 2.1.16 shows that $\overline{G}$ is soluble.

Suppose first that $G$ contains a normal subgroup $N$ such that $G/N$ is not cyclic and $N \not\leqslant Z(G)$. Then $C := C_G(N)$ and $C_G(C)$ both contain $Z(G)$, and since $\overline{G} = G/Z(G)$ is finite, so are $G/C$ and $G/C_G(C)$. It therefore follows from Proposition 5.8.14 that $\operatorname{diam}(\Xi^+(G)) = 2$.

If instead $G$ has no such subgroup $N$, then every proper quotient of $\overline{G}$ is cyclic, and Lemma 5.9.1 shows that either $\overline{G}$ is primitive, or every maximal subgroup of $\overline{G}$ is normal. We observe from Lemma 5.9.3 in the former case and Theorem 5.4.3 in the latter case that $\operatorname{diam}(\Xi^+(G)) = 2$. □

This result leads to the following open question.

**Question 5.9.10.** *Does there exist a group $G$ that contains an abelian maximal subgroup (with $\overline{G}$ infinite), such that $\Xi^+(G)$ has an edge and is not connected with diameter 2?*

As mentioned above, the Tarski monster groups are examples of infinite simple groups with abelian maximal subgroups. Note also that, for certain families of groups $G$ containing abelian maximal subgroups (with $\overline{G}$ infinite), we have already seen that $\Xi(G)$ has no connected component of diameter greater than 2. For example, this is the case if $G$ contains a normal subgroup $N$ satisfying the hypotheses of Lemma 5.8.6, or, by Theorem 5.4.3, if every maximal subgroup of $G$ is normal. We also note that if $G$ contains a normal subgroup $N$ satisfying the hypotheses of Lemma 5.8.7 (so that $G/C_G(N) \cong \mathbb{Z}$ by Proposition 5.8.5(iii)), then Lemma 2.1.12 shows that the first column of Table 5.8.2 does not apply. Hence if we can reduce the upper bound of 3 in the $(1, 3)$ entry of this table in this case, then we do not need to assume any finiteness conditions here.

## 5.10 Free products of groups

We conclude this chapter with a brief exploration of the non-commuting, non-generating graph of a free product of nontrivial groups, as defined below. Note that this is a special case of Theorem 5.9.8.

**Definition 5.10.1** ([105, p. 174])**.** Let $G_1$ and $G_2$ be groups with respective presentations $\langle X_1 \mid R_1 \rangle$ and $\langle X_2 \mid R_2 \rangle$, where $X_1$ and $X_2$ are disjoint. The *free product* of $G_1$ and $G_2$ is $G_1 * G_2 := \langle X_1 \cup X_2 \mid R_1 \cup R_2 \rangle$.

If necessary, we can relabel the generators for a given group $G_2$ so that $X_1$ and $X_2$ are disjoint as required. We may therefore consider $G_1$ and $G_2$ as subgroups of $G_1 * G_2$, with $G_1 \cap G_2 = 1$. Note that, up to isomorphism, $G_1 * G_2$ is in fact independent of the choice of presentations for $G_1$ and $G_2$ [105, p. 174]. It is also clear that $G_1 * G_2 \cong G_2 * G_1$.

**Example 5.10.2.** As the infinite cyclic group $\mathbb{Z}$ has presentation $\langle a \mid - \rangle$, the free product $\mathbb{Z} * \mathbb{Z}$ is the group with presentation $\langle a, b \mid - \rangle$, i.e., the free group on two generators. Additionally, the cyclic group $C_2$ has presentation $\langle c \mid c^2 = 1 \rangle$, and hence $C_2 * C_2$ is the group with presentation $\langle c, d \mid c^2 = d^2 = 1 \rangle$, i.e., the infinite dihedral group.

As there is no defining relation in $G_1 * G_2$ between any non-identity element of $G_1$ and any non-identity element of $G_2$, the minimum size of a generating set for $G_1 * G_2$

is the sum of the minimum size of a generating set for $G_1$ and the minimum size of a generating set for $G_2$. Recall from Corollary 5.2.7 that if $H$ is a non-abelian group that is not 2-generated, then $\Xi(H)$ is connected with diameter 2. We therefore need only consider $\Xi(G_1 * G_2)$ when $G_1$ and $G_2$ are each cyclic and nontrivial. Observe also that if $G_1$ and $G_2$ are nontrivial, then $Z(G_1 * G_2) = 1$. Hence each non-identity element of $G_1 * G_2$ is a vertex of $\Xi(G_1 * G_2)$.

As in §5.5, we assume the convention that each positive integer divides the order of an infinite group. Recall also from Proposition 5.2.5 that any nontrivial connected component of $\Xi(G)$, for any group $G$, has diameter at least 2.

**Theorem 5.10.3.** *Let $G_1 = \langle a \rangle$ and $G_2 = \langle b \rangle$ be (possibly infinite) nontrivial cyclic groups. If $G_1 \cong C_2 \cong G_2$, then $ab$ and $ba$ are isolated vertices of $\Xi(G_1 * G_2)$, while the remaining vertices form a connected component of diameter 2. Otherwise, $\Xi(G_1 * G_2)$ is connected with diameter 2.*

*Proof.* Let $G := G_1 * G_2$, and let $x := (ab)^j$ for some nonzero integer $j$. Since $G_1$ and $G_2$ are cyclic, it follows from [107, Corollary 4.1.6, Problem 4.1.9] that $C_G(x) = \langle ab \rangle$. Thus the neighbours of $x$ in $\Xi(G)$ are precisely the elements $f \in G \setminus \langle ab \rangle$ satisfying $\langle f, x \rangle < G$. By symmetry, the neighbours of $x' := (ba)^j$ are the elements $f \in G \setminus \langle ba \rangle$ satisfying $\langle f, x' \rangle < G$. We split the remainder of the proof into two cases. As a major component of the proof in each case, we will show that, for certain values of $j$, each element $f$ of the set $G \setminus \langle ab \rangle$ or $G \setminus \langle ba \rangle$ satisfies the above non-generation property.

**Case (a)**: $G_1 \cong C_2 \cong G_2$. For each integer $n \geqslant 2$, let $H_n$ be the dihedral group of order $2n$. Then there exist elements $\alpha, \beta \in H_n$ such that $\langle \alpha, \beta \rangle = H_n$, $|\alpha| = 2 = |\beta|$, and $|\alpha\beta| = n$. Let $\phi_n$ be the epimorphism from $G$ to $H_n$ defined by $(a)\phi_n := \alpha$ and $(b)\phi_n := \beta$. Then each $g \in G$ satisfies $(\langle g, (ab)^n \rangle)\phi_n = \langle (g)\phi_n, ((ab)\phi_n)^n \rangle = \langle (g)\phi_n, 1 \rangle$, which is a proper subgroup of the non-cyclic group $H_n = (G)\phi_n$. Thus $\langle g, (ab)^n \rangle < G$, and so $(ab)^n$ does not lie in any generating set for $G$ of size two. Hence each element of $G \setminus \langle ab \rangle$ is adjacent in $\Xi(G)$ to $(ab)^n$ for each $n \geqslant 2$, and also to $(ab)^{-n}$ by Proposition 5.2.1.

Now, $G \setminus \langle ab \rangle \neq \varnothing$, and $(ab)^{-1} = ba$. Thus each element of $\langle ab \rangle \setminus \{1, ab, ba\}$ is adjacent in $\Xi(G)$ to each element of $G \setminus \langle ab \rangle$, and so $d(r, s) \leqslant 2$ for all $r, s \in G \setminus \{1, ab, ba\}$. It remains to show that the vertices $ab$ and $ba$ of $\Xi(G)$ are isolated.

Suppose for a contradiction that some vertex $u$ of $\Xi(G)$ is adjacent to $ab$. Then $u$ does not centralise $ab$, and hence $u \in G \setminus \langle ab \rangle$. However, it is easy to see that $|G : \langle ab \rangle| = 2$, and so $\langle ab, u \rangle = G$, a contradiction. Therefore, $ab$ is an isolated vertex of $\Xi(G)$. By symmetry, the vertex $ba$ is also isolated.

**Case (b)**: $G_1 \ncong C_2$ or $G_2 \ncong C_2$. Let $m$ be an integer dividing $|G_1|$ and $n$ an integer dividing $|G_2|$, with $m, n \geqslant 2$, and let $k := m + n - 1$. In addition, let $\theta$ be the homomorphism from $G$ to the symmetric group $S_k$ defined by $(a)\theta := (1, 2, \ldots, m)$ and $(b)\theta := (m, m+1, \ldots, k)$. Then $(ab)\theta = (1, 2, \ldots, m-1, m+1, m+2, \ldots, k, m)$ and $(ba)\theta = (1, 2, \ldots, k)$. Hence $|(ab)\theta| = k = |(ba)\theta|$, and $(G)\theta$ is non-abelian and therefore non-cyclic (in fact, it can be shown that $(G)\theta$ contains $A_k$). Thus for all $g \in G$, the group $(\langle g, (ab)^k \rangle)\theta = \langle (g)\theta, ((ab)\theta)^k \rangle = \langle (g)\theta, 1 \rangle$ is a proper subgroup of $(G)\theta$. It follows that $(ab)^k$ does not lie in any generating set for $G$ of size two, and similarly, neither does $(ba)^k$. In fact, since $((ba)\theta)^{-k}((ab)\theta)^k = 1$, no generating set for $G$ of size two contains the element $(ba)^{-k}(ab)^k = (a^{-1}b^{-1})^k(ab)^k$.

Now, since either $a^{-1} \neq a$ or $b^{-1} \neq b$, the element $(a^{-1}b^{-1})^k(ab)^k$ does not lie in $\langle ab \rangle \cup \langle ba \rangle$. It follows that each element of $G \setminus \langle ab \rangle$ is adjacent in $\Xi(G)$ to $(ab)^k$; that each element of $G \setminus \langle ba \rangle$ is adjacent to $(ba)^k$; and that each non-identity element of $\langle ab \rangle \cup \langle ba \rangle$ is adjacent to $(a^{-1}b^{-1})^k(ab)^k$. Since $\langle ab \rangle \cap \langle ba \rangle = 1$, we conclude that any two vertices of $\Xi(G)$ have a common neighbour in $\{(ab)^k, (ba)^k, (a^{-1}b^{-1})^k(ab)^k\}$, and thus $\Xi(G)$ is connected with diameter 2. □

# Chapter 6

# The non-commuting, non-generating graph of a finite simple group

## 6.1 General results and the main theorem

In this chapter, we explore the diameter of the non-commuting, non-generating graph of a non-abelian finite simple group. Throughout, $G$ will denote any such group, except where specified otherwise. Recall from Theorem 2.4.4 that $G$ is 2-generated. Hence the graph is interesting in each case, in the sense that Corollary 5.2.7 does not apply.

As previously mentioned, we will not in general explore the non-commuting, non-generating graph of an infinite simple group. However, any such group that is not 2-generated has a graph that is connected with diameter 2 by Corollary 5.2.7 (see also the discussion following the statement of this corollary). Additionally, any infinite simple group that is minimal non-abelian, for example a Tarski monster group, has a graph with every vertex isolated.

We will again use the graph theoretic notation outlined at the start of Chapter 4, and the notation $\Xi(G)$ and $\Xi^+(G)$ from Definition 5.1.3. As in Chapter 5, when $x, y \in G \setminus \{1\}$ and the underlying group $G$ is clear, we will write $x \sim y$ in place of $x \sim_{\Xi(G)} y$, and $d(x, y) := d_{\Xi(G)}(x, y)$, except where specified otherwise.

The first result in this chapter describes important relationships between involutions and maximal subgroups of $G$.

**Proposition 6.1.1.** *Let $L$ and $M$ be maximal subgroups of the non-abelian finite simple group $G$, and suppose that $|L|$ is even.*

(i) *Suppose that $Z(L)$ contains an involution $a$. Then $L \setminus Z(L)$ contains a $G$-conjugate of $a$.*

(ii) *$L$ contains an involution that does not lie in $Z(L) \cup Z(M)$.*

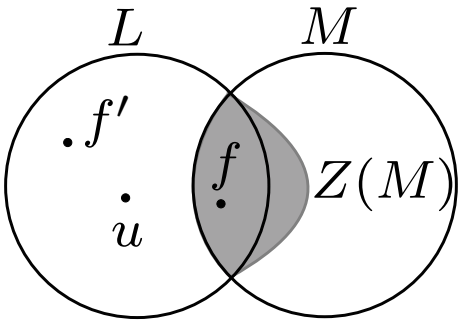



Figure 6.1.1: An illustration of Proposition 6.1.1(iv).

(iii) *Suppose that $|M|$ is even, and let $a$ be an involution of $L \setminus M$. Then $M \setminus Z(M)$ contains an involution $b$ that does not commute with $a$.*

(iv) *Suppose, as in Figure 6.1.1, that $L \cap M$ lies in $Z(M)$ and contains an involution $f$. Additionally, let $u \in L \setminus M$. Then $L \setminus M$ contains an involution $f'$ such that $[u, f'] \neq 1$.*

*Proof.*

(i) Let $a$ be an involution of $L$, and suppose first that $a \in Z(L)$. Then $C_G(a) = L$ by Proposition 2.1.7. As $G$ is simple (and has even order), Theorem 5.3.5 (with $a$ in place of $x$) shows that there exists an element $g \in G$ such that $a \neq a^g \in C_G(a) = L$. In fact, as $a \in Z(L)$, we deduce that $g \in G \setminus L$. Furthermore, $L^g \neq L$, since $L$ is maximal and non-normal in $G$. Finally, $L^g = C_G(a^g)$, and hence the involution $a^g$ is non-central in $L$.

(ii) We will prove that $L$ contains an involution $s$ that does not lie in $Z(L) \cup Z(M)$. It follows from (i) that there exists an involution $y \in L \setminus Z(L)$. If $y \notin Z(M)$, then we can set $s = y$. If instead $y \in Z(M)$ (so that $L \neq M$), then $C_G(y) = M$ by Proposition 2.1.7. Additionally, since $Z(L)$ and $L \cap M$ are proper subgroups of $L$, there exists $h \in L \setminus (Z(L) \cup M)$, and $y^h$ is a non-central involution of $L$. Moreover, $M \neq M^h = C_G(y^h)$. Therefore, $y^h \notin Z(M)$, and so we can set $s = y^h$.

(iii) We split the proof into two cases.

**Case (a)**: $|Z(M)|$ is odd. Let $S$ be the set of involutions of $M$, and let $Q_M$ be the subgroup of $M$ generated by $S$. Since conjugation preserves the order of an element, $Q_M$ is normal in $M$. If the involution $a \in L \setminus M$ commutes with each element of $S$, then $a \in C_G(Q_M)$, and so $Q_M \trianglelefteq \langle M, a \rangle = G$, contradicting

the simplicity of $G$. Thus there exists $r \in S \setminus C_G(a)$. As $S \cap Z(M) = 1$, we can set $b = r$.

**Case (b)**: $Z(M)$ contains an involution $z$. By applying (i) to $M$, we deduce that $M \setminus Z(M)$ contains an involution $c$. If $[a, c] \neq 1$, then we can set $b = c$. If instead $[a, c] = 1$, then consider the element $zc \in M \setminus Z(M)$. As $[z, c] = 1$, we see that $|zc| = 2$. In addition, the commutator identity given in Proposition 2.1.3(ii) shows that $[a, zc] = [a, c][a, z]^c = [a, z]^c$. Furthermore, $C_G(z) = M$ by Proposition 2.1.7. Since $a \notin M$, we conclude that $[a, z] \neq 1$. Hence $[a, zc] \neq 1$, and we may set $b = zc$.

(iv) Let $s \in L$ be the involution from (ii), so that $s \notin Z(M)$. Then $s \notin L \cap M \leqslant Z(M)$. If $[u, s] \neq 1$, then we can set $f' = s$. Assume therefore that $[u, s] = 1$. By Proposition 2.1.7, $C_G(f) = M$, and similarly, $C_G(f^s) = M^s \neq M$. Thus $f^s$ lies in $L$ but not in $Z(M)$, and hence not in $L \cap M$. If $f^s$ centralises $u$, then $C_L(u)$ contains $\langle s, f^s \rangle$, which contains $f$. This is a contradiction, as $u \notin M = C_G(f)$. We can therefore set $f' = f^s$. □

The following lemma, which gives upper bounds for the distances between certain vertices of $\Xi(G)$, is the key ingredient in many of this chapter's most important results.

**Lemma 6.1.2.** *Let $L$ and $M$ be maximal subgroups of the non-abelian finite simple group $G$, with $|L|$ and $|M|$ even. Additionally, let $x \in L \setminus Z(L)$ and $y \in M \setminus Z(M)$. Then $d(x, y) \leqslant 5$. Moreover, if $L$ contains an involution $a$ such that $d(x, a) \leqslant 1$, then $d(x, y) \leqslant 4$.*

*Proof.* We will use Corollary 5.2.8 several times in this proof without further reference. First, we may assume that $L \neq M$, as otherwise $d(x, y) \leqslant 2$. Proposition 6.1.1(i) shows that the set $\mathcal{A}$ of involutions of $L \setminus Z(L)$ is non-empty. We also observe that $d(x, u) \leqslant 2$ for all $u \in \mathcal{A}$. Choose $a \in \mathcal{A}$ so that $d(x, a) = \min_{u \in \mathcal{A}} d(x, u)$. Note that no element of $Z(L)$ is adjacent to $x$ in $\Xi(G)$, and so if $d(x, a) > 1$, then $x$ is neither equal nor adjacent to any involution of $L$. We split the remainder of the proof into three cases, depending on where $a$ lies with respect to $M$ and $Z(M)$. In particular, we will show that $d(x, y) \leqslant 5$, with $d(x, y) \leqslant 4$ if $d(x, a) \leqslant 1$.

**Case (a)**: $a \in M \setminus Z(M)$. Here, $d(a, y) \leqslant 2$, and so $d(x, y) \leqslant d(x, a) + d(a, y) \leqslant 4$.

**Case (b)**: $a \notin M$. By Proposition 6.1.1(iii), there exists an involution $b \in M \setminus Z(M)$ such that $[a, b] \neq 1$. Then $\langle a, b \rangle$ is a dihedral (and therefore proper) subgroup of $G$, and so $a \sim b$. Since $d(b, y) \leqslant 2$, we conclude that $d(x, y) \leqslant d(x, a) + d(a, b) + d(b, y) \leqslant 5$. Moreover, if $d(x, a) \leqslant 1$, then $d(x, y) \leqslant 4$.

**Case (c)**: $a \in Z(M)$. Here, $M = C_G(a)$ by Proposition 2.1.7, and Proposition 6.1.1(ii) yields an involution $a' \in \mathcal{A}$ that does not lie in $Z(M)$. Hence we can replace $a$ by $a'$ in the arguments in Cases (a) and (b) to deduce that $d(x, y) \leqslant 5$, with $d(x, y) \leqslant 4$ if either $a' \in M$ or $d(x, a') \leqslant 1$.

It remains to show (in the case $a \in Z(M)$) that if $d(x, a) \leqslant 1$, $a' \notin M = C_G(a)$, and $d(x, a') > 1$, then $d(x, y) \leqslant 4$. Since $a' \notin C_G(a)$ and $x, a' \in L$, we may assume that $x \neq a$, as otherwise $d(x, a') = 1$. Thus $d(x, a) = 1$, and hence $x \notin C_G(a) = M$.

Suppose for now that $L \cap M \leqslant Z(M)$. Then since $x \in L \setminus M$, and since $a$ is an involution of $Z(M)$, Proposition 6.1.1(iv) shows that there exists an involution $f' \in L \setminus M$ such that $x \sim f'$. In particular, $f' \in \mathcal{A}$, and we can replace $a$ with $f'$ in the argument in Case (b) to deduce that $d(x, y) \leqslant 4$.

Finally, suppose that there exists an element $c \in L \cap M$ that does not lie in $Z(M)$. As $a$ also lies in $L \cap M$, but not in $C_G(x)$, there exists an element $h \in L \cap M$ that centralises neither $M$ nor $x$. Thus $d(h, y) \leqslant 2$ and $x \sim h$, and so $d(x, y) \leqslant 3$. □

The following corollary is an immediate consequence of Lemma 6.1.2 and Proposition 5.3.1, which states that each non-isolated vertex of $\Xi(G)$ is a non-central element of some maximal subgroup of $G$.

**Corollary 6.1.3.** *If every maximal subgroup of the non-abelian finite simple group $G$ has even order, then* $\operatorname{diam}(\Xi^+(G)) \leqslant 5$.

Observe that the only non-elementary result used in the proof of Lemma 6.1.2 is Proposition 6.1.1, whose proof in turn uses elementary facts and the $p = 2$ case of Theorem 5.3.5. As we mentioned in §5.3, this $p = 2$ case was proved in [61] without using the classification of finite simple groups. Hence the proofs of Lemma 6.1.2 and Corollary 6.1.3 are also classification-free.

We now state this chapter's main theorem.

**Theorem 6.1.4.** *Let $G$ be a non-abelian finite simple group.*

(i) *$\Xi(G)$ is connected with diameter at most 5.*

(ii) *If $G$ is a sporadic simple group or the Tits group, then $\Xi(G)$ is connected with diameter at most 4.*

(iii) *For certain simple groups $G$, Table 6.1.1 lists upper bounds or exact values for* $\operatorname{diam}(\Xi(G))$.

The proof of the above theorem will be the primary focus of §6.2–6.6. By Corollary 6.1.3, if every maximal subgroup of $G$ has even order, then $\Xi^+(G)$ is connected

Table 6.1.1: Upper bounds or exact values for the diameters of the non-commuting, non-generating graphs of certain simple groups $G$. Here, $n$ is a positive integer and $q$ is a prime power.

| $G$ | $\mathrm{diam}(\Xi(G))$ |
|---|---|
| $\mathrm{M}_{11}, \mathrm{M}_{12}, \mathrm{M}_{22}, \mathrm{J}_2$ | 2 |
| $\mathrm{M}_{23}, \mathrm{J}_1$ | 3 |
| $\mathbb{B}, \mathrm{PSU}(7,2)$ | 4 |
| $A_n$; $n$ even | $\leqslant 3$ |
| $A_n$; $n$ odd | $\leqslant 4$ |
| $\mathrm{PSL}(n,q), \mathrm{Sz}(q)$ | $\leqslant 4$ |
| $G_2(q), {}^2G_2(q), {}^3D_4(q), F_4(q), E_8(q)$; $q$ odd | $\leqslant 4$ |

with diameter at most 5. Thus to prove Theorem 6.1.4(i), it remains to show that this remains true when $G$ has a maximal subgroup of odd order (i.e., when $G$ is a group listed in Theorem 4.2.3), and that, in general, $\Xi(G)$ has no isolated vertices. We show that this last statement is true in §6.2, and we give a formal proof of Theorem 6.1.4(i) in §6.5. We also prove in §6.5 a similar result about the diameter of the non-generating graph of a non-abelian finite simple group, as in Definition 5.1.2. A version of this result is an important component of the main theorem of [104], which determines when the non-generating graph of a finite group is connected, once vertices that are joined to all other vertices have been deleted, and which provides upper bounds for the diameter of this graph in the connected case.

Note also that in §6.2 and §6.4–6.6, we present examples of diameters achieved by certain simple alternating, linear, unitary and exceptional groups, computed using Magma. However, none of the (non-unitary) examples meet the corresponding upper bounds given in Table 6.1.1. Indeed, the following question is open.

**Question 6.1.5.** *Which, if any, of the upper bounds for* $\mathrm{diam}(\Xi(G))$ *given in Table 6.1.1 are tight? In the cases where the upper bound is not tight, what is the best possible upper bound?*

We now state a corollary of Theorem 6.1.4(i), which is analogous to Lemma 5.9.5(i) (except in this case, we know that $\Xi(G)$ has no isolated vertices), and which complements the finite case of Theorem 5.1.5.

**Corollary 6.1.6.** *Let $G$ be a non-abelian finite simple group, and let $H$ be a central extension of $G$. Then* $\mathrm{diam}(\Xi(H)) \leqslant \mathrm{diam}(\Xi(G)) \leqslant 5$.

*Proof.* This is an immediate consequence of Theorem 6.1.4 and Corollary 5.2.12, with $Z(H)$ in place of $N$. □

Finally, Theorem 6.1.4 and Table 6.1.1 lead to the following additional open questions.

**Question 6.1.7.** *Does there exist a non-abelian finite simple group $G$ such that* $\mathrm{diam}(\Xi(G)) = 5$*? In addition, for which non-abelian finite simple groups $G$ is* $\mathrm{diam}(\Xi(G))$ *equal to* $4$*?*

Recall from Theorem 4.1.4 and Proposition 4.1.5 that $\mathrm{PSU}(7,2)$ has an intersection graph of diameter 5, and that there may be additional non-abelian finite simple unitary groups with this property. By Proposition 5.2.15, the non-commuting, non-generating graph of any such group has diameter at least 4. Indeed, this fact will serve as part of the proof that $\Xi(\mathrm{PSU}(7,2))$ has diameter 4 (and similarly for the graph of the baby monster group).

## 6.2 Alternating groups

In this section, we prove the alternating case of Theorem 6.1.4. In fact, we prove the following more general result.

**Theorem 6.2.1.** *Let $G$ be an almost simple group whose socle is an alternating group $A_n$. Then $\Xi(G)$ is connected with diameter at most 4. Moreover, if $n$ is even, or if $G$ is not simple, then* $\mathrm{diam}(\Xi(G)) \leqslant 3$.

We will also conclude this section with a proof that $\Xi(G)$ has no isolated vertices whenever $G$ is a non-abelian finite simple group.

Observe that Theorem 6.2.1 shows that no almost simple group with alternating socle yields a positive answer to the finite case of Question 5.9.6. Additionally, it is well-known that the finite symmetric groups are 2-generated, and Theorem 2.4.5 shows that the same is true for the other proper overgroups of $A_6$ in $\mathrm{Aut}(A_6)$.

In order to prove Theorem 6.2.1, we will require a few intermediate results. Here, we consider the usual action of the symmetric and alternating groups of degree $n$ on the set $\Omega := \{1, 2, \ldots, n\}$. Note that a *derangement* of a permutation group is a permutation with no fixed points.

**Proposition 6.2.2.** *Let $G$ be an alternating or symmetric group of degree $n \geqslant 5$, and let $x$ be a derangement of $G$ that has at least two orbits on $\Omega$. In addition, let $\{\alpha_1, \alpha_2\}$ and $\{\beta_1, \beta_2\}$ be 2-subsets of distinct orbits of $\langle x \rangle$ on $\Omega$. Finally, if $\langle x \rangle$ has exactly two orbits on $\Omega$, then let $g := (\alpha_1, \alpha_2)(\beta_1, \beta_2)$, and otherwise, let $g := (\alpha_1, \alpha_2, \beta_1)$. Then $\{x, g\}$ is an edge of $\Xi(G)$.*

*Proof.* If $\langle x\rangle$ has exactly two orbits on $\Omega$, then at least one of these orbits has length at least three. Hence, in each case, $x^g \neq x$, and so $[x,g] \neq 1$. Additionally, $\langle x, g\rangle$ acts intransitively on $\Omega$ and is therefore a proper subgroup of $G$. Thus $x \sim g$. □

**Proposition 6.2.3.** *Let $G$ be an alternating or symmetric group of degree $n \geqslant 5$, and let $x, y \in G\backslash\{1\}$. Then $d(x,y) \leqslant 4$. Moreover, if $d(x,y) \geqslant 3$, then at least one of $x$ and $y$ is a derangement, and if $d(x,y) = 4$, then both elements are derangements.*

*Proof.* For each positive integer $k$, let $X_k := S_k$ if $G$ is a symmetric group, or $X_k := A_k$ if $G$ is an alternating group. Observe that for each $\alpha \in \Omega$, the point stabiliser $G_\alpha$ is a maximal subgroup of $G$ isomorphic to $X_{n-1}$. As $Z(X_{n-1}) = 1$, it follows from Corollary 5.2.8 that $d(g,h) \leqslant 2$ for all non-identity elements $g, h \in G_\alpha$. Additionally, given distinct $\alpha, \beta \in \Omega$, the intersection $G_\alpha \cap G_\beta$ is isomorphic to $X_{n-2}$ and is maximal in each of $G_\alpha$ and $G_\beta$. Thus for all $g \in G_\alpha$ and $m \in G_\beta$ satisfying $g, m \notin G_\alpha \cap G_\beta$, we obtain $d(g,m) \leqslant 2$ by applying Proposition 5.4.1(ii) to the triple $(g, G_\alpha, G_\beta)$ and the element $m$. We have shown that any two non-derangements of $G$ are joined in $\Xi(G)$ by a path of length at most two. It therefore suffices to prove that each derangement $x \in G$ is adjacent in $\Xi(G)$ to some non-derangement. This follows immediately from Proposition 6.2.2 if $\langle x\rangle$ has at least two orbits on $\Omega$. We may therefore assume that $\langle x\rangle$ acts transitively on $\Omega$.

Now, the element $x$ is equal to an $n$-cycle $(\alpha_1, \ldots, \alpha_n)$, with $\alpha_i \in \Omega$ for each $i$. It suffices to show that there exists $y \in N_{G_{\alpha_1}}(\langle x\rangle)$ with $x^y \neq x$; it will then follow that $\langle x, y\rangle \leqslant N_G(\langle x\rangle) < G$ and $[x,y] \neq 1$, so that $x \sim y$. Notice that, for each $n$-cycle $r \in \langle x\rangle$ with $r \neq x$, there exists an element $s \in N_{(S_n)_{\alpha_1}}(\langle x\rangle)$ such that $x^s = r$. There are exactly $\phi(n) - 1 \geqslant 1$ such $n$-cycles, where $\phi$ is Euler's totient function. Hence if $G = S_n$, then a suitable element $y$ exists. In particular, we can choose $y$ so that $x^y = x^{-1}$. If instead $G = A_n$, then the transitivity of $\langle x\rangle$ implies that $n$ is odd. As $n \geqslant 5$, we observe that $\phi(n) - 1 \geqslant 2$. Hence there exist $s, s' \in N_{(S_n)_{\alpha_1}}(\langle x\rangle)$ such that $x^s = x^{-1}$ and $x^{s'} = x^i$ for some $i \in \{2, \ldots, n-2\}$. Since $x^{ss'} = x^{-i} \neq x$, we can choose $y \in G \cap \{s, s', ss'\} \neq \varnothing$. □

The following proposition about simple alternating groups also applies to almost simple symmetric groups. However, the proof in the symmetric case is much simpler; see the proof of Theorem 6.2.1 below. Here, for an element $g \in G$, we write $\mathrm{supp}(g)$ to denote the support $\{\alpha \in \Omega \mid \alpha^g \neq \alpha\}$ of $g$.

**Proposition 6.2.4.** *Let $G$ be an alternating group of degree $n \geqslant 5$, and let $x$ and $y$ be derangements of $G$ such that each of $\langle x\rangle$ and $\langle y\rangle$ has at least two orbits on $\Omega$. Then $d(x,y) \leqslant 3$.*

*Proof.* Let $\{\alpha_1, \alpha_2\}$ and $B := \{\beta_1, \beta_2\}$ be 2-subsets of distinct orbits of $\langle x\rangle$ on $\Omega$, such that $|\alpha_1^{\langle x\rangle}| \geqslant |\beta_1^{\langle x\rangle}|$, and let $\{\gamma_1, \gamma_2\}$ and $D := \{\delta_1, \delta_2\}$ be 2-subsets of distinct orbits of $\langle y\rangle$ on $\Omega$. We may assume without loss of generality that $\alpha_1 = \gamma_1$. We split the proof into three cases, depending on how many orbits each of $\langle x\rangle$ and $\langle y\rangle$ have on $\Omega$. Notice that if $|\Omega| = 5$, then each of $\langle x\rangle$ and $\langle y\rangle$ has exactly two orbits on $\Omega$.

**Case (a)**: $\langle x\rangle$ and $\langle y\rangle$ each have exactly two orbits on $\Omega$. Proposition 6.2.2 shows that $x$ is adjacent in $\Xi(G)$ to $a := (\alpha_1, \alpha_2)(\beta_1, \beta_2)$, and that $y$ is adjacent to $b := (\alpha_1, \gamma_2)(\delta_1, \delta_2)$. In particular, if $a = b$, then $d(x, y) \leqslant 2$.

Assume therefore that $a \neq b$, and hence either $\alpha_2 \neq \gamma_2$ or $B \neq D$. As $|a| = |b| = 2$, the subgroup $\langle a, b\rangle$ of $G$ is dihedral, and therefore proper in $G$. Hence if $[a, b] \neq 1$, then $(x, a, b, y)$ is a path in $\Xi(G)$ and $d(x, y) \leqslant 3$. It is easy to check that if $[a, b] = 1$, then either $\gamma_2 = \alpha_2$ and $B \cap D = \varnothing$; or $\{\gamma_2\} \cup D = \{\alpha_2\} \cup B$. As $|\alpha_1^{\langle x\rangle}| \geqslant 3$, we can repeat the argument with $\alpha_2$ replaced by an element of $\alpha_1^{\langle x\rangle} \setminus \{\alpha_1, \alpha_2\}$ to obtain $[a, b] \neq 1$. Thus, in general, $d(x, y) \leqslant 3$.

**Case (b)**: $\langle x\rangle$ and $\langle y\rangle$ each have at least three orbits on $\Omega$. By Proposition 6.2.2, $x$ is adjacent in $\Xi(G)$ to $a := (\alpha_1, \alpha_2, \beta_1)$, and $y$ is adjacent to $b := (\alpha_1, \gamma_2, \delta_1)$. Observe that $t := \operatorname{supp}(a) \cup \operatorname{supp}(b) \leqslant 5$. Since $|\Omega| \geqslant 6$, the subgroup $\langle a, b\rangle$ of $G$ is intransitive, and therefore proper. Hence if $[a, b] \neq 1$, then $(x, a, b, y)$ is a path in $\Xi(G)$, and so $d(x, y) \leqslant 3$. If instead $[a, b] = 1$, then $t = 3$ and $b \in \{a, a^{-1}\}$. Thus in this case, Proposition 5.2.1 yields $d(x, y) \leqslant 2$.

**Case (c)**: Exactly one of $\langle x\rangle$ and $\langle y\rangle$ has exactly two orbits on $\Omega$. We may assume without loss of generality that $\langle x\rangle$ has exactly two orbits on $\Omega$, while $\langle y\rangle$ has at least three. Proposition 6.2.2 shows that $x$ is adjacent in $\Xi(G)$ to $a := (\alpha_1, \alpha_2)(\beta_1, \beta_2)$, and that $y$ is adjacent to $b := (\alpha_1, \gamma_2, \delta_1)$. Note that $[a, b] \neq 1$, that $t := \operatorname{supp}(a) \cup \operatorname{supp}(b) \leqslant 6$, and that $\langle a, b\rangle$ is an intransitive subgroup of $G$ (even if $n = t = 6$). Thus $(x, a, b, y)$ is a path in $\Xi(G)$, and $d(x, y) \leqslant 3$. □

We are now able to prove this section's main result.

*Proof of Theorem 6.2.1.* First, suppose that $G$ is not an alternating or symmetric group. Then the socle of $G$ is isomorphic to $A_6 \cong \mathrm{PSL}(2, 9)$, and so $G$ is isomorphic to $\mathrm{PGL}(2, 9)$, $\mathrm{M}_{10}$ or $\mathrm{P\Gamma L}(2, 9)$. Using the Magma code in `diam_nc_ng` (not to be confused with `comp_nc_ng`), we observe that $\Xi(G)$ is connected with diameter 3 in the first two cases, and diameter 2 in the third.

In the remaining cases, Proposition 6.2.3 shows that $\Xi(G)$ is connected with diameter at most 4. Hence if the finite almost simple group $G$ is not simple, then it follows from Theorem 5.1.5 that $\operatorname{diam}(\Xi(G)) \leqslant 3$.

Assume finally that $G \cong A_n$, with $n$ even. Then no derangement of $G$ is an $n$-cycle, and so each derangement of $G$ generates a cyclic subgroup with at least two orbits on $\Omega$. Thus Propositions 6.2.3 and 6.2.4 yield $\mathrm{diam}(\Xi(G)) \leqslant 3$. □

As stated in the above proof, $\mathrm{diam}(\Xi(G)) = 2$ when $G \cong \mathrm{Aut}(A_6)$. We also determine from the Magma code in `diam_nc_ng` that $\mathrm{diam}(\Xi(G)) = 2$ when $G$ is a simple alternating group of degree at most 10 or an almost simple symmetric group of even degree at most 8, and $\mathrm{diam}(\Xi(G)) = 3$ when $G$ is an almost simple symmetric group of odd degree at most 9, or the soluble group $S_4$. Indeed, it is an open question whether the general upper bound of 4 from Theorem 6.2.1 is tight, and similarly for the upper bound of 3 when $n$ is even (see Question 6.1.5). Note also that if $G$ is a symmetric group of degree less than 4, or an alternating group of degree less than 5, then $G$ is either abelian or minimal non-abelian, and hence $\Xi(G)$ has no edges.

We conclude this section by proving the following theorem, which applies to any non-abelian finite simple group, and which is a key component of the proof of Theorem 6.1.4. Note that our proof uses the classification of finite simple groups.

**Theorem 6.2.5.** *Let $G$ be a non-abelian finite simple group. Then $\Xi(G)$ has no isolated vertices.*

*Proof.* By Theorem 6.2.1, we may assume that $G$ is not an alternating group. Let $x$ be an element of $G$ that lies in a unique maximal subgroup of $G$, say $M$. It suffices by Proposition 5.3.1 to show that $x \notin Z(M)$ for each choice of $x$. In fact, we are done if we can prove that $C_G(x)$ is abelian; in this case, Theorem 2.1.16 yields $C_G(x) < M$, and hence $x \notin Z(M)$.

Suppose first that $G$ is a sporadic simple group. We deduce from [139] and the Atlas [42] that $\langle x \rangle$ has index at most two in $C_G(x)$, and hence $C_G(x)$ is abelian by Proposition 2.1.2.

Assume now that $G$ is a group of Lie type, and let $p$ be its defining characteristic. If $x$ is *semisimple*, i.e., if the prime $p$ does not divide $|x|$, then $C_G(x)$ is abelian [139]. Observe also from Proposition 2.5.15 that if $G$ is a classical group and an element $y \in G$ generates a cyclic subgroup that acts irreducibly on the natural module for $G$, then $y$ is semisimple. It therefore follows from [139] that if $x$ is not semisimple, then either $G \cong \mathrm{PSL}(2, p)$ and $|x| = p$; or $G \cong \mathrm{PSU}(3, p)$ and $x$ is a non-central element of some Sylow $p$-subgroup $P$ of $G$. Using Lemma 5.3.6 in the former case, and the fact that $P \leqslant M$ in the latter, we conclude that $x \notin Z(M)$. □

## 6.3 Sporadic simple groups

Throughout this section, $G$ will denote a (finite) sporadic simple group, or the Tits group ${}^2F_4(2)'$. Here, we show that Theorem 6.1.4 holds for every such group $G$, i.e., we prove the following theorem.

**Theorem 6.3.1.** *Let $G$ be a sporadic simple group or the Tits group. Then $\Xi(G)$ is connected with diameter at most 4. If $G \in \{\mathrm{M}_{11}, \mathrm{M}_{12}, \mathrm{M}_{22}, \mathrm{M}_{23}, \mathrm{J}_1, \mathrm{J}_2, \mathbb{B}\}$, then the exact value of $\mathrm{diam}(\Xi(G))$ is given in Table 6.1.1.*

As in §4.2, all information about $G$ (including its maximal subgroups and the conjugacy classes and centraliser orders of its elements) in this section is from [42, 85, 149], except where specified otherwise. Note in particular that these references list all maximal subgroups of $G$, except possibly when $G$ is the monster group; in this case, the socle of any missing maximal subgroup is a non-abelian simple group [149, p. 65].

We begin by examining the centres of maximal subgroups of $G$.

**Proposition 6.3.2.** *Each maximal subgroup of $G$ has a centre of order at most 2.*

*Proof.* Using the GAP code in `sporadic_cent`, we can show that if $G$ is not the monster group, then the centre of each maximal subgroup $M$ of $G$ contains at most one $M$-conjugacy class of non-identity elements, and hence at most one non-identity element. Thus $|Z(M)| \leqslant 2$. The GAP code in `monster_cent` shows that the same is true when $G$ is the monster group $\mathbb{M}$ and $M$ is a member of the set $\mathcal{M}$ of maximal subgroups of $G$ listed in [149, p. 67]. If instead $G = \mathbb{M}$ and $M \notin \mathcal{M}$, then the socle of $M$ is a non-abelian simple group, and hence $Z(M) = 1$. □

Notice that the above proposition, together with Lemma 5.3.7 (or Lemma 5.3.6), serves as an alternative proof for the fact that $\Xi(G)$ has no isolated vertices.

We will use our next result (and Lemma 6.1.2) to show that $\Xi(G)$ has diameter at most 4 when each maximal subgroup of $G$ has even order.

**Proposition 6.3.3.** *Let $x$ be an element of $G$ of order at least 3, and suppose that $x$ lies in a maximal subgroup of $G$ of even order. Then $x$ is adjacent in $\Xi(G)$ to some involution of $G$.*

*Proof.* For a group $H$, we will write $Q_H$ to denote the subgroup of $H$ generated by all involutions of $H$. By the definition of $\Xi(G)$, it suffices to show that there exists a maximal subgroup of $G$ that contains both $x$ and an involution $y$ that does not centralise $x$. Let $M$ be a maximal subgroup of $G$ of even order, with $x \in M$. Since

$|x| > 2$, Proposition 6.3.2 shows that $x \notin Z(M)$. Hence if $Q_M = M$, then $x$ does not centralise $Q_M$, and so does not centralise every involution of $M$. In general, as conjugation preserves the order of an element, $Q_M$ is a normal subgroup of $M$, and hence $Q_M = M$ whenever $M$ is a simple group. It is also clear that if the number of involutions of $M$ is greater than $|C_M(x)|$, then $M$ contains an involution that does not centralise $x$.

Using the GAP code in `no_invol_neighbs`, we can determine all elements $g \in G$ (up to conjugacy) that do not lie in any simple maximal subgroup, and do not lie in any maximal subgroup whose involutions are more numerous than its elements that centralise $g$. If $g$ is such an element and $|g| \geqslant 3$, then one of the following holds:

(i) $G = \mathrm{J}_1$ and $|g| \in \{7, 19\}$;

(ii) $G = \mathrm{M}_{23}$ and $|g| = 23$;

(iii) $G = \mathrm{Ly}$ and $|g| \in \{37, 67\}$;

(iv) $G = \mathrm{Co}_1$ and $g$ is an element of the conjugacy class of $G$ labelled 3A in [42];

(v) $G = \mathrm{J}_4$ and $|g| \in \{29, 43\}$;

(vi) $G = \mathrm{Fi}'_{24}$ and $|g| = 29$;

(vii) $G = \mathbb{B}$ and $|g| = 47$; or

(viii) $G = \mathbb{M}$ and $|g| = 41$.

In case (iv), $g$ lies in a maximal subgroup $K$ of $G$ of shape $(A_5 \times \mathrm{J}_2){:}2$. As $A_5$ and $\mathrm{J}_2$ are simple, we deduce that $Q_K \cong (Q_{A_5} \times Q_{\mathrm{J}_2}){:}2 \cong (A_5 \times \mathrm{J}_2){:}2 \cong K$. Hence there exists an involution in $K$ that does not commute with $g$. In all other cases, $|g|$ is odd and $C_G(g) = \langle g \rangle$. Thus if $x = g$, then we can choose $y$ to be any involution of $M$. This completes the proof. Note that in cases (ii) and (vii), $g$ lies in no maximal subgroup of $G$ of even order, and so $x$ cannot in fact be equal to $g$. □

Before proving this section's main theorem, we require two additional results about the baby monster group $\mathbb{B}$. Here, and in the proof of the section's main theorem, it may be helpful to refer to Table 4.2.1, which lists the maximal subgroups of $\mathbb{B}$ and their factorised orders. Note also that

$$|\mathbb{B}| = 2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47.$$

The following proposition is relatively elementary, but we will use it twice in the proof of the subsequent result.

**Proposition 6.3.4.** *Suppose that $G$ is the baby monster group, and let $R$ and $M$ be maximal subgroups of $G$ isomorphic to $\mathrm{Fi}_{23}$. Additionally, let $s$ be an element of $R$ of order 23. Then $R \cap M$ contains an element $f$ such that $d(s, f) \leqslant 1$.*

*Proof.* Let $S := \langle s \rangle$. If $S \leqslant M$, then we can set $f = s$. Suppose therefore that $S \not\leqslant M$, so that $S \cap M = 1$. As $|R|\,|M| > |G|$, there exists $f \in (R \cap M) \setminus \{1\}$. The centraliser of $s$ in $R$ is equal to $S$, and since $f \notin S$, we deduce that $s \sim f$. □

**Proposition 6.3.5.** *Suppose that $G$ is the baby monster group, and let $s, y \in G \setminus \{1\}$, with $|s| = 23$. Then $d(s, y) \leqslant 3$.*

*Proof.* The subgroup $S := \langle s \rangle$ of $G$ is a Sylow 23-subgroup, and $s$ lies in a maximal subgroup $R$ isomorphic to $\mathrm{Fi}_{23}$, as well as a maximal subgroup $T$ of shape $2^{1+22}{\cdot}\mathrm{Co}_2$. Any maximal subgroup of $G$ that contains $s$ and is not $G$-conjugate to $R$ or $T$ has shape 47:23. Moreover, $C_R(s) = S$ and (using both Proposition 6.3.2 and the Atlas) $C_G(s) = C_T(s) = Z(T) \times S \cong C_2 \times S$. Using this fact or Proposition 6.3.2, we also deduce that $s$ is not centralised by any maximal subgroup of $G$.

Since $\Xi(G)$ has no isolated vertices by Theorem 6.2.5, Proposition 5.3.1 shows that there exists a maximal subgroup $L$ of $G$ with $y \in L \setminus Z(L)$. Suppose first that $Z(L) > 1$ and $|L|\,|T| > |G|$, so that $L \cap T \neq 1$. We may assume that $L \neq T$, as otherwise $d(s, y) \leqslant 2$ by Corollary 5.2.8. If $L \cap T$ contains a non-identity element of $Z(L) \cup Z(T)$, then, since $Z(L)$ and $Z(T)$ are nontrivial, applying Corollary 2.1.8 to the pairs $(L, T)$ and $(T, L)$ yields $Z(L) \cup Z(T) \subseteq L \cap T$. As $Z(L) \cap Z(T) = 1$ by Proposition 2.1.7, $Z(L) \cup Z(T)$ is a proper subset of $\langle Z(L), Z(T) \rangle$. Therefore, in general, $L \cap T$ contains an element $c \notin Z(L) \cup Z(T)$. Moreover, any such $c$ satisfies $d(c, y) \leqslant 2$ by Corollary 5.2.8. In particular, if $S \leqslant L \cap T$, then we can set $c = s$, and so $d(s, y) \leqslant 2$. Assume therefore that $S \not\leqslant L \cap T$. We claim that $s \sim c$. Indeed, if $s \nsim c$, then $c$ centralises $s$, and hence lies in $(Z(T) \times S) \setminus (Z(T) \cup S)$. Thus $c = zs^i$ for some $i \in \{1, 2, \ldots, 22\}$, where $z$ is the unique involution of $Z(T)$. However, this implies that $\langle c^2 \rangle = \langle s^{2i} \rangle = S$, and so $S \leqslant L \cap T$, a contradiction. Therefore, $s \sim c$ and $d(s, y) \leqslant 3$.

Next, suppose that $Z(L) = 1$, $L \ncong R$, and $|L|\,|R| > |G|$, so that $L \cap R \neq 1$. Since $Z(T) \neq 1$, we observe from Table 4.2.1 that $|S|$ does not divide $|L|$ for any $L$ satisfying the given assumptions, and so $S \cap L = 1$. As $C_R(s) = S$, each $b \in L \cap R$ is adjacent to $s$ in $\Xi(G)$. Moreover, $d(b, y) \leqslant 2$ by Corollary 5.2.8, and so again $d(s, y) \leqslant 3$.

Now, assume that $|y| \notin \{25, 47, 55\}$. Using Table 4.2.1, the GAP code in `sporadic_cent` and `baby_monster`, and the fact that $G$ contains a unique conjugacy class of elements of order 52, we can show that there exists a maximal subgroup $K$

of $G$ containing $y$, such that either $Z(K) > 1$ and $|K|\,|T| > |G|$; or $Z(K) = 1$, $|K|\,|R| > |G|$, and $K \ncong R$. Furthermore, if $y \in Z(K)$, then $y$ is an involution by Proposition 6.3.2, and so Proposition 6.1.1(i) shows that $K \setminus Z(K)$ contains a $G$-conjugate of $y$. It follows that $y$ is a non-central element of some $G$-conjugate of $K$. Thus in general, we can set $L$ to be equal to a $G$-conjugate of $K$, and the previous two paragraphs show that $d(s, y) \leqslant 3$.

We will complete the proof by considering the remaining elements $y$. Note that in each case, Proposition 6.3.2 shows that no maximal subgroup of $G$ centralises $y$.

**Case (a)**: $|y| = 47$. Here, $C_G(y) = \langle y \rangle$, and each maximal subgroup of $G$ containing $y$ has shape 47:23. As $S$ is a Sylow subgroup of $G$, it follows that $y \sim s'$ for some non-identity element $s'$ of a $G$-conjugate $S'$ of $S$. To complete the proof in this case, we will show that $d(s, s') \leqslant 2$.

The element $s'$ lies in a maximal subgroup $M$ of $G$ that is $G$-conjugate to $R$. If $\langle s \rangle = \langle s' \rangle$, then since $s$ is not isolated in $\Xi(G)$, we observe from Proposition 5.2.1 that $d(s, s') = 2$. Otherwise, $[s, s'] \neq 1$, and so if either $s$ or $s'$ lies in $R \cap M$ in this case, then $d(s, s') = 1$. Suppose finally that $s, s' \notin R \cap M$. Then Proposition 6.3.4 shows that $R \cap M$ contains an element $f$ such that $d(s, f) = 1$. By symmetry, $R \cap M$ also contains an element $f'$ such that $d(s', f') = 1$. Hence $R \cap M$ contains an element $t$ that centralises neither $s$ nor $s'$. Thus $s \sim t \sim s'$, and $d(s, s') \leqslant 2$.

**Case (b)**: $|y| \in \{25, 55\}$. The group $G$ contains a unique conjugacy class of elements of order $|y|$. If $|y| = 25$, then since HN contains elements of order 25, we may choose $L$ to be one of the maximal subgroups of shape HN:2. If instead $|y| = 55$, then since HS contains an element of order 11, we may choose $L$ to be one of the maximal subgroups of shape $(5{:}4) \times (\mathrm{HS}{:}2)$. Moreover, HN and HS contain elements of order 35 and 7, respectively, and so in either case, $L$ contains an element of order 35. Additionally, in each case, no involution of $G$ has a centraliser whose order is equal to $|L|$. Applying Proposition 6.3.2, we deduce that $Z(L) = 1$. The remainder of the proof holds whether $|y|$ is equal to 25 or 55.

First suppose that $L \cap R$ contains a non-identity element $g$. Then $g$ does not lie in $S \cup Z(L) \cup Z(R)$, as $|S|$ does not divide $|L|$, and both $Z(L)$ and $Z(R)$ are trivial. Hence Corollary 5.2.8 yields $d(s, g) \leqslant 2$ and $d(g, y) \leqslant 2$. Additionally, $C_G(y) = \langle y \rangle$, and so $C_G(y) \cap C_G(s) = 1$. Thus either $s \sim g$ or $d(g, y) \leqslant 1$ (in fact, $g$ cannot be equal to $y$, as $R$ contains no element of order $|y|$). It follows that $d(s, y) \leqslant 3$.

Suppose finally that $L \cap R = 1$. Each of $G$ and $R$ has a unique conjugacy class of elements of order 35, and $L$ contains elements of order 35 by the second last paragraph. Hence there exists a $G$-conjugate $M$ of $R$ such that $L \cap M$ contains an element $m$ of order 35, and since $C_G(y) = \langle y \rangle$, we observe that $m \sim y$. Additionally,

Proposition 6.3.4 shows that $R \cap M$ contains an element $f$ such that $d(s, f) \leqslant 1$. Note that $f \in M \setminus \langle m \rangle$, since $m \in L$ and $L \cap R = 1$. The subgroup $\langle m \rangle$ of $M$ is equal to $C_M(m)$, and so $f \sim m$. Thus $d(s, y) \leqslant d(s, f) + d(f, m) + d(m, y) \leqslant 3$. □

We are now able to prove this section's main theorem.

*Proof of Theorem 6.3.1.* For $G \in \{\mathrm{M}_{11}, \mathrm{M}_{12}, \mathrm{M}_{22}, \mathrm{M}_{23}, \mathrm{J}_1, \mathrm{J}_2\}$, the Magma code[1] in `diam_nc_ng` yields the specified value for $\mathrm{diam}(\Xi(G))$. Suppose therefore that $G$ is not isomorphic to one of these groups, and let $x$ be a non-identity element of $G$ that lies in a maximal subgroup of even order. If $|x| > 2$, then Proposition 6.3.3 implies that $x$ is adjacent in $\Xi(G)$ to an involution of $G$, and hence there exists a maximal subgroup $L$ of $G$ with $x \in L \setminus Z(L)$ and $|L|$ even. If instead $|x| = 2$, then such $L$ exists by Theorem 6.2.5 and Proposition 5.3.1. If $y$ is another non-identity element of $G$ that lies in a maximal subgroup of even order, then the same holds for $y$, and it follows immediately from Lemma 6.1.2 that $d(x, y) \leqslant 4$. Hence if each maximal subgroup of $G$ has even order, then $\mathrm{diam}(\Xi(G)) \leqslant 4$.

Now, the intersection graph of the baby monster group $\mathbb{B}$ has diameter 5 by Theorem 4.1.4(ii), and so Proposition 5.2.15 implies that $\mathrm{diam}(\Xi(\mathbb{B})) \geqslant 4$. Thus to complete the proof (for all sporadic simple groups), it remains to show that $d(g, h) \leqslant 4$ whenever $g, h \in G \setminus \{1\}$ and $h$ lies in no maximal subgroup of even order. By Theorem 4.2.3, $G$ is isomorphic to Th or to $\mathbb{B}$ (since $\mathrm{M}_{23}$ was accounted for at the start of the proof), and up to conjugacy, $G$ contains a unique maximal subgroup $K$ of odd order.

First assume that $G \cong \mathrm{Th}$. Then $K$ has shape 31:15. Let $m \in K$. If $|m| = 31$, then $m$ lies in a maximal subgroup of $G$ of shape $2^5{\cdot}\mathrm{L}_5(2)$, and otherwise, $|C_G(m)|$ is even. Thus each element of $G$ lies in a maximal subgroup of even order[2], and so the element $h$ does not exist.

Suppose finally that $G \cong \mathbb{B}$. Then $K$ has shape 47:23, and each non-identity element of $K$ has order 23 or 47. Each Sylow 23-subgroup of $G$ has order 23, and 23 divides the order of the maximal subgroup $\mathrm{Fi}_{23}$ of $G$. On the other hand, no element of $K$ of order 47 lies in a maximal subgroup of $G$ of even order. Thus $|h| = 47$. Additionally, $C_G(h) = \langle h \rangle$, and so $s \sim h$ for each element $s \in K$ of order 23. As $d(g, s) \leqslant 3$ by Proposition 6.3.5, we conclude that $d(g, h) \leqslant 4$, as required. □

[1] In each case, we can construct the group $G$ in Magma using the permutation representation of the smallest degree given in [147].

[2] This is why Th was not a listed exception in the proof of Proposition 6.3.3. We also observed a similar fact in the proof of Theorem 4.1.4.

## 6.4 Linear groups

Let $n$ be a positive integer greater than 1, $q$ a prime power, and $V$ the vector space $\mathbb{F}_q^n$. In this section, we prove the linear case of Theorem 6.1.4. In fact, we prove the following more general theorem. Here, and throughout this section, $(n, q)$ denotes an ordered pair, and not the greatest common divisor of $n$ and $q$.

**Theorem 6.4.1.** *Let $G \in \{\mathrm{GL}(n,q), \mathrm{SL}(n,q), \mathrm{PGL}(n,q), \mathrm{PSL}(n,q)\}$, with $(n,q) \neq (2,2)$ and $G \notin \{\mathrm{SL}(2,3), \mathrm{PSL}(2,3)\}$. Then $\Xi(G)$ is connected with diameter at most 4. Moreover, if $G/Z(G) \ncong \mathrm{PSL}(n,q)$, then $\mathrm{diam}(\Xi(G)) \leqslant 3$.*

Hence no almost simple group in this theorem yields a positive answer to the finite case of Question 5.9.6.

Note that if $n = q = 2$, or if $G = \mathrm{PSL}(2,3)$, then $G$ is minimal non-abelian, and thus $\Xi(G)$ has no edges. If instead $G = \mathrm{SL}(2,3)$, then the Magma computations given in `linear_examples` show that the isolated vertices of $\Xi(G)$ are precisely the elements $A \in G \setminus Z(G)$ such that $\langle A \rangle$ acts reducibly on $V$. As $\mathrm{SL}(2,3)$ is soluble and not minimal non-abelian, we deduce from Theorem 5.1.5 that the remaining vertices form a connected component of diameter 2. At the end of this section, we will give exact values, again calculated using Magma, for the diameter of $\Xi(G)$ for certain examples of linear groups $G$ from Theorem 6.4.1.

In order to prove Theorem 6.4.1, we will first prove several results about paths in $\Xi(G)$ between certain elements of $G \setminus Z(G)$ and elements that stabilise one-dimensional subspaces of $V$. Note that the stabiliser $G_X$ of such a subspace $X$ in $G$ contains each scalar matrix in $\mathrm{GL}(n,q)$. As in Definition 3.2.1, $I_m$ denotes the $m \times m$ identity matrix over $\mathbb{F}_q$ for each positive integer $m$, and $E_{i,j}$ denotes the $n \times n$ matrix whose $(i,j)$ entry is equal to 1, and whose remaining entries are equal to 0.

**Proposition 6.4.2.** *Let $G \in \{\mathrm{GL}(n,q), \mathrm{SL}(n,q)\}$, with $(n,q) \neq (2,2)$ and $G \neq \mathrm{SL}(2,3)$. In addition, let $X$ and $Y$ be (possibly equal) one-dimensional subspaces of $V$, with $x \in G_X \setminus Z(G)$ and $y \in G_Y \setminus Z(G)$. Then:*

(i) *no commutator in $G_X$ is a non-identity scalar matrix;*

(ii) *$Z(G)$ is a proper subgroup of $G_X \cap G_Y$;*

(iii) *if $X \neq Y$, then* $C_G(G_X \cap G_Y) = \begin{cases} G_X \cap G_Y, & \text{if } n = 2, \text{ or } n = 3 \text{ and } q = 2; \\ Z(G), & \text{otherwise;} \end{cases}$

(iv) *$C_G(G_X) = Z(G)$;*

(v) *$d_{\Xi(G)}(x,y) \leqslant 2$; and*

(vi) $d_{\Xi(G/Z(G))}(Z(G)x, Z(G)y) \leqslant 2$.

*Proof.*

(i) Up to conjugacy in $G$, the subgroup $G_X$ consists of the matrices in $G$ with a first row of the form $(\lambda_1 \;\; 0 \;\; 0 \;\; \cdots \;\; 0)$, with $\lambda_1 \in \mathbb{F}_q^\times$. Observe that if $T = (t_{ij})_{n\times n}$ and $U = (u_{ij})_{n\times n}$ are matrices in $G_X$, then $(TU)_{11} = t_{11}u_{11}$. It follows that the $(1,1)$ entry of $[T,U]$ is equal to 1, and hence if $[T,U] \in Z(G)$, then $[T,U] = 1$.

(ii) It suffices to prove the result in the case $X \neq Y$. Up to conjugacy by a fixed element of $G$, the subgroup $G_X$ is as in the proof of (i), and $G_Y$ is the set of matrices with a second row of the form $(0 \;\; \lambda_2 \;\; 0 \;\; \cdots \;\; 0)$, with $\lambda_2 \in \mathbb{F}_q^\times$. If $n \geqslant 3$, then $I_n + E_{n,1} \in (G_X \cap G_Y) \setminus Z(G)$. If instead $n = 2$ and $q \geqslant 4$, then let $\omega$ be a primitive element of $\mathbb{F}_q$. As $\omega^{-1} \neq \omega$, the matrix $\begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}$ lies in $(G_X \cap G_Y) \setminus Z(G)$. Finally, if $G = \mathrm{GL}(2,3)$, then $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ lies in $(G_X \cap G_Y) \setminus Z(G)$.

(iii), (iv) Assume that $X \neq Y$, and (conjugating by an element of $G$ if necessary) that $G_X$ and $G_Y$ are as in the proof of (ii). Additionally, let $W = (w_{ij})_{n\times n} \in C_G(G_X \cap G_Y)$. We will first show that $W \in G_X \cap G_Y$ if $n = 2$, or if $n = 3$ and $q = 2$, and that otherwise $W$ is a diagonal matrix (if $n = 2$, then these statements are equivalent). We split this part of the proof into three cases.

**Case (a)**: $n = 2$. As we observed in the proof of (ii), $G_X \cap G_Y$ contains a diagonal matrix $A$ with distinct diagonal entries. By comparing $AW$ and $WA$, which must be equal, we see that $w_{12} = 0 = w_{21}$. Hence $W$ lies in the subgroup of $G$ of diagonal matrices, which is equal to $G_X \cap G_Y$.

**Case (b)**: $n = 3$ and $q > 2$. Let $b \in \mathbb{F}_q^\times \setminus \{1\}$. Then $G_X \cap G_Y$ contains the diagonal matrices $B := \mathrm{diag}(1, b, b^{-1})$ and $B' := \mathrm{diag}(b, 1, b^{-1})$. By comparing $BW$ and $WB$, we see that $w_{12}$, $w_{13}$, $w_{21}$ and $w_{31}$ are all equal to 0, while comparing $B'W$ and $WB'$ yields $w_{23} = 0 = w_{32}$. Therefore, $W$ is a diagonal matrix.

**Case (c)**: $n \geqslant 4$, or $n = 3$ and $q = 2$. Let $r$ and $s$ be distinct integers such that $3 \leqslant r \leqslant n$ and $1 \leqslant s \leqslant n$. Then $G_X \cap G_Y$ contains the matrix $C := I_n + E_{r,s}$. For each index $j \neq s$, we observe that $(CW)_{rj} = w_{rj} + w_{sj}$ and $(WC)_{rj} = w_{rj}$, and so $w_{sj} = 0$. As $s$ can take any value, except for 3 when

$n = 3$, it follows that $w_{ij} = 0$ for all distinct $i$ and $j$, with the extra condition that $i \neq 3$ if $n = 3$. Thus $W \in G_X \cap G_Y$ if $n = 3$ and $q = 2$, and otherwise $W$ is a diagonal matrix.

We have shown that if $n = 2$, or if $n = 3$ and $q = 2$, then $C_G(G_X \cap G_Y) \leqslant G_X \cap G_Y$. It is clear that $G_X \cap G_Y$ is abelian if $n = 2$. In fact, if $n = 3$ and $q = 2$, then each matrix in $G_X \cap G_Y$ has each diagonal entry equal to 1, and so this subgroup is again abelian. Hence $C_G(G_X \cap G_Y) = G_X \cap G_Y$ in both of these cases.

Next, let $D_n := I_n + \sum_{j=1}^{n-1} E_{n,j}$, which lies in $G_X$, and in $G_X \cap G_Y$ if $n > 2$. If $n > 3$, or if $n = 3$ and $q > 2$, then since $W$ is diagonal, we observe for each $j$ that $(D_nW)_{nj} = w_{jj}$ and $(WD_n)_{nj} = w_{nn}$. Thus $w_{jj} = w_{nn}$ for all $j$, and so $W \in Z(G)$, yielding (iii).

Finally, since $C_G(G_X) \leqslant C_G(G_X \cap G_Y)$, we deduce (iv) directly from (iii), unless $n = 2$, or $n = 3$ and $q = 2$. If $n = 2$, then we can compare $D_2W$ and $WD_2$ to show that the diagonal matrix $W$ lies in $Z(G)$. If instead $n = 3$ and $q = 2$, then we let $F := I_3 + E_{2,3} \in G_X$, and compare $FW$ and $WF$, as well as $D_3W$ and $WD_3$, to conclude that the matrix $W \in C_G(G_X \cap G_Y)$ lies in $Z(G)$. This completes the proof of (iv).

(v) If $x, y \in G_X$, then it follows from (iv) that $x, y \in G_X \setminus Z(G_X)$, and so Corollary 5.2.8 implies that $d(x, y) \leqslant 2$. We reach the same conclusion if $x, y \in G_Y$, and so we may assume that $x, y \notin G_X \cap G_Y$. Then $x, y \notin C_G(G_X \cap G_Y)$ by (iii), and hence $C_{G_X \cap G_Y}(x)$ and $C_{G_X \cap G_Y}(y)$ are proper subgroups of $G_X \cap G_Y$. Thus there exists an element $g \in G_X \cap G_Y$ that centralises neither $x$ nor $y$. We conclude that $x \sim g \sim y$ and $d(x, y) \leqslant 2$.

(vi) If $x$ or $y$ lies in $G_X \cap G_Y$, then we may assume that $G_X = G_Y$. By Corollary 5.2.8 in this case, or by the proof of (v) otherwise, there exists a path $(u_1, \ldots, u_j)$ in $\Xi(G)$, where $j \leqslant 3$, $u_1 = x$, $u_j = y$, and $u_2 \in G_X \cap G_Y$. In particular, $[u_i, u_{i+1}] \neq 1$ for each $i \in \{1, \ldots, j-1\}$, and so $[u_i, u_{i+1}] \notin Z(G)$ by (i). Moreover, $\langle u_i, u_{i+1}, Z(G)\rangle$ is a subgroup of either $G_X$ or $G_Y$. Hence Proposition 5.2.11, with $N = Z(G)$, shows that $(Z(G)u_1, \ldots, Z(G)u_j)$ is a walk in $\Xi(G/Z(G))$. □

Note that if $n = q = 2$ or $G = \mathrm{SL}(2, 3)$, then $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in Z(G_X) \setminus Z(G)$, and $G_X \cap G_Y = Z(G)$ whenever $X \neq Y$.

For the following proposition, recall Definition 2.5.1, of companion matrices and hypercompanion matrices.

**Proposition 6.4.3.** *Let $G \in \{\mathrm{GL}(n,q), \mathrm{SL}(n,q)\}$ and $A \in G$. Suppose also that $\langle A \rangle$ acts reducibly on $V$, but does not stabilise any one-dimensional subspace of $V$. Then there exists a one-dimensional subspace $X$ of $V$ and a matrix $B \in G_X$, with $\{A, B\}$ an edge of $\Xi(G)$, and $\{Z(G)A, Z(G)B\}$ an edge of $\Xi(G/Z(G))$.*

*Proof.* The assumption that $\langle A \rangle$ stabilises a proper subspace of $V$ of dimension greater than one implies that $n > 2$. Additionally, Proposition 2.5.4 implies that the characteristic polynomial $\chi_A$ of $A$ is reducible over $\mathbb{F}_q$. However, this polynomial has no linear factor in $\mathbb{F}_q$, as otherwise $A$ would have an eigenvalue in $\mathbb{F}_q$, and $\langle A \rangle$ would stabilise the one-dimensional subspace of $V$ spanned by a corresponding eigenvector. By Theorem 2.5.2 and Corollary 5.2.14, we may assume without loss of generality that $A = (a_{ij})_{n \times n}$ is a direct sum of hypercompanion matrices. In particular, $A$ can be viewed as a block matrix, with each block consisting of at least 2 rows and at least 2 columns, and with the final row of blocks equal to $(0 \quad 0 \quad \cdots \quad 0 \quad R)$, with $R$ a hypercompanion matrix and a proper submatrix of $A$. Note that this holds even if $\chi_A = f^k$ for some irreducible polynomial $f$ and some integer $k > 1$; in this case, $R$ is the companion matrix $C(f)$. Observe also that, in each case, $a_{12} = 1$ and $a_{1j} = 0$ for all $j \neq 2$.

Now, let $B = (b_{ij})_{n \times n}$ be the matrix equal to $I_n + E_{2,1}$. Then $B \in G_X$, where $X$ is the subspace of $V$ spanned by the vector $(1 \quad 0 \quad 0 \quad \cdots \quad 0)$. Additionally, each matrix in $Z(G) \cup \{B\}$ can be viewed as a block matrix, with each block the same size as the corresponding block in $A$, and with the final row of blocks equal to $(0 \quad 0 \quad \cdots \quad 0 \quad S)$ for some nonzero block $S$. This means that every matrix in $\langle A, B, Z(G) \rangle$ has this same structure, and hence $\langle A, B, Z(G) \rangle < G$.

Finally, we show that $A$ and $B$ do not commute, nor do their images in $G/Z(G)$. Suppose for a contradiction that $[A, B] \in Z(\mathrm{GL}(n,q))$, i.e., that $(B^{-1})^A B = kI_n$ for some $k \in \mathbb{F}_q^\times$. Then $(B^{-1})^A = kB^{-1}$. As $B$ has eigenvalue 1 with algebraic multiplicity $n$, so does each of $B^{-1}$ and $(B^{-1})^A$, while $kB^{-1}$ has eigenvalue $k$. Thus $k = 1$, i.e., $[A, B] = 1$. However, $(AB)_{11} = 1$ and $(BA)_{11} = 0$. This is a contradiction, and so $[A, B] \notin Z(\mathrm{GL}(n,q))$. The result now follows from Proposition 5.2.11. □

**Proposition 6.4.4.** *Let $G \in \{\mathrm{GL}(n,q), \mathrm{SL}(n,q)\}$, with $G \neq \mathrm{SL}(2,3)$, and let $A \in G$. Suppose also that $\langle A \rangle$ acts irreducibly on $V$, and that $A^{q-1} \in Z(G)$. Then there exists a one-dimensional subspace $X$ of $V$ and a matrix $B \in G_X$, with $\{A, B\}$ an edge of $\Xi(G)$, and $\{Z(G)A, Z(G)B\}$ an edge of $\Xi(G/Z(G))$.*

*Proof.* Note that $q \neq 2$, as otherwise, $A$ would lie in $Z(G)$, and then $\langle A \rangle$ would act reducibly on $V$. By Lemma 2.5.6 and Corollary 5.2.14, we may assume without loss of generality that $A$ is the companion matrix $C(x^n - b)$, for some $b \in \mathbb{F}_q^\times$ such that $x^n - b$ is irreducible over $\mathbb{F}_q$. In particular, $b \neq 1$. Let $X$ be the subspace of $V$ spanned by the vector $(1 \;\; 0 \;\; 0 \;\; \cdots \;\; 0)$. By Proposition 5.2.11, it suffices to show that there exists a matrix $B \in G_X$ such that $[A, B] \notin Z(G)$ and $\langle A, B, Z(G) \rangle < G$.

First suppose that $n > 2$, and let $B$ be the matrix obtained from $I_n$ by swapping its last two rows, and then multiplying the final row by $-1$. Then $B \in G_X$. Observe that $A^{-1}$ is the matrix obtained from $A^T$ by replacing its $(1, n)$ entry by its multiplicative inverse, while $B^{-1}$ is the matrix obtained from $B$ by multiplying each of its final two rows by $-1$. A simple calculation using these observations shows that the $(1, 1)$ entry of $[A, B]$ is equal to 0, and so $[A, B] \notin Z(G)$.

Next, suppose that $n = 2$ and $q \notin \{3, 5\}$. Let $\omega$ be a primitive element of $\mathbb{F}_q$, and let $B := \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}$. Then $B \in G_X$, and $[A, B] = \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega^{-2} \end{pmatrix}$, which is not in $Z(G)$, as $|\omega|$ does not divide 4.

Suppose now that $n = 2$ and $q = 5$. Then $b \neq -1$, as the binomial $x^2 + 1$ is reducible over $\mathbb{F}_5$. This means that $\det(A) \neq 1$, and so $G = \mathrm{GL}(2, 5)$. Letting $B := \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, we see that $B \in G_X$ and $[A, B] = \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} \notin Z(G)$.

In all of the above cases, $A$, $B$ and the matrices in $Z(G)$ are all monomial. Since the set of monomial matrices in $G$ is a proper subgroup of $G$, it follows that $\langle A, B, Z(G) \rangle < G$.

Finally, suppose that $G = \mathrm{GL}(2, 3)$, so that $b = 2$, and let $B := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. Then $B \in G_X$, and $[A, B] = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \notin Z(G)$. Additionally, $A$, $B$ and the matrices in $Z(G)$ each have determinant 1, and hence $\langle A, B, Z(G) \rangle \leqslant \mathrm{SL}(2, 3) < G$. □

As mentioned at the start of this section, if $G = \mathrm{SL}(2, 3)$, and if $A$ is a matrix in $G$ such that $\langle A \rangle$ acts irreducibly on $V$, then no matrix adjacent to $A$ in $\Xi(G)$ lies in the stabiliser in $G$ of a one-dimensional subspace of $V$.

In the proof of the following proposition, we use the well-known fact that $-1$ is a square in $\mathbb{F}_q$ if and only if $q \not\equiv 3 \pmod 4$.

**Proposition 6.4.5.** *Let $G \in \{\mathrm{GL}(n, q), \mathrm{SL}(n, q)\}$, with $(n, q) \neq (2, 2)$, and let $A \in G$. Suppose that $\langle A \rangle$ acts irreducibly on $V$, and that $A^{q-1} \notin Z(G)$.*

(i) *If either* $n > 2$, $q \not\equiv 3 \pmod 4$, *or* $G = \mathrm{GL}(n,q)$, *then there exists a one-dimensional subspace* $X$ *of* $V$ *and a matrix* $K \in G_X$, *with* $\{A, K\}$ *an edge of* $\Xi(G)$, *and* $\{Z(G)A, Z(G)K\}$ *an edge of* $\Xi(G/Z(G))$.

(ii) *If* $G = \mathrm{SL}(2,q)$, *with* $q \equiv 3 \pmod 4$, *then there exists a matrix* $D \in G$ *such that* $\langle D\rangle$ *acts irreducibly on* $V$, *with* $D^2, D^{q-1} \in Z(G)$, $\{A, D\}$ *an edge of* $\Xi(G)$, *and* $\{Z(G)A, Z(G)D\}$ *an edge of* $\Xi(G/Z(G))$.

*Proof.* Proposition 2.5.15 implies that $A$ lies in a Singer cycle $S$ of $\mathrm{GL}(n,q)$. By Lemma 2.5.13 and Proposition 2.5.14, $Z(\mathrm{GL}(n,q)) < S$, and $N := N_{\mathrm{GL}(n,q)}(S)$ is the group $S{:}\langle B\rangle$ of order $n(q^n-1)$, where $B \in \mathrm{GL}(n,q)$ is similar to the companion matrix $C(x^n-1)$. These results also show that $B$ stabilises a one-dimensional subspace $X$ of $V$ and satisfies $J^B = J^q$ for each $J \in S$. Note also that $C(x^n-1)$, and hence $B$, has determinant 1 if $q$ is even or if $n$ is odd, and determinant $-1$ otherwise. Additionally, $[A,B] = A^{-1}A^B = A^{q-1}$, which is not an element of $Z(G)$ by assumption.

Using [17, §1.6.4], we observe that $|G|/|N| = |G|/(n(q^n-1)) \geqslant r/n$, where $r := q^{n(n-1)/2}$. Notice that $r \geqslant 2^{n(n-1)/2} > n$ when $n \geqslant 3$, and that $r \geqslant 3 > 2$ when $n = 2$ and $q \geqslant 3$. Since $(n,q) \neq (2,2)$, we deduce in general that $r > n$, and hence $|N| < |G|$.

We will now prove (i). By Proposition 5.2.11, it suffices to show that there exists a matrix $K \in G_X$, with $[A,K] \notin Z(G)$ and $\langle A, K, Z(G)\rangle < G$. If either $q$ is even, $n$ is odd, or $G = \mathrm{GL}(n,q)$, then $B \in G_X$, and so $\langle A, B, Z(G)\rangle \leqslant G \cap N < G$. Since $[A,B] \neq Z(G)$, we can set $K = B$.

If instead $G = \mathrm{SL}(2,q)$, with $q \equiv 1 \pmod 4$, then $-1$ has a square root $\alpha$ in $\mathbb{F}_q$. As $\det(B) = -1$, it follows that $\det(\alpha B) = 1$, and hence $\alpha B \in G_X$. Since $[A, \alpha B] = [A,B] \notin Z(G)$, and since $\langle A, \alpha B, Z(G)\rangle \leqslant G \cap \langle A, B, Z(G)\rangle \leqslant G \cap N < G$, we can set $K = \alpha B$.

In the cases remaining in (i), i.e., where $G = \mathrm{SL}(n,q)$, with $n$ even and greater than 2 and $q$ odd, the matrix $B^2$ has determinant 1, and so $B^2 \in G_X$. Additionally, $[A, B^2] = A^{-1}A^{B^2} = A^{q^2-1}$. As $\langle A\rangle$ acts irreducibly on $V$, Proposition 2.5.10 implies that $A^{q^2-1} \notin Z(G)$. Furthermore, $\langle A, B^2, Z(G)\rangle \leqslant G \cap \langle A, B, Z(G)\rangle < G$, and so we can set $K = B^2$.

Next, we prove (ii). Assume that $G = \mathrm{SL}(2,q)$, with $q \equiv 3 \pmod 4$, and let $R$ be a generator for the cyclic group $S$. Then $\det(R)$ is a primitive element of $\mathbb{F}_q$ [20, p. 453], and hence $T := R^{(q-1)/2}$ has determinant $-1$. As $\det(B) = -1$, it follows that $TB \in G \cap N$. Thus $\langle A, TB, Z(G)\rangle \leqslant G \cap N < G$. Using the commutator identity in Proposition 2.1.3(ii) and the fact that $A$ and $T$ lie in the cyclic group

$S$, we conclude that $[A, TB] = [A, B][A, T]^B = [A, B] \notin Z(G)$. It follows from Proposition 5.2.11 that $\{A, TB\}$ and $\{Z(G)A, Z(G)TB\}$ are edges of $\Xi(G)$ and $\Xi(G/Z(G))$, respectively.

Now, as $|B| = 2$, we see that $(TB)^2 = TT^B = T^{q+1}$. Since $|R| = |S| = q^2 - 1$ by Definition 2.5.11, and since $(q-1)/2$ divides $(q^2-1)$, it follows that

$$|T| = |R^{(q-1)/2}| = \frac{q^2-1}{(q-1)/2} = 2(q+1).$$

Similarly, $q+1$ divides $2(q+1)$, and so

$$|(TB)^2| = |T^{q+1}| = \frac{2(q+1)}{q+1} = 2.$$

Hence $(TB)^2$ is the unique involution of $S$, i.e., $-I_2$. As 2 divides $q-1$, it follows that $(TB)^{q-1} \in Z(G)$. Finally, suppose for a contradiction that $TB$ stabilises a proper nonzero (and hence one-dimensional) subspace $U$ of $V$. Then there exists $\lambda \in \mathbb{F}_q^\times$ such that, for all $u \in U$, the element $u^{TB}$ is equal to $\lambda u$ and $u^{(TB)^2} = \lambda^2 u$. However, $v^{(TB)^2} = -v$ for all $v \in V$, and since $q \equiv 3 \pmod 4$, there is no $\lambda \in \mathbb{F}_q^\times$ such that $\lambda^2 = -1$. Therefore, $\langle TB \rangle$ acts irreducibly on $V$, and we can set $D = TB$. □

Note that if $G = \mathrm{SL}(2, q)$, with $q \equiv 3 \pmod 4$, then whether or not the conclusion of Proposition 6.4.5(i) applies may depend on the choice of $A$, as shown by the Magma computations given in `linear_examples`. In particular, when $q = 11$, for a certain choice of $A$, there exists a matrix $K$ that stabilises a one-dimensional subspace of $V$, such that $\{A, K\}$ and $\{Z(G)A, Z(G)K\}$ are edges of $\Xi(G)$ and $\Xi(G/Z(G))$, respectively. On the other hand, another choice of $A$ has no neighbour in $\Xi(G)$ that stabilises a one-dimensional subspace of $V$. However, when $q = 7$, each choice of $A$ has a neighbour $K$ in $\Xi(G)$ that stabilises a one-dimensional subspace of $V$, such that $\{Z(G)A, Z(G)K\}$ is an edge of $\Xi(G/Z(G))$.

Observe that the second paragraph of the above proof does not hold if $n = q = 2$, as here $|G| = n(q^n - 1)$, and so $\langle A, B \rangle = G$. In addition, if $G = \mathrm{SL}(2, 3)$ and $A$ is a matrix in $G$ such that $\langle A \rangle$ acts irreducibly on $V$, then Theorem 2.5.2, Proposition 2.5.4 and the fact that $\det(A) = 1$ imply that $A$ is similar to the matrix $C := \begin{pmatrix} 0 & 1 \\ 2 & a \end{pmatrix}$, for some $a \in \mathbb{F}_3$. In fact, if $a = \pm 1$, then $\langle C \rangle$ stabilises the one-dimensional subspace of $V$ spanned by the vector $(1 \quad a)$, and thus we require $a = 0$. Hence $C^{q-1} = C^2 \in Z(G)$, and it follows that $A^{q-1} \in Z(G)$. Therefore, in this case, the above proposition holds vacuously.

We now prove this section's main theorem.

*Proof of Theorem 6.4.1.* Let $x, y \in G \setminus Z(G)$. By Proposition 6.4.2, there is a path in $\Xi(G)$ of length at most two joining any two elements of $G \setminus Z(G)$ that stabilise a one-dimensional subspace of $V$. Furthermore, Propositions 6.4.3–6.4.5 show that either there exists an element $u \in G \setminus Z(G)$ such that $\langle u \rangle$ stabilises a one-dimensional subspace of $V$ and $d(x, u) \leqslant 1$; or $\langle x \rangle$ acts irreducibly on $V$, $x^{q-1} \notin Z(G)$, and $G/Z(G) \cong \mathrm{PSL}(2, q)$ with $q \equiv 3 \pmod 4$. By the symmetry in $x$ and $y$, it follows that if $G/Z(G)$ is not isomorphic to $\mathrm{PSL}(2, q)$ with $q \equiv 3 \pmod 4$, then $d(x, y) \leqslant 4$, and so $\mathrm{diam}(\Xi(G)) \leqslant 4$. In fact, if $G/Z(G)$ is not simple, i.e., if $G/Z(G) \ncong \mathrm{PSL}(n, q)$ for any $n$ and $q$, then Theorem 5.1.5 shows that $\mathrm{diam}(\Xi(G)) \leqslant 3$.

It remains to show that $d(x, y) \leqslant 4$ when $G/Z(G) \cong \mathrm{PSL}(2, q)$ with $q \equiv 3 \pmod 4$. We first suppose that $G$ itself is simple. By the argument in the previous paragraph, we may assume that $\langle x \rangle$ acts irreducibly on $V$, and that $x^{q-1} \neq 1$. By Proposition 6.4.5, there exists an element $D \in \mathrm{SL}(2, q)$ whose image $h$ in $G$ is adjacent to $x$ in $\Xi(G)$, such that $D^2 \in Z(\mathrm{SL}(2, q))$. Hence $|h| = 2$, and $x$ is a non-central element of a maximal subgroup of $G$ that contains both $x$ and $h$. Thus if $G$ contains a maximal subgroup $M$ of even order such that $y \in M \setminus Z(M)$, then Lemma 6.1.2 yields $d(x, y) \leqslant 4$.

Suppose now that there is no such maximal subgroup $M$ of even order. Then since $y$ is not isolated in $\Xi(G)$ by Theorem 6.2.5 (or by Propositions 6.4.2–6.4.5), we deduce from Proposition 5.3.1 that $y$ is a non-central element of a maximal subgroup $L$ of odd order. It follows from [95, Theorem 2] (see also [17, Table 8.1]) that $L$ is the stabiliser of a one-dimensional subspace of $V$. Now, Proposition 6.4.5 shows that $\langle D \rangle$ acts irreducibly on $V$, and $D^{q-1} \in Z(\mathrm{SL}(2, q))$. Thus we deduce from Proposition 6.4.4 that $h \sim k$ for some $k \in G$ that stabilises a one-dimensional subspace of $V$, and Proposition 6.4.2 yields $d(k, y) \leqslant 2$. Thus $d(x, y) \leqslant d(x, h) + d(h, k) + d(k, y) \leqslant 4$. Therefore, $\mathrm{diam}(\Xi(\mathrm{PSL}(2, q))) \leqslant 4$. We now obtain $\mathrm{diam}(\Xi(\mathrm{SL}(2, q))) \leqslant 4$ by setting $N = Z(\mathrm{SL}(2, q))$ in Corollary 5.2.12. □

Using the Magma code in `diam_nc_ng`, we can determine the diameter of $\Xi(G)$ for sufficiently small almost simple linear groups $G$. We list several examples in Table 6.4.1. Here, given a positive integer $n$ and a prime power $q$, the corresponding *diameter profile* is the 4-tuple $(u, v, w, x)$, where $u := \mathrm{diam}(\Xi(\mathrm{PSL}(n, q)))$, $v := \mathrm{diam}(\Xi(\mathrm{SL}(n, q)))$, $w := \mathrm{diam}(\Xi(\mathrm{PGL}(n, q)))$, and $x := \mathrm{diam}(\Xi(\mathrm{GL}(n, q)))$. Note that if $\Xi(\mathrm{PSL}(n, q))$ has diameter 2, then so does $\Xi(\mathrm{SL}(n, q))$ by Proposition 5.2.5 and Corollary 5.2.12, and so we do not need to check the latter diameter computationally. Similarly, if $\Xi(\mathrm{PGL}(n, q))$ has diameter 2, then so does $\Xi(\mathrm{GL}(n, q))$.

Observe that no graph associated with Table 6.4.1 has a diameter of 4. Indeed,

Table 6.4.1: The diameter profiles of the non-commuting, non-generating graphs of almost simple linear groups for certain pairs $(n, q)$ of positive integers $n$ and prime powers $q$.

| $(n, q)$ | Diameter profile |
|---|---|
| $(2,4), (2,8), (2,16), (2,32), (3,2), (4,2)$ | $(2,2,2,2)$ |
| $(2,5), (2,7), (2,9)$ | $(2,2,3,2)$ |
| $(2,11), (2,13)$ | $(3,3,3,2)$ |
| $(3,3), (3,4)$ | $(3,3,3,3)$ |

it is an open question whether the upper bound of 4 in Theorem 6.4.1 is tight (see Question 6.1.5). We can also show using the aforementioned Magma code that $\Xi(\mathrm{P\Gamma L}(2,4))$ is connected with diameter 3, as is $\Xi(\mathrm{Aut}(\mathrm{PSL}(3,q)))$ when $q \in \{2,3\}$. On the other hand, $\Xi(\mathrm{\Gamma L}(2,4))$, $\Xi(\mathrm{P\Gamma L}(3,4))$ and $\Xi(\mathrm{Aut}(\mathrm{PSL}(3,4)))$ each have diameter 2, as does $\Xi(\mathrm{P\Gamma L}(2,q))$ when $q \in \{8,16,32\}$. Using Theorem 2.4.5, we deduce that all of the almost simple groups mentioned in this paragraph and the last are 2-generated (note that $\mathrm{PGL}(4,2) = \mathrm{PSL}(4,2)$).

## 6.5 Unitary groups

In this section, we prove the unitary case of Theorem 6.1.4. As this is the final case required to prove Theorem 6.1.4(i), this section also contains a formal proof of the latter theorem. We also prove here an analogue of Theorem 6.1.4 for the non-generating graph of a non-abelian finite simple group.

Notice that Corollary 6.1.3 and Theorem 6.2.5 imply Theorem 6.1.4(i) for finite simple unitary groups whose maximal subgroups all have even order. Hence by Theorem 4.2.3, it suffices to consider the simple unitary groups of odd prime dimension.

**Theorem 6.5.1.** *Let $H := \mathrm{PSU}(n,q)$, with $n$ an odd prime and $q$ a prime power such that $H$ is simple.*

(i) *$\Xi(H)$ is connected with diameter at most 5.*

(ii) *Suppose that $n = 7$ and $q = 2$. Then $\Xi(H)$ is connected with diameter 4.*

Question 6.1.7 is open in the unitary case, i.e., we do not know whether there exists a finite simple unitary group $H$ where $\mathrm{diam}(\Xi(H)) = 5$. However, Theorem 6.5.1(ii) shows that there is at least such a group $H$ with $\mathrm{diam}(\Xi(H)) = 4$.

Let $G := \mathrm{SU}(n, q)$, with $n$ an odd prime and $q$ a prime power, and let $V := \mathbb{F}_{q^2}^n$ be the associated unitary space. Additionally, let $Z := Z(G)$, and recall from Proposition 2.3.2 that this is the subgroup of scalar matrices of $G$. By Proposition 2.2.10, we may fix a basis $\{e_1, e_2, \ldots, e_n\}$ for $V$ so that the Gram matrix of the corresponding unitary form is the $n \times n$ identity matrix $I_n$. Then by Lemma 2.2.6, a matrix $A \in \mathrm{SL}(n, q^2)$ lies in $G$ if and only if $A^{-1} = A^{\sigma T}$, where $\sigma$ is the unique involution of $\mathrm{Aut}(\mathbb{F}_{q^2})$. In other words, $A^{\sigma T}$ is the matrix obtained from $A^T$ by replacing each entry with its $q$-th power.

**Proposition 6.5.2.** *Suppose that $n = 3$ and $q > 2$, let $\omega$ be a primitive element of $\mathbb{F}_{q^2}$, and let $\lambda := \omega^{q-1}$. Additionally, for each $i \in \{1, 2, 3\}$, let $B_i$ be the diagonal $3 \times 3$ matrix whose $i$-th diagonal entry is equal to $\lambda^{-2}$ and whose remaining two diagonal entries are equal to $\lambda$, and let $A_1$ and $A_2$ be $G$-conjugates of $B_1$.*

(i) *$B_i \in G \setminus Z$ for each $i$.*

(ii) *$B_2$ and $B_3$ are each conjugate to $B_1$ in $G$.*

(iii) *$\langle A_1, A_2 \rangle$ is a proper subgroup of $G$ that stabilises a one-dimensional subspace of $V$.*

(iv) *If $A_1$ is not adjacent in $\Xi(G)$ to any $B_i$, then $A_1$ is a diagonal matrix.*

*Proof.* It is clear that $\det(B_i) = 1$ for each $i$. Additionally, $\lambda^q = \lambda^{-1}$. Thus $B_i^{-1} = B_i^{\sigma T}$, and so $B_i \in G$. Moreover, since $|\lambda| = q + 1 > 3$, we deduce that $\lambda \neq \lambda^{-2}$. Hence $B_i \notin Z$, and (i) follows. The matrices $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ lie in $G$ and conjugate $B_1$ to $B_2$ and $B_3$, respectively, hence (ii).

To prove (iii), we may assume without loss of generality that $A_1 = B_1$. Let $F$ be an element of $G$ such that $A_2 = B_1^F$, and note that $B_1$ acts as the scalar $\lambda$ on the subspace $E := \langle e_2, e_3 \rangle$ of $V$. Similarly, $A_2$ acts as the scalar $\lambda$ on $E^F = \langle e_2^F, e_3^F \rangle$. Hence $\langle B_1, A_2 \rangle$ stabilises each subspace of $E \cap E^F$, which has positive dimension since $\dim(V) = 3$. The group $G$ acts irreducibly on $V$ [89, Proposition 2.10.6], and thus properly contains $\langle B_1, A_2 \rangle$. This completes the proof of (iii).

Finally, (ii) and (iii) show that if a $G$-conjugate of $B_1$ is not adjacent in $\Xi(G)$ to any $B_i$, then that $G$-conjugate lies in $C_G(\{B_1, B_2, B_3\})$. Notice that $C_G(B_1)$ is the subgroup of $G$ consisting of direct sums $X \oplus Y$, where $X$ is a $1 \times 1$ matrix and $Y$ is a $2 \times 2$ matrix. By considering the centralisers of $B_2$ and $B_3$ in $G$ similarly, we deduce that $C_G(\{B_1, B_2, B_3\})$ is the subgroup of $G$ of diagonal matrices. Therefore, we obtain (iv). □

Recall Definition 2.5.1, of a companion matrix.

**Lemma 6.5.3.** *Suppose that $n$ is an odd prime.*

(i) *The companion matrix $C(x^n - 1)$ is an element of $G$.*

(ii) *Let $R$ be an element of $G$ that is conjugate to $C(x^n - 1)$. Then $ZR$ is adjacent in $\Xi(G/Z)$ to an involution of $G/Z$.*

(iii) *Let $R$ and $S$ be elements of $G$ that are conjugate to the companion matrix $C(x^n - 1)$. Then $d_{\Xi(G/Z)}(ZR, ZS)$ is at most 3 if $n = 3$, or at most 2 otherwise.*

*Proof.* Throughout this proof, we write "$\sim$" as shorthand for "$\sim_{\Xi(G/Z)}$".

(i) Notice that $C(x^n - 1)^{-1} = C(x^n - 1)^{\sigma T}$, and $\det(C(x^n - 1)) = 1$ since $n$ is odd. Hence $C(x^n - 1) \in G$.

(ii) By (i) and Corollary 5.2.14, we may assume without loss of generality that $R = C(x^n - 1)$. If $q$ is odd, then let $A$ be the matrix obtained from $I_n$ by multiplying its final two rows by $-1$, and otherwise let $A$ be the matrix obtained from $I_n$ by swapping its last two rows. Then $\det(A) = 1$ and $A^{-1} = A = A^{\sigma T}$. If $q$ is odd, then the $(1, 1)$ entry of $[R, A] = R^T ARA$ is equal to $-1$, while its $(n, n)$ entry is equal to 1. If instead $q$ is even, then the $(1, 1)$ entry of $[R, A]$ is equal to 0. Hence, in either case, $[R, A] \notin Z$. Moreover, $R$, $A$ and all elements of $Z$ are monomial matrices, and so $\langle R, A, Z\rangle$ lies in the proper subgroup of $G$ consisting of monomial matrices. Thus Proposition 5.2.11, with $N = Z$, shows that $ZR \sim ZA$. As $A$ is an involution, so is $ZA$.

(iii) We may assume that $d_{\Xi(G/Z)}(ZR, ZS) > 1$, and, as above, that $R = C(x^n - 1)$. Then $R$ stabilises the subspace $X$ of $V$ spanned by the all-ones vector. Let $F$ be an element of $G$ such that $S = R^F$, and let $L := G_X$, so that $R \in L$ and $S \in L^F$. Additionally, let $L_0 := G_{\langle e_1\rangle}$. Then Proposition 2.5.3 shows that $C_{L_0}(R) = Z$, and thus $C_{L_0^F}(S) = Z$. It also follows from Proposition 6.4.2(i) that if $A \in L$ satisfies $[R, A] \in Z$, then $[R, A] = 1$. As $Z \leqslant L$, we deduce from Proposition 5.2.11 that if $[R, B] \neq 1$ for some $B \in L$, then $ZR \sim ZB$. Similarly, if $[S, D] \neq 1$ for some $D \in L^F$, then $ZS \sim ZD$. We split the remainder of the proof into three cases.

**Case (a)**: $n \geqslant 7$, or $n = 5$ and $q \neq 4$. By Theorem 3.5.1(i), the pointwise stabiliser in $G$ of $\{X, X^F, \langle e_1\rangle, \langle e_1\rangle^F\}$, which is equal to $L \cap L^F \cap L_0 \cap L_0^F$, contains a non-scalar matrix $D$. As $D$ lies in $(L_0 \cap L_0^F) \setminus Z$, it centralises

neither $R$ nor $S$, by the previous paragraph. Additionally, $D \in L \cap L^F$, and so the previous paragraph yields $ZR \sim ZD \sim ZS$.

**Case (b)**: $n = 5$ and $q = 4$. Let $v \in X$ be the all-ones vector. The unitary form on $V$ maps $(v, v)$ to $1 \in \mathbb{F}_q$, and so $X$ is non-degenerate. By [17, Table 2.3], $|L| = 5|\mathrm{SU}(4, 4)|$. Using this fact and the Magma code in `su54`, we can show that $|L \cap L^F|$ is even (for any $F \in G$), while $|C_G(R)| = 625$ (and hence $|C_G(S)| = 625$). It follows from the second last paragraph that if $D$ is any involution of $L \cap L^F$, then $ZR \sim ZD \sim ZS$.

**Case (c)**: $n = 3$. For each $i \in \{1, 2, 3\}$, let $B_i$ be the element of $G \setminus Z$ from Proposition 6.5.2. Then $B_i \in L_0 \setminus Z$, and so $[R, B_i] \notin Z$. Additionally, $\langle Z, R, B_i\rangle$ lies in the proper subgroup of $G$ consisting of monomial matrices. It therefore follows from Proposition 5.2.11 that $ZR \sim ZB_i$. Similarly, $ZS \sim ZB_i^F$. Recall also from Proposition 6.5.2(ii)–(iii) that $\langle B_i, B_1^F\rangle$ stabilises a one-dimensional subspace of $V$. Hence, as in the third last paragraph, if $B_1^F$ is adjacent in $\Xi(G)$ to $B_i$ for some $i$, then $ZB_i \sim ZB_1^F$, and thus $ZR \sim ZB_i \sim ZB_1^F \sim ZS$. Otherwise, the element $B_1^F$ of $G \setminus Z$ is diagonal by Proposition 6.5.2(iv), and so replacing $B_i$ with $B_1^F$ in the above argument yields $ZR \sim ZB_1^F$. Therefore, $ZR \sim ZB_1^F \sim ZS$. □

Next, we prove this section's main theorem.

*Proof of Theorem 6.5.1.* Throughout this proof, we write "$\sim$" as shorthand for "$\sim_{\Xi(H)}$", and similarly $d(\cdot, \cdot) := d_H(\cdot, \cdot)$.

(i) Let $x$ and $y$ be vertices of $\Xi(H)$, which Theorem 6.2.5 shows are not isolated, and recall that $G = \mathrm{SU}(n, q)$ and $Z = Z(G)$. We will show that $d(x, y) \leqslant 5$. By Proposition 5.3.1, each of $x$ and $y$ is non-central in some maximal subgroup of $H$. Furthermore, using Lemma 6.1.2, we may assume that each maximal subgroup of $H$ that contains $x$, but does not centralise $x$, has odd order. Then [95, Theorem 2] shows that $x$ lies in a maximal subgroup $N_G(S)/Z$ of $H$, where $S$ is a Singer cycle of $G$, i.e., the intersection of $G$ and a Singer cycle of $\mathrm{GL}(n, q^2)$ (see [10, §1] and [78, §5]). Recall from Lemma 6.5.3(i) that $C(x^n - 1) \in G$, and from Lemma 2.5.13 that this companion matrix can be viewed as a field automorphism of $\mathbb{F}_{q^{2n}}$ of order $n$. Hence it follows from [78, p. 512] that $N_G(S) = S{:}\langle C\rangle$ for some conjugate $C$ of $C(x^n - 1)$.

Now, $ZC$ is adjacent in $\Xi(H)$ to some involution $r \in H$ by Lemma 6.5.3(ii), and in particular $ZC, r \in L \setminus Z(L)$ for some maximal subgroup $L$ of $H$ of even order. As $|C| = n$ is prime, each non-identity element of $\langle ZC\rangle$ lies in

$L \setminus Z(L)$. Since $Z \leqslant S$ by Proposition 2.5.14, it follows that $x = ZAC^i$ for some $A \in S \setminus Z$ and some $i \in \{0, 1, \ldots, n-1\}$.

Similarly to the proof of Proposition 6.4.5 (except that we are now working over $\mathbb{F}_{q^2}$ instead of $\mathbb{F}_q$), we can use Proposition 2.5.14 to observe that $[A, C] = A^{-1}A^C = A^{-1}A^{q^2} = A^{q^2-1}$. Thus $[A, C] \notin Z$ by Corollary 2.5.17. Moreover, $\langle A, C, Z\rangle \leqslant N_G(S) < G$. Therefore, Proposition 5.2.11, with $N = Z$, yields $ZA \sim ZC$. We now conclude from Proposition 5.2.2 that $ZAC^i \sim ZC$ for all $i$. In particular, $x \sim ZC$.

Suppose now that $H$ contains a maximal subgroup $M$ of even order such that $y \in M \setminus Z(M)$. Since the elements $ZC$ and $r$ of $L \setminus Z(L)$ are adjacent vertices of $\Xi(H)$ with $|r| = 2$, we deduce from Lemma 6.1.2 that $d(ZC, y) \leqslant 4$, and so $d(x, y) \leqslant 5$. If instead there is no such $M$, then Theorem 4.2.3 implies that $y$ lies in an $H$-conjugate of $N_G(S)/Z$. We can therefore repeat the argument from the previous paragraph to show that $y \sim ZD$ for some $G$-conjugate $D$ of $C$. Since $d(ZC, ZD) \leqslant 3$ by Lemma 6.5.3(iii), we deduce that $d(x, y) \leqslant d(x, ZC) + d(ZC, ZD) + d(ZD, y) = 5$.

(ii) In this proof, all information about $H = \mathrm{PSU}(7, 2)$ is determined using the Magma code in `psu72`, except where stated otherwise. Since the intersection graph of $H$ has diameter 5 by Proposition 4.1.5, it follows from Proposition 5.2.15 that $\mathrm{diam}(\Xi(H)) \geqslant 4$.

Now, let $x, y \in H \setminus \{1\}$. It remains to show that $d(x, y) \leqslant 4$. If $x$ lies in a maximal subgroup of $H$ of odd order, then $|x| \in \{7, 43\}$, and if $x$ does not lie in a maximal subgroup of even order, then $|x| = 43$. Suppose for now that $|x|, |y| \neq 43$. By (i) and Proposition 5.3.1, $x$ is a non-central element of a maximal subgroup $M$ of $H$. Since the Sylow 7-subgroups of $H$ have order 7 and are non-central subgroups of maximal subgroups of even order, we may assume that $|M|$ is even. For any such $M$, the centraliser in $M$ of the subgroup generated by all involutions of $M$ is equal to $Z(M)$. Hence there exists an involution $a \in M$ such that $x \sim a$. A similar statement holds for $y$, and so Lemma 6.1.2 implies that $d(x, y) \leqslant 4$.

Assume from now on that $|x| = 43$, so that $x$ lies in no maximal subgroup of $G$ of even order. As in the proof of (i), $x$ is adjacent in $\Xi(H)$ to the image $t$ in $H$ of some $G$-conjugate of $C(x^7 - 1)$. Since $n > 3$, it follows from Lemma 6.5.3(iii) that if $|y| = 43$, then $d(x, y) \leqslant 4$.

Suppose finally that $|y| \neq 43$, and let $T$ be the subgroup $\langle t\rangle$ of $H$ of order 7. Then there exist maximal subgroups $K$ and $L$ of $H$ such that $y \in K \setminus Z(K)$,

$t \in L \setminus Z(L)$, and either:

(I) $|K \cap L| > |C_G(t)| + |Z(K)|$; or

(II) $Z(K) = 1$, $C_L(t) = T$, $T \cap K = 1$, and $|K|\,|L| > |H|$.

In case (I), there exists an element $f \in K \cap L$ that centralises neither $t$ nor $K$. Hence $t \sim f$, and $d(f, y) \leqslant 2$ by Corollary 5.2.8, yielding $d(t, y) \leqslant 3$. In case (II), since $|K|\,|L| > |H|$, we deduce that $K \cap L > 1$. We also observe that $t$ is adjacent in $\Xi(H)$ to each non-identity element $r$ of $K \cap L$. As $d(r, y) \leqslant 2$ by Corollary 5.2.8, we again obtain $d(t, y) \leqslant 3$. We conclude in general that $d(x, y) \leqslant d(x, t) + d(t, y) \leqslant 4$. □

Using the Magma code in `diam_nc_ng`, we observe that the non-commuting, non-generating graphs of the groups $\mathrm{PSU}(3, 3)$, $\mathrm{PSU}(3, 4)$ and $\mathrm{PSU}(4, 2)$ are connected with diameters 2, 2 and 3, respectively.

We are now able to prove the first part of Theorem 6.1.4, which states that, for an arbitrary non-abelian finite simple group $G$, the graph $\Xi(G)$ has diameter at most 5. The proof's argument was summarised below the statement of this theorem, but here we give a formal proof.

*Proof of Theorem 6.1.4(i).* By Theorem 6.2.5, $\Xi(G)$ has no isolated vertices. Thus if every maximal subgroup of $G$ has even order, then Corollary 6.1.3 yields the result. We may therefore assume that $G$ has a maximal subgroup of odd order. By Theorem 4.2.3, $G$ is either an alternating group, a sporadic group, a linear group of prime dimension, or a unitary group of odd prime dimension. Theorems 6.2.1, 6.3.1, 6.4.1 and 6.5.1 show that $\mathrm{diam}(\Xi(G)) \leqslant 5$ in each case. □

Finally, we prove an analogue of Theorem 6.1.4 for the non-generating graph of a non-abelian finite simple group, as in Definition 5.1.2.

**Theorem 6.5.4.** *Let $\overline{\Gamma}(G)$ be the non-generating graph of a non-abelian finite simple group $G$. Then $\overline{\Gamma}(G)$ is connected, with diameter at most 3 if every maximal subgroup of $G$ has even order, or diameter at most 4 otherwise. Furthermore, if $G$ is the baby monster group or $\mathrm{PSU}(7, 2)$, then $\mathrm{diam}(\overline{\Gamma}(G)) = 4$.*

*Proof.* Let $x$ and $y$ be non-identity elements of $G$, and let $M_1$ and $M_2$ be maximal subgroups of $G$ containing $x$ and $y$, respectively. Suppose first that $|M_1|$ and $|M_2|$ are both even. Then there exist involutions $a \in M_1$ and $b \in M_2$, and $\langle a, b\rangle$ is a (proper) dihedral subgroup of $G$. Therefore, $(x, a, b, y)$ contains a path from $x$ to $y$ in $\overline{\Gamma}(G)$, and so $d(x, y) \leqslant 3$. Thus if every maximal subgroup of $G$ has even order, then we are done.

Suppose now that $|M_1|$ is odd. We deduce from Theorems 4.2.3 and 6.1.4 that if $G$ is not a unitary group of odd prime dimension, then $\mathrm{diam}(\Xi(G)) \leqslant 4$. As $\Xi(G)$ is a spanning subgraph of $\overline{\Gamma}(G)$, it follows in this case that $\mathrm{diam}(\overline{\Gamma}(G)) \leqslant 4$.

Assume therefore that $G = \mathrm{PSU}(n, q)$, with $n$ an odd prime and $q$ a prime power. As in the proof of Theorem 6.5.1, we can use [95, Theorem 2], Lemma 2.5.13 and [78, p. 512] to show that $M_1$ is the image in $G$ of the subgroup $S{:}\langle C\rangle$ of $\mathrm{SU}(n, q)$, where $S$ is a Singer cycle of $\mathrm{SU}(n, q)$ and $C$ is a conjugate of the companion matrix $C(x^n - 1)$. Furthermore, Lemma 6.5.3(ii) shows that the image $c$ of $C$ in $G$ is adjacent in $\Xi(G)$ to an involution $a \in G$. Hence $c$ and $a$ are adjacent in $\overline{\Gamma}(G)$.

Now, if $|M_2|$ is even, then $M_2$ again contains an involution $b$, and $(x, c, a, b, y)$ contains a path from $x$ to $y$ in $\overline{\Gamma}(G)$, yielding $d(x, y) \leqslant 4$. Otherwise, it follows from the previous paragraph and Theorem 4.2.3 that $y$ is adjacent in $\overline{\Gamma}(G)$ to a $G$-conjugate $c'$ of $c$. Moreover, Lemma 2.5.13 shows that $c$ and $c'$ stabilise one-dimensional subspaces $X$ and $X'$, respectively, of $\mathbb{F}_{q^2}^n$. Since $q \neq 2$ when $n = 3$, we deduce from Theorem 3.5.1 that $G_X \cap G_{X'}$ contains a non-identity element $t$. Hence $(x, c, t, c', y)$ contains a path from $x$ to $y$ in $\overline{\Gamma}(G)$, again yielding $d(x, y) \leqslant 4$. Therefore, $\mathrm{diam}(\overline{\Gamma}(G)) \leqslant 4$.

Finally, suppose that $G$ is the baby monster group or $\mathrm{PSU}(7, 2)$. We recall from Theorem 4.1.4(ii) and Proposition 4.1.5 that the intersection graph of $G$ is connected with diameter 5. Hence Proposition 5.2.15 yields $\mathrm{diam}(\overline{\Gamma}(G)) \geqslant 4$. By the previous paragraphs, we conclude that $\mathrm{diam}(\overline{\Gamma}(G)) = 4$. □

As we noted in §6.1, a version of the above theorem serves as part of the proof of the main theorem of [104].

## 6.6 Exceptional groups of Lie type

Let $q$ be a prime power. In this section, we complete the proof of Theorem 6.1.4(iii) by proving the following result about certain families of finite simple exceptional groups of Lie type.

**Theorem 6.6.1.** *Let $G$ be a finite simple group. If $G \cong \mathrm{Sz}(q)$, or if $q$ is odd and $G \in \{G_2(q), {}^2G_2(q), {}^3D_4(q), F_4(q), E_8(q)\}$, then $\Xi(G)$ is connected with diameter at most 4.*

Throughout this section, for a group $H$, we will write $Q_H$ to denote the subgroup of $H$ generated by its involutions. Note that $Q_H$ is a characteristic subgroup of $H$, as automorphisms preserve the orders of elements. In order to prove Theorem 6.6.1,

we will study $Q_H$ and its centraliser in $H$, for certain groups $H$. We require the following definition.

**Definition 6.6.2** ([92, Definition 2.2.6])**.** Let $H$ and $K$ be groups, such that there exists an isomorphism $\theta : Z(H) \to Z(K)$. Then the *central product* of $H$ and $K$ (associated with $\theta$) is the group $H \circ K := (H \times K)/\{(z, (z^{-1})\theta) \mid z \in Z(H)\}$.

In general, the isomorphism type of $H \circ K$ may depend on the isomorphism $\theta$. However, for all central products $H \circ K$ below, $|Z(H)| = |Z(K)| \leqslant 2$, and so $\theta$ is unique.

**Proposition 6.6.3.** *Let $S := \mathrm{SL}(2, q)$, and let $H$ be a quasisimple group containing a subgroup $K$, such that $K \cong S$ and $Z(H) = Z(K)$. Additionally, let $R$ be the central product $S \circ H$, and let $\pi$ be the natural epimorphism $S \times H \to R$. If $Q_R \neq R$, then $q = 3$, $Q_R$ is a maximal subgroup of $R$ that contains $(H)\pi$, and $C_R(Q_R) = Z(R)$.*

*Proof.* Let $z_1$ and $z_2$ be generators for $Z(S)$ and $Z(H) = Z(K)$, respectively, with $z_1 = 1_S$ and $z_2 = 1_H$ if these centres are trivial. Then $\ker \pi = \langle (z_1, z_2) \rangle \leqslant S \times K$, and $\tilde{S} := (S)\pi$ and $\tilde{K} := (K)\pi$ are normal subgroups of $J := S \circ K = (S \times K)\pi$. Similarly, $\tilde{S}$ and $\tilde{H} := (H)\pi$ are normal subgroups of $R$. As $\ker \pi$ has trivial intersection with each of $S$, $K$ and $H$, these three subgroups are isomorphic to $\tilde{S}$, $\tilde{K}$ and $\tilde{H}$, respectively. Additionally, $[\tilde{H}, \tilde{S}] = ([H, S])\pi = 1$, and $\tilde{H}\tilde{S} = R$. Notice that the centres of $R$, $J$, $\tilde{H}$, $\tilde{S}$ and $\tilde{K}$ all coincide, and that this common centre $\mathcal{Z}$ has order $(2, q-1)$ and is equal to $\tilde{H} \cap \tilde{S}$.

Now, [17, Lemma 1.12.3] and its proof show that $J \cong \Omega^+(4, q)$. Suppose first that $q \neq 3$. Then [91, Theorem 8.5] implies that $Q_J = J$. Additionally, since $\mathcal{Z} < \tilde{K} \leqslant \tilde{H}$, we deduce from Proposition 2.4.2 that no proper normal subgroup of the quasisimple group $\tilde{H}$ contains $\tilde{K}$, and hence (by repeated application of the Correspondence Theorem) no proper normal subgroup of $R$ contains $J$. Since the normal subgroup $Q_R$ of $R$ contains $Q_J = J$, we obtain $Q_R = R$.

Suppose from now on that $q = 3$. We calculate that $\tilde{S} \cap Q_J$ is a maximal subgroup of $\tilde{S}$, and that $\tilde{K} \cap Q_J > \mathcal{Z}$. As the normal subgroup $\tilde{H} \cap Q_R$ of $\tilde{H}$ contains $\tilde{K} \cap Q_J$, it follows from Proposition 2.4.2 that $\tilde{H} \leqslant Q_R$. Since $R = \tilde{H}\tilde{S}$, Lemma 2.1.1 now yields $Q_R = \tilde{H}\tilde{S} \cap Q_R = \tilde{H}(\tilde{S} \cap Q_R)$.

If $\tilde{S} \cap Q_R = \tilde{S}$, then $Q_R = R$. We will therefore assume that $\tilde{S} \cap Q_R < \tilde{S}$. Then $\tilde{S} \cap Q_R$ is equal to the maximal subgroup $\tilde{S} \cap Q_J$ of $\tilde{S}$, and $Q_R = \tilde{H}(\tilde{S} \cap Q_J)$, which is maximal in $\tilde{H}\tilde{S} = R$. Since $[\tilde{H}, \tilde{S}] = 1$, we observe that

$$\mathcal{Z} \leqslant C_R(Q_R) = C_{\tilde{H}\tilde{S}}(\tilde{H}(\tilde{S} \cap Q_J)) \leqslant Z(\tilde{H})C_{\tilde{S}}(\tilde{S} \cap Q_J).$$

We calculate that $C_{\tilde{S}}(\tilde{S} \cap Q_J)$ is equal to $\mathcal{Z} = Z(\tilde{H}) = Z(R)$, and hence so is $C_R(Q_R)$. □

The following lemma shows that, with certain exceptions, all finite quasisimple groups are generated by their involutions.

**Proposition 6.6.4.** *Let $H$ be a finite quasisimple group. If $|Z(H)| = 2$, then assume that $H/Z(H)$ is not isomorphic to $A_7$, or to $\mathrm{PSL}(2,q)$ for any odd $q$. Then $Q_H = H$.*

*Proof.* As $H$ is quasisimple, each of its proper normal subgroups lies in $Z(H)$ by Proposition 2.4.2. Additionally, $Q_H \trianglelefteq H$, and so it suffices to show that there exists an involution $a \in H \setminus Z(H)$. Since $|H|$ is even by the Feit-Thompson Theorem, the involution $a$ certainly exists if $|Z(H)|$ is odd. If instead $|Z(H)|$ is even, then the main theorem of [64] yields the existence of $a$. □

**Lemma 6.6.5.** *Suppose that $q$ is odd, let $a$ be an involution of a simple group $G \in \{G_2(q), {}^2G_2(q), {}^3D_4(q), F_4(q), E_8(q)\}$, and let $Y := C_G(a)$. Then $C_Y(Q_Y) = Z(Y) = \langle a \rangle$.*

*Proof.* We observe from Theorem 4.5.1 and Table 4.5.1 of [62], as well as the explanation of the table, that $Z(Y) = \langle a \rangle$, and either:

(a) $G \cong {}^2G_2(q)$ and $Y \cong C_2 \times \mathrm{PSL}(2,q)$;

(b) $G \cong F_4(q)$ and $Y \cong \mathrm{Spin}(9,q)$;

(c) $G \cong E_8(q)$ and $Y$ has shape $J{:}2$, where $J = (\mathrm{Spin}^+(16,q)/A)$, and $A$ is a central subgroup of $\mathrm{Spin}^+(16,q)$ of order 2; or

(d) $Y = R{:}A$, with $|A| = 2$ and $R \cong \mathrm{SL}(2,q) \circ H$, where $(G,H)$ lies in the set

$$\{(G_2(q), \mathrm{SL}(2,q)), ({}^3D_4(q), \mathrm{SL}(2,q^3)), (F_4(q), \mathrm{Sp}(6,q)), (E_8(q), E_7(q)_{\mathrm{sc}})\}.$$

Additionally, $Z(Y) = Z(R)$, and $A$ induces an outer automorphism on the image of $H$ under the natural epimorphism $\pi : \mathrm{SL}(2,q) \times H \to R$.

Here, $\mathrm{Spin}(9,q)$, $\mathrm{Spin}^+(16,q)$ and $E_7(q)_{\mathrm{sc}}$ are quasisimple groups with centres isomorphic to $C_2$, $C_2^2$ and $C_2$, respectively, and with central quotients isomorphic to $\Omega_9(q)$, $\mathrm{P}\Omega^+(16,q)$ and $E_7(q)$, respectively [109, Table 22.1, Corollary 24.13, Theorem 24.17]. We will divide the remainder of the proof into the four cases above. In each case, since $Z(Y) = \langle a \rangle$, it remains to show that $C_Y(Q_Y) = Z(Y)$.

**Case (a)**. As $q \geqslant 27$ (see §2.4), the group $\mathrm{PSL}(2,q)$ is simple. It is clear that $Q_Y = Y$, and hence $C_Y(Q_Y) = Z(Y)$.

**Case (b)**. Proposition 6.6.4 (or [4, Theorem 1.1]) yields $Q_Y = Y$, and so $C_Y(Q_Y) = Z(Y)$.

**Case (c)**. Since $\mathrm{Spin}^+(16,q)$ is quasisimple and its central quotient is isomorphic to $\mathrm{P\Omega}^+(16,q)$, the same is true for $J$. Proposition 6.6.4 therefore shows that $J = Q_J$, and so $Q_Y = Q_J{:}2 = Y$. Thus $C_Y(Q_Y) = Z(Y)$.

**Case (d)**. If $G \cong G_2(3)$, then $Y \cong \mathrm{SO}^+(4,3)$ [148, p. 125]. We calculate $Q_Y = Y$, and so $C_Y(Q_Y) = Z(Y)$.

Suppose therefore that $G \ncong G_2(3)$. Notice that $Q_Y$ contains $\langle Q_R, A\rangle$, which is equal to $Q_R{:}A$ since $Q_R$ is a characteristic subgroup of $R$. In particular, if $Q_R = R$, then $Q_Y = Y$ and $C_Y(Q_Y) = Z(Y)$. Thus we may assume that $Q_R < R$ and $Q_Y < Y$.

Observe from Proposition 2.4.3 that $H \ncong \mathrm{SL}(2,3)$ is quasisimple. In order to apply Proposition 6.6.3, we will show that $H$ contains a subgroup $K$ such that $K \cong \mathrm{SL}(2,q)$ and $Z(H) = Z(K)$. Observe that this holds if $H$ contains a subgroup $L$ such that $Z(H) = Z(L)$ and $L \cong \mathrm{SL}(2,q^i)$ for some positive integer $i$. Hence this is the case if $H \in \{\mathrm{SL}(2,q), \mathrm{SL}(2,q^3)\}$. If instead $H = E_7(q)_{\mathrm{sc}}$, then $H$ contains a subgroup $L$ isomorphic to $\mathrm{SL}(2,q^7)$, with $Z(H) = Z(L)$ [74, p. 927]. Finally, if $H = \mathrm{Sp}(6,q)$, then let $V_1$, $V_2$ and $V_3$ be non-degenerate two-dimensional subspaces of $V := \mathbb{F}_q^6$ (equipped with a non-degenerate symplectic form), such that $V_2 \oplus V_3$ is the perpendicular space of $V_1$ with respect to $V$, and $V_3$ is the perpendicular space of $V_2$ with respect to $V_2 \oplus V_3$ (this is possible by Proposition 2.2.11). Then the intersection of the stabilisers in $H$ of $V_1$, $V_2$ and $V_3$ is isomorphic to $\mathrm{Sp}(2,q)^3 = \mathrm{SL}(2,q)^3$ [89, Lemma 4.1.1(i)]. The diagonal subgroup of this direct product is isomorphic to $\mathrm{SL}(2,q)$ and has centre $Z(H)$.

Proposition 6.6.3 now shows that $Q_R$ is a maximal subgroup of $R$, that $(H)\pi \leqslant Q_R$, and that $C_R(Q_R) = Z(R)$. It follows from this first fact that the proper subgroup $Q_Y$ of $Y$ is maximal and equal to $Q_R{:}A$. Since $(H)\pi \leqslant Q_R \leqslant R = (\mathrm{SL}(2,q))\pi(H)\pi$ and $[(\mathrm{SL}(2,q))\pi, (H)\pi] = ([\mathrm{SL}(2,q), H])\pi = 1$, the outer automorphism of $(H)\pi$ induced by $A$ does not extend to an inner automorphism of $Q_R$. Therefore, $C_Y(Q_R) = C_R(Q_R) = Z(R)$, which is equal to $Z(Y)$ from the start of the proof. As $Z(Y) \leqslant C_Y(Q_Y) \leqslant C_Y(Q_R)$, we conclude that $C_Y(Q_Y) = Z(Y)$. □

Note that the simple groups in the statement of the above lemma are precisely the finite simple groups of Lie type in odd characteristic whose involutions are all

centralised by maximal subgroups of *maximal rank* (see [62, Theorem 4.5.1] and [96]).

We now prove this section's main theorem. Recall Definition 2.1.18, of an abstract Frobenius group.

*Proof of Theorem 6.6.1.* First, $\Xi(G)$ has no isolated vertices by Theorem 6.2.5. Additionally, Theorem 4.2.3 implies that each maximal subgroup of $G$ has even order, and so it suffices by Proposition 5.3.1 and Lemma 6.1.2 to show that each non-involution $x \in G \setminus \{1\}$ is adjacent in $\Xi(G)$ to some involution of $G$. Let $M$ be a maximal subgroup of $G$ containing $x$. Assume first that $G \ncong \mathrm{Sz}(q)$, so that $q$ is odd, and let $a$ be an involution of $M$. If $x \sim a$, then we are done. Otherwise, $x \in C_G(a)$. By Lemma 6.6.5, $a$ is the unique non-identity element of $C_G(a)$ that centralises each involution of $C_G(a)$. Hence $[x, a'] \neq 1$ for some involution $a' \in C_G(a)$. As $\langle x, a' \rangle \leqslant C_G(a)$, we deduce that $x \sim a'$, as required.

Assume now that $G \cong \mathrm{Sz}(q)$. By [136, Theorem 4], the centraliser in $G$ of any non-identity element is a nilpotent subgroup of $G$. However, since the non-abelian finite simple group $G$ is not isomorphic to $\mathrm{PSL}(2, r)$ for any prime power $r$, no maximal subgroup of $G$ is nilpotent [123, p. 183]. Hence $Z(M) = 1$, and in particular, $C_M(x) < M$. If $M$ is isomorphic to the simple group $\mathrm{Sz}(q_0)$, for some proper power $q_0$ of 2 that divides $q$, then $M$ is equal to $Q_M$, the normal subgroup of $M$ generated by all involutions of $M$. As $C_M(x) < M$, it follows in this case that there exists an involution $a \in M$ that does not centralise $x$, and so $x \sim a$. If instead $M \ncong \mathrm{Sz}(q_0)$, then by [136, §4, p. 133, Theorem 9] and [148, p. 117], $M$ is conjugate in $G$ to either:

(a) the Frobenius group $M_1 := S{:}C_{q-1}$, where $S$ is a Sylow 2-subgroup of $G$;

(b) the dihedral group $M_2 := D_{2(q-1)}$;

(c) the Frobenius group $M_3 := C_{q+\sqrt{2q}+1}{:}C_4$; or

(d) the Frobenius group $M_4 := C_{q-\sqrt{2q}+1}{:}C_4$.

If $M \cong M_2$, then again $Q_M = M$, and so $x \sim a$ for some involution $a \in M$. If instead $M$ is isomorphic to $M_3$ or $M_4$, then let $N$ be the normal subgroup $C_{q\pm\sqrt{2q}+1}$ of $M$. By Theorem 2.1.19, any two distinct complements of $N$ in $M$ intersect trivially, and so there exists such a complement $H$ with $x \notin H$. Let $h$ be the unique involution of $H$. Then Theorem 2.1.19 implies that $x \notin C_G(h)$, and so $x \sim h$.

Suppose finally that $M \cong M_1$. If $x \notin S$, then Theorem 2.1.19 shows that $x$ does not commute with any involution of $S$, and so $x$ is adjacent in $\Xi(G)$ to every such

involution. Now, $Z(S)$ consists of all elements of $S$ of order at most 2, and each element of $S \setminus Z(S)$ has order 4 [136, Lemma 1, Theorem 7]. Additionally, $G$ has a unique conjugacy class of cyclic subgroups of order 4 (see [136, p. 121, Proposition 18]), and so if the non-involution $x$ lies in $S$, then it also lies in a $G$-conjugate $L$ of $M_3$. By the previous paragraph, $x$ is adjacent in $\Xi(G)$ to an involution of $L$, as required. □

For the finite simple exceptional groups $G$ not of type $E_6$, ${}^2E_6$, $E_7$ or $E_8$, it is possible to prove that $\Xi(G)$ has no isolated vertices without using Theorem 6.2.5 (and without showing that each non-involution is adjacent to an involution, as in the proof of Theorem 6.6.1). First, if $G \cong \mathrm{Sz}(q)$, then each maximal subgroup of $G$ has trivial centre, as shown in the proof of Theorem 6.6.1. Hence Proposition 5.3.1 implies that no vertex in $\Xi(G)$ is isolated. If instead $G \cong {}^2G_2(q)$, then we deduce from [140, p. 63] and [148, §5.4.3] that each maximal subgroup of $G$ has a centre of order at most 2. Thus Proposition 5.3.1 and Lemma 5.3.7 (or Lemma 5.3.6) show that no vertex of $\Xi(G)$ is isolated.

In the remaining cases, let $p$ be the defining characteristic of $G$, and assume that the order of $x \in G$ is either a power of $p$ or coprime to $p$. Then $|C_G(x)|$ is known; see [39, §3, pp. 209–210], [53, Tables 1–2], [90, Table II], [128, Theorem 2.1, Theorem 3.2], [129, Theorem 2.1, Theorem 3.2], [130, Theorem 2.1, Theorem 4.1] and [133, p. 677]. Additionally, for each $y \in G$, there are unique elements $g, h \in G$ such that $y = gh = hg$, $|g|$ is a power of $p$, and $|h|$ is coprime to $p$ (see, for example, [109, pp. 16–17, p. 193]). As noted in [130, p. 13], it follows from this uniqueness property that $C_G(y) = C_G(g) \cap C_G(h)$. We can show that $|Z(M)| \leqslant 2$ for each maximal subgroup $M$ of $G$ (and that $|Z(M)| = 1$ if $q$ is a proper power of 2) using the aforementioned information about centraliser orders, and the information about the maximal subgroups of $G$ given in [46, Remark 4.12], [97, Theorem 2], [40, Theorem 1, p. 23], [148, Table 4.1, §4.8.6], and the main theorems of [90, 96, 108]. It again follows that $\Xi(G)$ has no isolated vertices.

We conclude this chapter by noting that $\Xi(\mathrm{Sz}(8))$ has diameter 3, while $\Xi(G_2(3))$ has diameter 2 (calculated using the Magma code in `diam_nc_ng`, with $G_2(3)$ constructed via the `ChevalleyGroup` function). As alluded to in §6.1, it is an open question whether any finite simple exceptional group of Lie type has a non-commuting, non-generating graph with diameter greater than 3.

# Appendix A

# GAP and Magma code

In this appendix, we summarise the files [54] containing GAP and Magma code that are associated with this thesis, and where in the thesis they are used. See the comments in the files themselves for further details.

The files containing GAP code are as follows:

- `baby_monster`: Verifies certain information about the elements and maximal subgroups of the baby monster group. Used in the proof of Proposition 6.3.5.
- `monster_cent`: Determines the known maximal subgroups of the monster group (as listed in [149, p. 67]) that have nontrivial centres, and the non-identity central elements of those maximal subgroups. Used in the proof of Proposition 6.3.2.
- `no_invol_neighbs`: Determines the conjugacy classes of elements of a sporadic simple group $G$ that may not be adjacent in $\Xi(G)$ to any involution of $G$, based on two necessary criteria. Used in the proof of Proposition 6.3.3.
- `sporadic_cent`: Determines the maximal subgroups of a sporadic simple group (other than the monster group) that have nontrivial centres, and the non-identity central elements of those maximal subgroups. Used in the proofs of Propositions 6.3.2 and 6.3.5.

In addition, the files containing Magma code are as follows:

- `base_size_functions`: Calculates the base size of a permutation group. Required by `base_size_linear` and `base_size_s_u_o`.
- `base_size_linear`: Calculates the base sizes of subspace actions of finite almost simple linear groups. Used in §3.2–3.3.
- `base_size_s_u_o`: Calculates the base sizes of subspace actions of finite almost simple symplectic, unitary and orthogonal groups. Used in §3.4–3.6.

- `comp_nc_ng`: Determines the diameters of the connected components of $\Xi(G)$ for a group $G$. Required by `nc_ng_22_groups`, and used in §5.5 and §5.8–5.9. This code utilises Proposition 5.2.1, and considers the subgraph of $\Xi(G)$ induced by representatives of generators for the non-central cyclic subgroups of $G$. As such, isolated vertices of $\Xi(G)$ are identified in the code's output if they generate the same cyclic subgroup. Additionally, a component of the induced subgraph may have diameter 1. Here, there exist vertices $x$ and $y$ in the corresponding component of the original graph such that $\langle x \rangle = \langle y \rangle$ and $d(x, y) = 2$ (see Propositions 5.2.1 and 5.2.5). The code's output accounts for this case by converting the component's diameter from 1 to 2. In all other cases, corresponding components of the two graphs have equal diameters. Note that this code can only be used when $G$ has at most $2^{16} - 1 = 65535$ non-central cyclic subgroups (this is the maximum order of a graph in Magma).

- `diam_nc_ng`: Given a (finite, non-abelian) group $G$, calculates whether the diameter of $\Xi(G)$ is equal to 2, equal to 3, or greater than 3 (by Proposition 5.2.5, these are the only possibilities). Used in §5.9 and throughout Chapter 6. Compared with `comp_nc_ng`, this code is more suitable when considering reasonably large groups. Additionally, the code here utilises Proposition 5.2.1 and Corollary 5.2.14, which describe certain symmetries of the graph related to pairs of vertices of $\Xi(G)$ that generate the same cyclic subgroup, and related to pairs of edges of $\Xi(G)$ that are conjugate under elements of $G$ (in particular, elements that centralise a vertex in the intersection of the two edges). As in `comp_nc_ng`, we consider the graph obtained from $\Xi(G)$ by identifying vertices that generate the same cyclic subgroup, and the code accounts for the possibility that this induced subgraph has diameter 1.

- `linear_examples`: Verifies certain information about the non-commuting, non-generating graphs of the groups $\mathrm{SL}(2, 3)$, $\mathrm{SL}(2, 7)$ and $\mathrm{SL}(2, 11)$. Used in §6.4.

- `nc_ng_22_groups`: Verifies certain information about $[2, 2]$-groups (and one small group that is not a $[2, 2]$-group). Used in and below Example 5.8.9.

- `p_groups_small`: Finds a $p$-group of the smallest order satisfying properties (iii)(a), (b) and (c) of Theorem 5.6.1, respectively. Used below the proof of this theorem.

- `psu32_spread`: Verifies that the graph $\Xi(\mathrm{PSU}(3, 2))$ has spread 9. Used below the proof of Corollary 5.2.3.

- `psu37`: Determines useful information about the elements and maximal subgroups of $\mathrm{PSU}(3,7)$. Used in the proof of Proposition 4.1.5.
- `psu72`: Determines useful information about the elements and maximal subgroups of $\mathrm{PSU}(7,2)$. Used in the proofs of Proposition 4.1.5 and Theorem 6.5.1.
- `su54`: Determines useful information about the elements and maximal subgroups of $\mathrm{SU}(5,4)$. Used in the proof of Lemma 6.5.3.

Note that, in order to run the code in `base_size_linear`, `base_size_s_u_o` or `diam_nc_ng` to verify results in this thesis concerning sufficiently large groups, significant amounts of time and memory (e.g., a few days and tens of gigabytes in some cases) are required (and similarly when the code in `base_size_functions` is directly applied to large groups). The code in each of `psu32_spread` and `su54` has a runtime of approximately 1–2 hours, while the code in each remaining file listed above has a runtime of at most a few minutes.

# Bibliography


[1] A. Abdollahi, S. Akbari, and H. R. Maimani. Non-commuting graph of a group. *J. Algebra*, 298(2):468–492, 2006. 95, 98

[2] Saad Adnan. On groups having exactly 2 conjugacy classes of maximal subgroups. II. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. (8)*, 68(3):179, 1980. 123, 124

[3] M. Aschbacher and R. Guralnick. Some applications of the first cohomology group. *J. Algebra*, 90(2):446–460, 1984. 25

[4] Peter C. Austin and Erich W. Ellers. Products of involutions in the finite Chevalley groups of type $F_4(K)$. *Comm. Algebra*, 30(8):4019–4029, 2002. 192

[5] Reinhold Baer. Classes of finite groups and their properties. *Illinois J. Math.*, 1:115–187, 1957. 12, 150

[6] Adolfo Ballester-Bolinches and Luis M. Ezquerro. *Classes of finite groups*, volume 584 of *Mathematics and Its Applications (Springer)*. Springer, Dordrecht, 2006. 12

[7] Kristine Bauer, Debasis Sen, and Peter Zvengrowski. A generalized Goursat lemma. *Tatra Mt. Math. Publ.*, 64:1–19, 2015. 115

[8] Gilbert Baumslag. *Lecture notes on nilpotent groups*. Regional Conference Series in Mathematics, No. 2. American Mathematical Society, Providence, R.I., 1971. 112

[9] James Michael Belk. *Thompson's group F*. PhD thesis, Cornell University, August 2004. 138

[10] Áron Bereczky. Maximal overgroups of Singer elements in classical groups. *J. Algebra*, 234(1):187–206, 2000. 33, 186

[11] Hans Ulrich Besche, Bettina Eick, and E. A. O'Brien. The groups of order at most 2000. *Electron. Res. Announc. Amer. Math. Soc.*, 7:1–4, 2001. 120, 138, 151

[12] Mai Hoang Bien and Do Hoang Viet. Intersection graphs of general linear groups. *J. Algebra Appl.*, 20(3):Paper No. 2150039, 14, 2021. 83

[13] A. V. Borovik. Tame groups of odd and even type. In *Algebraic groups and their representations (Cambridge, 1997)*, volume 517 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 341–366. Kluwer Acad. Publ., Dordrecht, 1998. 25

[14] J. Bosák. The graphs of semigroups. In *Theory of Graphs and its Applications (Proc. Sympos. Smolenice, 1963)*, pages 119–125. Publ. House Czech. Acad. Sci., Prague, 1964. 83

[15] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. 1

[16] Richard Brauer and K. A. Fowler. On groups of even order. *Ann. of Math. (2)*, 62:565–583, 1955. 3

[17] John N. Bray, Derek F. Holt, and Colva M. Roney-Dougal. *The maximal subgroups of the low-dimensional finite classical groups*, volume 407 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2013. With a foreword by Martin Liebeck. 13, 16, 18, 19, 20, 22, 23, 25, 39, 40, 41, 44, 46, 48, 49, 50, 53, 56, 60, 63, 64, 67, 70, 72, 75, 76, 77, 87, 89, 180, 182, 186, 190

[18] Thomas Breuer. Tutorial for the gap character table library. `https://www.math.rwth-aachen.de/~Thomas.Breuer/ctbllib/doc/chap2.html`. Accessed: January 15, 2021. 146

[19] Thomas Breuer, Robert M. Guralnick, and William M. Kantor. Probabilistic generation of finite simple groups. II. *J. Algebra*, 320(2):443–494, 2008. 4

[20] J. R. Britnell, A. Evseev, R. M. Guralnick, P. E. Holmes, and A. Maróti. Sets of elements that pairwise generate a linear group. *J. Combin. Theory Ser. A*, 115(3):442–465, 2008. 180

[21] José Burillo, Sean Cleary, Armando Martino, and Claas E. Röver. Commensurations and metric properties of Houghton's groups. *Pacific J. Math.*, 285(2):289–301, 2016. 155

[22] Timothy Burness, Robert Guralnick, and Scott Harper. The spread of a finite group. *Ann. of Math. (2)*, 193(2):619–687, 2021. 4, 96, 98, 152, 156

[23] Timothy C. Burness. On base sizes for actions of finite classical groups. *J. Lond. Math. Soc. (2)*, 75(3):545–562, 2007. 2, 37, 43, 76

[24] Timothy C. Burness. Simple groups, generation and probabilistic methods. In *Groups St Andrews 2017 in Birmingham*, volume 455 of *London Math. Soc. Lecture Note Ser.*, pages 200–229. Cambridge Univ. Press, Cambridge, 2019. 94

[25] Timothy C. Burness and Michael Giudici. *Classical groups, derangements and primes*, volume 25 of *Australian Mathematical Society Lecture Series*. Cambridge University Press, Cambridge, 2016. 17, 40, 41

[26] Timothy C. Burness, Robert M. Guralnick, and Jan Saxl. On base sizes for symmetric groups. *Bull. Lond. Math. Soc.*, 43(2):386–391, 2011. 2

[27] Timothy C. Burness, Robert M. Guralnick, and Jan Saxl. On base sizes for algebraic groups. *J. Eur. Math. Soc. (JEMS)*, 19(8):2269–2341, 2017. 2, 36, 45, 48, 53, 62, 63, 70, 75

[28] Timothy C. Burness, Martin W. Liebeck, and Aner Shalev. Base sizes for simple groups and a conjecture of Cameron. *Proc. Lond. Math. Soc. (3)*, 98(1):116–162, 2009. 2

[29] Timothy C. Burness, Andrea Lucchini, and Daniele Nemmi. On the soluble graph of a finite group. Preprint, 2021, arXiv:2111.05697. 85, 103

[30] Timothy C. Burness, E. A. O'Brien, and Robert A. Wilson. Base sizes for sporadic simple groups. *Israel J. Math.*, 177:307–333, 2010. 2

[31] José Cáceres, Delia Garijo, Antonio González, Alberto Márquez, and María Luz Puertas. The determining number of Kneser graphs. *Discrete Math. Theor. Comput. Sci.*, 15(1):1–14, 2013. 2

[32] Peter J. Cameron. Some open problems on permutation groups. In *Groups, combinatorics & geometry (Durham, 1990)*, volume 165 of *London Math. Soc. Lecture Note Ser.*, pages 340–350. Cambridge Univ. Press, Cambridge, 1992. 2

[33] Peter J. Cameron. *Permutation groups*, volume 45 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1999. 1, 2

[34] Peter J. Cameron. Graphs defined on groups. *Int. J. Group Theory*, 11(2):53–107, 2022. i, 3, 4, 5, 85, 95, 103

[35] Peter J. Cameron, Saul D. Freedman, and Colva M. Roney-Dougal. The non-commuting, non-generating graph of a nilpotent group. *Electron. J. Combin.*, 28(1):Paper No. 1.16, 15, 2021. 4

[36] Peter J. Cameron and William M. Kantor. Random permutations: some group-theoretic aspects. *Combin. Probab. Comput.*, 2(3):257–262, 1993. 2

[37] Peter J. Cameron, Andrea Lucchini, and Colva M. Roney-Dougal. Generating sets of finite groups. *Trans. Amer. Math. Soc.*, 370(9):6751–6770, 2018. 102

[38] L. Carlitz. Note on a quartic congruence. *Amer. Math. Monthly*, 63:569–571, 1956. 31

[39] Bomshik Chang. The conjugate classes of Chevalley groups of type $(G_2)$. *J. Algebra*, 9:190–211, 1968. 194

[40] Arjeh M. Cohen, Martin W. Liebeck, Jan Saxl, and Gary M. Seitz. The local maximal subgroups of exceptional groups of Lie type, finite and algebraic. *Proc. London Math. Soc. (3)*, 64(1):21–48, 1992. 194

[41] P. M. Cohn. *Basic algebra*. Springer-Verlag London, Ltd., London, 2003. Groups, rings and fields. 7

[42] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups*. Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray. 1, 86, 92, 123, 169, 170, 171

[43] Hannah J. Coutts, Martyn Quick, and Colva M. Roney-Dougal. The primitive permutation groups of degree less than 4096. *Comm. Algebra*, 39(10):3526–3546, 2011. 153

[44] Charles Garnet Cox. A note on the $R_\infty$ property for groups $\mathrm{FAlt}(X) \leqslant G \leqslant \mathrm{Sym}(X)$. *Comm. Algebra*, 47(3):978–989, 2019. 99, 155

[45] Charles Garnet Cox. On the spread of infinite groups. *Proc. Edinb. Math. Soc. (2)*, 65(1):214–228, 2022. 155, 156

[46] David A. Craven. The maximal subgroups of the exceptional groups $F_4(q)$, $E_6(q)$ and ${}^2E_6(q)$ and related almost simple groups. Preprint, 2021, arXiv:2103.04869. 194

[47] Eleonora Crestani and Andrea Lucchini. The non-isolated vertices in the generating graph of a direct powers of simple groups. *J. Algebraic Combin.*, 37(2):249–263, 2013. 4, 114, 157

[48] B. Csákány and G. Pollák. The graph of subgroups of a finite group. *Czechoslovak Math. J.*, 19(94):241–247, 1969. 3, 83, 85, 87

[49] Francesca Dalla Volta and Andrea Lucchini. Generation of almost simple groups. *J. Algebra*, 178(1):194–223, 1995. 25

[50] Warwick de Launey and Dane Flannery. *Algebraic design theory*, volume 175 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2011. 33, 34

[51] John D. Dixon and Brian Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996. 41, 43

[52] Klaus Doerk and Trevor Hawkes. *Finite soluble groups*, volume 4 of *De Gruyter Expositions in Mathematics*. Walter de Gruyter & Co., Berlin, 1992. 106

[53] Hikoe Enomoto. The conjugacy classes of Chevalley groups of type $(G_2)$ over finite fields of characteristic 2 or 3. *J. Fac. Sci. Univ. Tokyo Sect. I*, 16:497–512 (1970), 1969. 194

[54] Saul D. Freedman. *Diameters of graphs related to groups and base sizes of primitive groups - GAP and Magma code (thesis data)*. August 2022, `https://doi.org/10.17630/56ceed97-0a86-4684-b0a9-e454c1a7440b`. 1, 195

[55] Saul D. Freedman, Michael Giudici, and Cheryl E. Praeger. Total closure for permutation actions of finite nonabelian simple groups (submitted). arXiv:2206.02347. 2, 46

[56] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.8.4*, 2016. 1

[57] Nick Gill, Bianca Lodà, and Pablo Spiga. On the height and relational complexity of a finite permutation group. *Nagoya Math. J. to appear*. 1, 45

[58] Michael Giudici and Bojan Kuzma. Realizability problem for commuting graphs. *J. Aust. Math. Soc.*, 101(3):335–355, 2016. 101

[59] Michael Giudici and Luke Morgan. A theory of semiprimitive groups. *J. Algebra*, 503:146–185, 2018. 13

[60] Michael Giudici and Chris Parker. There is no upper bound for the diameter of the commuting graph of a finite group. *J. Combin. Theory Ser. A*, 120(7):1600–1603, 2013. 3

[61] George Glauberman. Central elements in core-free groups. *J. Algebra*, 4:403–420, 1966. 107, 164

[62] Daniel Gorenstein, Richard Lyons, and Ronald Solomon. *The classification of the finite simple groups. Number 3. Part I. Chapter A*, volume 40 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1998. Almost simple $K$-groups. 191, 193

[63] Edouard Goursat. Sur les substitutions orthogonales et les divisions régulières de l'espace. *Ann. Sci. École Norm. Sup. (3)*, 6:9–102, 1889. 115

[64] Robert L. Griess, Jr. Finite groups whose involutions lie in the center. *Quart. J. Math. Oxford Ser. (2)*, 29(115):241–247, 1978. 191

[65] Karl W. Gruenberg. *Cohomological topics in group theory*. Lecture Notes in Mathematics, Vol. 143. Springer-Verlag, Berlin-New York, 1970. 100

[66] V. S. Guba. A finitely generated simple group with free 2-generated subgroups. *Sibirsk. Mat. Zh.*, 27(5):50–67, 204, 1986. 99

[67] Simon Guest and Pablo Spiga. Finite primitive groups and regular orbits of group elements. *Trans. Amer. Math. Soc.*, 369(2):997–1024, 2017. 42

[68] Narain Gupta and Said Sidki. On the Burnside problem for periodic groups. *Math. Z.*, 182(3):385–388, 1983. 112

[69] Robert M. Guralnick and Geoffrey R. Robinson. On extensions of the Baer-Suzuki theorem. *Israel J. Math.*, 82(1-3):281–297, 1993. 107

[70] Bui Xuan Hai, Bui Xuan Binh Minh, Le Van Chua, and Mai Hoang Bien. Low diameter algebraic graphs. In *Extended Abstracts EuroComb 2021*, pages 465–471, Cham, 2021. Springer International Publishing. 83

[71] Zoltán Halasi. On the base size for the symmetric group acting on subsets. *Studia Sci. Math. Hungar.*, 49(4):492–500, 2012. 2

[72] Zoltán Halasi, Martin W. Liebeck, and Attila Maróti. Base sizes of primitive groups: bounds with explicit constants. *J. Algebra*, 521:16–43, 2019. 2, 36, 40, 41, 42, 44, 46, 48, 49, 54, 63, 67, 75, 81

[73] M. Hazewinkel, editor. *Encyclopaedia of mathematics. Supplement. Vol. III.* Kluwer Academic Publishers, Dordrecht, 2001. 9

[74] Gerhard Heide, Jan Saxl, Pham Huu Tiep, and Alexandre E. Zalesski. Conjugacy action, induced representations and the Steinberg square for simple groups of Lie type. *Proc. Lond. Math. Soc. (3)*, 106(4):908–930, 2013. 192

[75] Christoph Hering. Transitive linear groups and linear groups which contain irreducible subgroups of prime order. *Geometriae Dedicata*, 2:425–460, 1974. 146

[76] I. N. Herstein. A remark on finite groups. *Proc. Amer. Math. Soc.*, 9:255–257, 1958. 10

[77] Marcel Herzog, Patrizia Longobardi, and Mercede Maj. On a graph related to the maximal subgroups of a group. *Bull. Aust. Math. Soc.*, 81(2):317–328, 2010. 3, 83, 85, 131

[78] Marshall D. Hestenes. Singer groups. *Canadian J. Math.*, 22:492–513, 1970. 33, 88, 89, 186, 189

[79] Petra E. Holmes and Robert A. Wilson. $\mathrm{PSL}_2(59)$ is a subgroup of the Monster. *J. London Math. Soc. (2)*, 69(1):141–152, 2004. 86

[80] Petra E. Holmes and Robert A. Wilson. On subgroups of the Monster containing $A_5$'s. *J. Algebra*, 319(7):2653–2667, 2008. 86

[81] Derek F. Holt and Colva M. Roney-Dougal. Constructing maximal subgroups of classical groups. *LMS J. Comput. Math.*, 8:46–79, 2005. 33

[82] John F. Humphreys. *A course in group theory.* Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1996. 6

[83] B. Huppert. *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin-New York, 1967. 34, 88

[84] I. Martin Isaacs. *Finite group theory*, volume 92 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2008. 11

[85] Christoph Jansen, Klaus Lux, Richard Parker, and Robert Wilson. *An atlas of Brauer characters*, volume 11 of *London Mathematical Society Monographs. New Series*. The Clarendon Press, Oxford University Press, New York, 1995. Appendix 2 by T. Breuer and S. Norton, Oxford Science Publications. 87, 170

[86] Veronica Kelsey. *Base size and generating graphs of primitive permutation groups*. PhD thesis, University of St Andrews, September 2021. 45

[87] Veronica Kelsey and Colva M. Roney-Dougal. On relational complexity and base size of finite primitive groups. *Pacific J. Math.* To appear. arXiv:2107.14208. 45

[88] Evgenii I. Khukhro. *Nilpotent groups and their automorphisms*, volume 8 of *De Gruyter Expositions in Mathematics*. Walter de Gruyter & Co., Berlin, 1993. 147

[89] Peter Kleidman and Martin Liebeck. *The subgroup structure of the finite classical groups*, volume 129 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1990. 13, 14, 15, 16, 17, 18, 19, 22, 23, 24, 39, 40, 41, 44, 46, 48, 49, 66, 67, 70, 71, 72, 75, 77, 184, 192

[90] Peter B. Kleidman. The maximal subgroups of the Steinberg triality groups ${}^3D_4(q)$ and of their automorphism groups. *J. Algebra*, 115(1):182–199, 1988. 194

[91] Frieder Knüppel and Gerd Thomsen. Involutions and commutators in orthogonal groups. *J. Austral. Math. Soc. Ser. A*, 65(1):1–36, 1998. 190

[92] C. R. Leedham-Green and S. McKay. *The structure of groups of prime power order*, volume 27 of *London Mathematical Society Monographs. New Series*. Oxford University Press, Oxford, 2002. Oxford Science Publications. 190

[93] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. 31, 32, 34, 56

[94] Martin W. Liebeck. On minimal degrees and base sizes of primitive permutation groups. *Arch. Math. (Basel)*, 43(1):11–15, 1984. 36

[95] Martin W. Liebeck and Jan Saxl. On point stabilizers in primitive permutation groups. *Comm. Algebra*, 19(10):2777–2786, 1991. 86, 87, 182, 186, 189

[96] Martin W. Liebeck, Jan Saxl, and Gary M. Seitz. Subgroups of maximal rank in finite exceptional groups of Lie type. *Proc. London Math. Soc. (3)*, 65(2):297–325, 1992. 193, 194

[97] Martin W. Liebeck and Gary M. Seitz. Maximal subgroups of exceptional groups of Lie type, finite and algebraic. *Geom. Dedicata*, 35(1-3):353–387, 1990. 194

[98] Martin W. Liebeck and Aner Shalev. Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky. *J. Algebra*, 184(1):31–57, 1996. 4, 94

[99] Martin W. Liebeck and Aner Shalev. Simple groups, permutation groups, and probability. *J. Amer. Math. Soc.*, 12(2):497–520, 1999. 2, 38, 40

[100] Martin W. Liebeck and Aner Shalev. Bases of primitive permutation groups. In *Groups, combinatorics & geometry (Durham, 2001)*, pages 147–154. World Sci. Publ., River Edge, NJ, 2003. 37, 47

[101] Clara Löh. *Geometric group theory*. Universitext. Springer, Cham, 2017. An introduction. 138

[102] Andrea Lucchini. The diameter of the generating graph of a finite soluble group. *J. Algebra*, 492:28–43, 2017. 4, 112, 157

[103] Andrea Lucchini, Attila Maróti, and Colva M. Roney-Dougal. On the generating graph of a simple group. *J. Aust. Math. Soc.*, 103(1):91–103, 2017. 149, 155

[104] Andrea Lucchini and Daniele Nemmi. On the connectivity of the non-generating graph. *Arch. Math. (Basel)*, 118(6):563–576, 2022. 165, 189

[105] Roger C. Lyndon and Paul E. Schupp. *Combinatorial group theory*. Springer-Verlag, Berlin-New York, 1977. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 89. 158

[106] Xuanlong Ma. On the diameter of the intersection graph of a finite simple group. *Czechoslovak Math. J.*, 66(141)(2):365–370, 2016. 3, 84, 85

[107] Wilhelm Magnus, Abraham Karrass, and Donald Solitar. *Combinatorial group theory*. Dover Publications, Inc., New York, revised edition, 1976. Presentations of groups in terms of generators and relations. 159

[108] Gunter Malle. The maximal subgroups of ${}^2F_4(q^2)$. *J. Algebra*, 139(1):52–69, 1991. 194

[109] Gunter Malle and Donna Testerman. *Linear algebraic groups and finite groups of Lie type*, volume 133 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2011. 36, 191, 194

[110] G. A. Miller and H. C. Moreno. Non-abelian groups in which every subgroup is abelian. *Trans. Amer. Math. Soc.*, 4(4):398–404, 1903. 83, 105, 118

[111] G. L. Morgan and C. W. Parker. The diameter of the commuting graph of a finite group with trivial centre. *J. Algebra*, 393:41–59, 2013. 3

[112] Joy Morris and Pablo Spiga. On the base size of the symmetric and the alternating group acting on partitions. *J. Algebra*, 587:569–593, 2021. 2

[113] Mariapia Moscatiello and Colva M. Roney-Dougal. Base sizes of primitive permutation groups. *Monatsh. Math.*, 198(2):411–443, 2022. 2, 39, 40, 42, 44, 46, 48, 63, 67, 75

[114] Aglaia Myropolska. The class $\mathcal{MN}$ of groups in which all maximal subgroups are normal. Preprint, 2015, arXiv:1509.08090. 112

[115] Aglaia Myropolska. Andrews-Curtis and Nielsen equivalence relations on some infinite groups. *J. Group Theory*, 19(1):161–178, 2016. 112

[116] A. Yu. Ol'shanskiĭ. Groups of bounded period with subgroups of prime order. *Algebra i Logika*, 21(5):553–618, 1982. 11

[117] Oystein Ore. Contributions to the theory of groups of finite order. *Duke Math. J.*, 5(2):431–460, 1939. 11

[118] Sam Perlis. *Theory of matrices*. Dover Publications, Inc., New York, 1991. Reprint of the 1958 edition. 26

[119] E. L. Pervova. Maximal subgroups of some non locally finite $p$-groups. *Internat. J. Algebra Comput.*, 15(5-6):1129–1150, 2005. 112

[120] Cheryl E. Praeger. The inclusion problem for finite primitive permutation groups. *Proc. London Math. Soc. (3)*, 60(1):68–88, 1990. 154

[121] L. Rédei. Das "schiefe Produkt" in der Gruppentheorie mit Anwendung auf die endlichen nichtkommutativen Gruppen mit lauter kommutativen echten Untergruppen und die Ordnungszahlen, zu denen nur kommutative Gruppen gehören. *Comment. Math. Helv.*, 20:225–264, 1947. 105

[122] Steven Roman. *Field theory*, volume 158 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2006. 32

[123] John S. Rose. On finite insoluble groups with nilpotent maximal subgroups. *J. Algebra*, 48(1):182–196, 1977. 193

[124] John S. Rose. *A course on group theory*. Cambridge University Press, Cambridge-New York-Melbourne, 1978. 10

[125] Hossein Shahsavari and Behrooz Khosravi. On the intersection graph of a finite group. *Czechoslovak Math. J.*, 67(142)(4):1145–1153, 2017. 84

[126] Rulin Shen. Intersection graphs of subgroups of finite groups. *Czechoslovak Math. J.*, 60(135)(4):945–950, 2010. i, 3, 83, 87, 90

[127] Wu Jie Shi. Finite groups having at most two classes of maximal subgroups of the same order. *Chinese Ann. Math. Ser. A*, 10(5):532–537, 1989. 123

[128] Ken-ichi Shinoda. The conjugacy classes of Chevalley groups of type $(F_4)$ over finite fields of characteristic 2. *J. Fac. Sci. Univ. Tokyo Sect. I A Math.*, 21:133–159, 1974. 194

[129] Ken-ichi Shinoda. The conjugacy classes of the finite Ree groups of type $(F_4)$. *J. Fac. Sci. Univ. Tokyo Sect. I A Math.*, 22:1–15, 1975. 194

[130] Toshiaki Shoji. The conjugacy classes of Chevalley groups of type $(F_4)$ over finite fields of characteristic $p \neq 2$. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 21:1–17, 1974. 194

[131] M. W. Short. *The primitive soluble permutation groups of degree less than* 256, volume 1519 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1992. 35

[132] Simon M. Smith. A classification of primitive permutation groups with finite stabilizers. *J. Algebra*, 432:12–21, 2015. 131

[133] N. Spaltenstein. Caractères unipotents de ${}^3D_4(\mathbb{F}_q)$. *Comment. Math. Helv.*, 57(4):676–691, 1982. 194

[134] Robert Steinberg. Generators for simple groups. *Canadian J. Math.*, 14:277–283, 1962. 25

[135] D. A. Suprunenko. *Matrix groups*. American Mathematical Society, Providence, R.I., 1976. Translated from the Russian, Translation edited by K. A. Hirsch, Translations of Mathematical Monographs, Vol. 45. 30

[136] Michio Suzuki. On a class of doubly transitive groups. *Ann. of Math. (2)*, 75:105–145, 1962. 146, 147, 193, 194

[137] Donald E. Taylor. *The geometry of the classical groups*, volume 9 of *Sigma Series in Pure Mathematics*. Heldermann Verlag, Berlin, 1992. 21

[138] Jacques Thévenaz. Maximal subgroups of direct products. *J. Algebra*, 198(2):352–361, 1997. 115

[139] Gareth Tracey. Personal communication regarding material in a forthcoming paper, joint with Robert M. Guralnick, tentatively titled 'On elements of finite groups contained in a unique maximal subgroup', 11 April 2022. 108, 155, 169

[140] Harold N. Ward. On Ree's series of simple groups. *Trans. Amer. Math. Soc.*, 121:62–89, 1966. 194

[141] William C. Waterhouse. Two generators for the general linear groups over finite fields. *Linear and Multilinear Algebra*, 24(4):227–230, 1989. 51

[142] B. A. F. Wehrfritz. *Finite groups*. World Scientific Publishing Co., Inc., River Edge, NJ, 1999. A second course on group theory. 7

[143] A. J. Weir. Sylow $p$-subgroups of the general linear group over finite fields of characteristic $p$. *Proc. Amer. Math. Soc.*, 6:454–464, 1955. 71

[144] Guo Wenbin. *The Theory of Classes of Groups*, volume 505 of *Mathematics and Its Applications*. Springer Netherlands, 2000. 6

[145] Helmut W. Wielandt. Permutation groups through invariant relations and invariant functions, 1969. Lecture Notes, Ohio State University, 1969. 46

[146] J. S. Williams. Prime graph components of finite groups. *J. Algebra*, 69(2):487–513, 1981. 84

[147] Robert Wilson, Peter Walsh, Jonathan Tripp, Ibrahim Suleiman, Richard Parker, Simon Norton, Simon Nickerson, Steve Linton, John Bray, and Rachel Abbott. *ATLAS of Finite Group Representations - Version 3*. `https://brauer.maths.qmul.ac.uk/Atlas/v3/`. Accessed: June 9, 2021. 87, 174

[148] Robert A. Wilson. *The finite simple groups*, volume 251 of *Graduate Texts in Mathematics*. Springer-Verlag London, Ltd., London, 2009. 14, 24, 192, 193, 194

[149] Robert A. Wilson. Maximal subgroups of sporadic groups. In *Finite simple groups: thirty years of the atlas and beyond*, volume 694 of *Contemp. Math.*, pages 57–72. Amer. Math. Soc., Providence, RI, 2017. 87, 170, 195

[150] Qinhai Zhang, Xiujuan Sun, Lijian An, and Mingyao Xu. Finite $p$-groups all of whose subgroups of index $p^2$ are abelian. *Algebra Colloq.*, 15(1):167–180, 2008. 105, 118