LOCAL FUSION GRAPHS OF FINITE GROUPS

A thesis submitted to the University of Manchester
for the degree of Doctor of Philosophy
in the Faculty of Engineering and Physical Sciences

2012

John Joseph Ballantyne

School of Mathematics

Contents

Abstract **5**

Declaration **6**

Copyright Statement **7**

Acknowledgements **8**

1 Introduction **9**

1.1 Preliminary Results 16

2 Symmetric Groups **21**

2.1 The x-graph 21

2.2 The diameter of $\mathcal{F}(G, X)$ 23

2.3 The $C_G(t)$-orbit structure of $\mathcal{F}(G, X)$ 29

2.4 Connectedness when π is restricted 31

3 Linear Groups of Small Dimension **35**

3.1 A brief review 35

3.2 The local fusion graphs of $PSL_2(q)$ 37

4 Finite Coxeter Groups **42**

4.1 Reflection Groups 42

4.2 The Classical Coxeter Groups 45

4.3 The Exceptional Coxeter Groups 62

5 Sporadic Simple Groups **64**

5.1 The Mathieu Groups . . . 66

5.2 The Leech Lattice Groups . . . 67

5.3 The Fischer Groups . . . 68

5.4 The Monstrous Groups . . . 69

5.5 The Pariahs . . . 70

6 A Review of Finite Groups of Lie-Type **72**

6.1 Algebraic Group Theory . . . 72

6.2 Subgroups of Algebraic Groups . . . 73

6.3 Groups with a BN-pair . . . 74

6.4 Classification of Simple Algebraic Groups . . . 75

6.5 Finite Groups of Lie-Type . . . 77

6.6 Classical Groups . . . 78

6.7 Maximal Subgroups . . . 83

6.8 Generation of Classical Groups . . . 85

7 Groups of Lie-Type over Fields of Odd Characteristic **90**

7.1 Strategy . . . 90

7.2 Linear Groups . . . 91

7.3 Symplectic Groups . . . 95

7.4 Unitary Groups . . . 100

7.5 Orthogonal Groups . . . 108

7.6 Exceptional and Twisted Groups . . . 118

8 Groups of Lie-Type over Fields of Even Characteristic **120**

8.1 Involutions . . . 120

8.2 Linear Groups . . . 123

8.3 Symplectic Groups . . . 127

8.4 Unitary Groups . . . 129

8.5 Orthogonal Groups . . . 131

8.6 Exceptional and Twisted Groups 136

9 Coprimality Graphs of Symmetric Groups **139**

9.1 Representation Theory of the Symmetric Group 140

9.2 Applying Representation Theory 144

9.3 Products of Permutations 151

9.4 The proof of Theorems 9.3 and 9.4 158

9.5 The proof of Theorem 9.1 169

10 A Computational Application of Local Fusion Graphs **171**

10.1 Bray's Algorithm 172

10.2 Finding Centraliser Elements 173

10.3 Calculating Cycle Elements 174

10.4 Experimental Data 176

10.5 Implementation in MAGMA 180

Bibliography **185**

Word count 58421

The University of Manchester

John Joseph Ballantyne
Doctor of Philosophy
Local Fusion Graphs of Finite Groups
January 3, 2012

Let G be a group, with X a G-conjugacy class of involutions. The local fusion graph $\mathcal{F}(G,X)$ has X as its vertex set, with vertices $x, y \in X$ joined by an edge if, and only if, $x \neq y$ and the order of the product xy is odd. In this thesis we study these, and other related graphs, for a variety of finite groups, paying particular attention to the cases where G is a finite simple group. We also present a computational algorithm regarding centralisers of involutions, which makes use of local fusion graphs.

Declaration

No portion of the work referred to in this thesis has been submitted in support of an application for another degree or qualification of this or any other university or other institute of learning.

Copyright Statement

Acknowledgements

Firstly, I would like to thank my supervisor Peter Rowley. The mathematical debt I owe him is outweighed only by the one I owe him at the bar!

Secondly, the School of Mathematics at the University of Manchester, including all the staff and fellow students who have helped me in any way over the last four years.

Thirdly, the Engineering and Physical Sciences Research Council, for funding my PhD research.

Fourthly, my parents, for their constant support, and their financial backing during my time as an undergraduate and Masters student.

And finally, my wife Inga, for countless things, but particularly for moving with me to Manchester, allowing me to pursue my dream.

Chapter 1

Introduction

When working with a finite group, it can often be of benefit to consider combinatorial structures on which the group acts. Not only might this shed light on properties of the group one is studying, but these objects can often be of interest in their own right. Over the last fifty years or so, there have been a number of successful applications of this technique where the structure involved has been a graph. These graphs come in all shapes and sizes; to give a flavour of the theory we cite just a few examples. One of the more well known graphs associated to a group G is the *Cayley graph*, defined using a generating set $S = S^{-1}$ for G. The vertices of the Cayley graph are the elements of G, and vertices x and y are joined by an edge if and only if $x = ys$ for some $s \in S$. Another variety are *commuting graphs*, which have a subset of a group G as their vertex set, with vertices adjacent if and only if they commute. When the vertex set is chosen to be a G-conjugacy class of involutions these commuting graphs have been of particular interest: in [35], Bernd Fischer used such objects to construct three previously unknown finite simple groups; while in more recent years extensive research into the structure of these graphs has been carried out by a number of authors, for example in [10], [11], [12], [13], [14] and [34]. Yet another type of graph are S_3-*involution graphs*, as studied by Devillers, Giudici, Li and Praeger. Here we again have a G-conjugacy class of involutions as the vertex set, but with vertices joined by an edge if and only if the subgroup they generate lies in a particular G-conjugacy class of subgroups isomorphic to Sym(3). In [31] it is shown that an interesting tower of graphs associated with the subgroup chain $\mathrm{Alt}(5) \leq PSL(2,11) \leq M_{11} \leq M_{12}$ can be described in terms of S_3-involution graphs.

Drawing motivation from such examples, in this thesis we introduce a new family of graphs, which we call *coprimality graphs*. It is our aim to determine structural properties of some such graphs, paying particular attention to a subfamily known as *local fusion graphs*. In addition, we shall describe how such graphs can be of use in a computational context.

Let us now give formal definitions of the objects we shall study.

Definition 1.1. Let G be a group, with a G-conjugacy class X of elements of prime order p. Let π be a nonempty set of integers which are coprime to p. The *π-coprimality graph*, denoted $\mathcal{C}_\pi(G, X)$ has X as its vertex set, with $x, y \in X$ joined by an edge if and only if $x \neq y$ and the order of the product xy lies in π. If π consists of all integers which are coprime to p, we simply refer to the *coprimality graph*, $\mathcal{C}_{p'}(G, X)$.

Notice that G acts vertex transitively on each of its π-coprimality graphs $\mathcal{C}_\pi(G, X)$. This follows immediately from the fact that X is a G-conjugacy class. Moreover, π-coprimality graphs are undirected, since for any product xy where $x, y \in G$, we have $yx = x^{-1}xyx = (xy)^x$, and so, being conjugate elements, yx and xy have the same order.

Due to their very broad definition, coprimality graphs encompass many types of graph which have been previously studied. For example, when their vertex sets are chosen to be conjugacy classes, then both the S_3-involution graphs investigated by Devillers and Giudici in [30], and the commuting graphs studied by Baumeister and Stein in [17] are coprimality graphs, where $p = 2$ and 3 in each case respectively. This generality comes at a cost however, as it is usually difficult to answer questions about the full set of coprimality graphs of a given group. Therefore, for the majority of this thesis our attention is restricted to a particularly interesting type of coprimality graph.

Definition 1.2. Let G be a group, with a G-conjugacy class X of involutions. Let π be a nonempty set of odd integers. The π-*local fusion graph*, denoted $\mathcal{F}_\pi(G,X)$ has X as its vertex set, with $x,y \in X$ joined by an edge if and only if $x \neq y$ and the order of the product xy lies in π. If π consists of all odd integers, we simply refer to the *local fusion graph*, $\mathcal{F}(G,X)$.

Involutions play a fundamental role in finite group theory, as demonstrated by their crucial importance to the Classification of Finite Simple Groups. An indication as to their special nature is the fact that any two involutions x and y in a finite group generate a dihedral subgroup (see [61]). No analagous result exists for elements of arbitrary order. It is this property which allows us to explain the motivation behind our particular focus on local fusion graphs. For suppose that x and y are G-conjugate involutions lying in a conjugacy class X, and that x and y are adjacent in $\mathcal{F}(G,X)$. Then the product xy has odd order, say $2m+1$, where $m \geq 1$. Using the fact that $\langle x,y\rangle$ is a dihedral group, we can see that

$$y = x^{(yx)^m},$$

so x and y are in fact conjugate in $\langle x,y\rangle$. Thus, if we have a path

$$x = x_1 \to x_2 \to \cdots \to x_m = z$$

from x to z in $\mathcal{F}(G,X)$, then $g_1g_2\cdots g_{m-1}$ conjugates x to z, where $g_i \in \langle x_i, x_{i+1}\rangle$ for $1 \leq i \leq m-1$. This accounts for the naming of our graphs, since we have, in some sense, local control of fusion between the involutions of X.

The majority of this thesis is concerned with the study of the structure of the local fusion graphs of finite simple groups. From this viewpoint, our main result is the following:

Theorem 1.3. *Let G be a finite simple group, with X a G-conjugacy class of involutions. Then $\mathcal{F}(G,X)$ is connected.*

In light of the Jordan-Holder theorem, finite simple groups can be seen as the 'building blocks' of finite groups. Therefore, to have any hope of understanding local fusion graphs of finite groups in general, it is necessary to have some understanding of the local fusion graphs of finite simple groups. Theorem 1.3 is a first step along this road. There is another nice consequence of Theorem 1.3, which arises through a connection to a famous result.

Theorem 1.4 (Baer-Suzuki)**.** *Let G be a finite group, with X a G-conjugacy class of p-elements. If every pair of elements $x, y \in X$ generates a p-group, then $\langle X \rangle \leq O_p(G)$.*

An elegant proof of this result, which does not rely on the Classification of Finite Simple Groups, may be found in [38]. In recent years a variety of generalisations and analogues of the Baer-Suzuki Theorem have been established. Some such results can be found in [41], [42] and [59]. The relevance of Theorem 1.3 is to a particular subcase of the Baer-Suzuki Theorem.

Theorem 1.5. *Let G be a nonabelian finite group, with X a G-conjugacy class of involutions. If every pair of elements $x, y \in X$ generates a 2-group, then G is not simple.*

Theorem 1.5 is a direct consequence of Theorem 1.4, and is weaker in two ways: firstly, it only considers the case where $p = 2$; and secondly, it does not give specific information about any nontrivial normal subgroup of G. However, our interest in Theorem 1.5 lies in the following restatement:

Theorem 1.5$'$ *Let G be a nonabelian finite group, with X a G-conjugacy class of involutions. If $\mathcal{F}(G, X)$ is totally disconnected, then G is not simple.*

As we shall now see, the hypotheses of Theorems 1.5 and 1.5$'$ are equivalent.

Proof of equivalence. Let G be a nonabelian finite group, with X a G-conjugacy class of involutions. First assume that every pair $x, y \in X$ generates a 2-group. Then certainly every product xy has even order, so $\mathcal{F}(G, X)$ can have no edges, and is therefore totally disconnected. Now assume that $\mathcal{F}(G, X)$ is totally disconnected, and suppose there exist $x, y \in X$ such that xy has order $2^k m$, where $m \neq 1$ is odd. Then $(xy)^k$ has order m. However,

$$(xy)^k = x(yxy \cdots xy) =: xz,$$

and since both x and y are involutions, z is a conjugate of either x or y, so must lie in X. This implies that $\mathcal{F}(G, X)$ has at least one edge, contradicting our assumption that it was totally disconnected. □

It is now apparent that by proving Theorem 1.3, we are generalising Theorem 1.5′ by weakening the hypothesis that $\mathcal{F}(G, X)$ be totally disconnected, to that it simply be disconnected.

The proof of Theorem 1.3 relies on the Classification of Finite Simple Groups.

Theorem 1.6 (CFSG). *Let G be a finite simple group. Then G is isomorphic to one of the following:*

(i) a cyclic group of prime order p;

(ii) an alternating group $\mathrm{Alt}(n)$, where $n \geq 5$;

(iii) a classical group:

linear:	$PSL_n(q)$, $n \geq 2$, *excluding* $PSL_2(2)$ *and* $PSL_2(3)$;
symplectic:	$PSp_{2n}(q)$, $n \geq 2$, *excluding* $PSp_4(2)$;
unitary:	$PSU_n(q)$, $n \geq 3$, *excluding* $PSU_3(2)$;
orthogonal:	$P\Omega_{2n+1}(q)$, $n \geq 3$, q *odd;*
	$P\Omega^+_{2n}(q)$, $n \geq 4$;
	$P\Omega^-_{2n}(q)$, $n \geq 4$

where q is a power p^a of a prime p;

(iv) an exceptional or twisted group of Lie-type:

$$G_2(q), q \geq 3; F_4(q); E_6(q); {}^2E_6(q); {}^3D_4(q); E_7(q); E_8(q)$$

where q is a prime power, or

$$^2B_2(2^{2n+1}), n \geq 1; {}^2G_2(3^{2n+1}), n \geq 1; {}^2F_4(2^{2n+1}), n \geq 1$$

or the Tits group $^2F_4(2)'$*;*

(v) one of 26 *sporadic simple groups:*

- *the five Mathieu group* M_{11}*,* M_{12}*,* M_{22}*,* M_{23}*,* M_{24}*;*
- *the seven Leech lattice groups* Co_1*,* Co_2*,* Co_3*,* M^cL*,* HS*,* Suz*,* J_2*;*
- *the three Fischer groups* Fi_{22}*,* Fi_{23}*,* Fi'_{24}*;*
- *the five Monstrous groups* $\mathbb{M}$, $\mathbb{B}$*,* Th*,* HN*,* He*;*
- *the six pariahs* J_1*,* J_3*,* J_4*,* $O'N$*,* Ly*,* Ru*.*

For each of the groups listed in Theorem 1.6 we verify that Theorem 1.3 holds. This case by case analysis influences the structure of this thesis, with the main purpose of a number of chapters being to prove a subcase of Theorem 1.3 for a specific family of groups. However, in many situtations we are able to go further, and prove more detailed results regarding the structure of our graphs. Let us now give a brief overview of the material we present in each chapter.

In Chapter 2 we investigate the local fusion graphs of symmetric (and alternating) groups. Playing a central role here are 'x-graphs', which characterise the orbits of the local fusion graphs of symmetric groups under the action of an involution centraliser. This approach allows us to give quite detailed information regarding the structure of our graphs, with the main result being the following:

Theorem 1.7. *If* $G = \mathrm{Sym}(n)$*, where* $n \geq 5$*, and* X *is a* G*-conjugacy class of involutions, then* $\mathcal{F}(G, X)$ *is connected, and* $\mathrm{Diam}(\mathcal{F}(G, X)) = 2$*.*

Chapter 3 addresses similar questions for the groups $PSL_2(q)$, and we achieve some comparable results to those for symmetric groups. The key technique here is to utilise the action of $PSL_2(q)$ on the projective line.

Theorem 1.8. *If $G = PSL_2(q)$, where $q \geq 4$, and X is a G-conjugacy class of involutions, then $\mathcal{F}(G, X)$ is connected, and* $\mathrm{Diam}(\mathcal{F}(G, X)) = 2$.

In Chapter 5 we study the local fusion graphs of the sporadic simple groups. Here our approach is rather different. The complex character tables of the sporadic simple groups are known, and can be found in [26]. They are also stored by the computational algebra packages Magma [18] and GAP [36]. Given the character table of a finite group, it is a relatively straightforward calculation to find the number of neighbours of a given vertex of a local fusion graph. Performing these calculations for all the sporadic groups allows us to establish the following result:

Theorem 1.9. *If G is a sporadic simple group with G-conjugacy class of involutions X, then $\mathcal{F}(G, X)$ is connected.*

Chapters 6, 7 and 8 focus on the finite groups of Lie-type. Chapter 6 consists of a review of some properties of classical groups and other groups of Lie-type, touching on algebraic groups, BN-pairs, and the various geometries associated to such groups. This is all in preparation for the analysis of the local fusion graphs of finite, simple groups of Lie-type which follows in Chapters 7 and 8. A number of techniques are used in these chapters, but all working towards the same goal:

Theorem 1.10. *If G is a finite, simple group of Lie-type, with G-conjugacy class of involutions X, then $\mathcal{F}(G, X)$ is connected.*

At this point the proof of Theorem 1.3 will be complete. The remaining chapters of the thesis are concerned with other matters. In Chapter 4 we analyse some local fusion graphs of finite Coxeter groups. The most notable result here concerns the Coxeter groups of type B_n, and in particular shows that local fusion graphs may have arbitrarily large diameter.

Theorem 1.11. *Let $G = C(B_n)$, the Coxeter group of type B_n, where $n \geq 3$. Then G contains a G-conjugacy class of involutions X such that $\mathcal{F}(G, X)$ is connected and* $\mathrm{Diam}(\mathcal{F}(G, X)) = n - 2$.

Our focus shifts in Chapter 9, where we investigate coprimality graphs of symmetric groups. This requires an introduction to the representation theory of finite symmetric groups, which briefly covers Young diagrams, the Hook Formula, and the Murnaghan-Nakayama rule. We then establish some preparatory results regarding the multiplication of pairs of permutations in $\mathrm{Sym}(n)$. Subsequently we prove our main results in this area:

Theorem 1.12. *Suppose that $G = \mathrm{Sym}(n)$ and that x is an element of order p, p a prime. Let X be the G-conjugacy class of x. Then $\mathcal{C}_{p'}(G,X)$ is connected unless $n = 4$ and x has cycle type 2^2.*

Theorem 1.13. *Suppose that $G = \mathrm{Sym}(n)$ and X is the G-conjugacy class of a p-cycle, where p is an odd prime. Then $\mathrm{Diam}(\mathcal{C}_{p'}(G,X)) = 2$ unless $n = 3 = p$ when $\mathrm{Diam}(\mathcal{C}_{p'}(G,X)) = 1$.*

Theorem 1.14. *Suppose that $G = \mathrm{Sym}(n)$ and X is the G-conjugacy class of elements of cycle type p^r, where p is an odd prime. If $r < \sqrt{p}$, then $\mathrm{Diam}(\mathcal{C}_{p'}(G,X)) \leq 5$.*

Theorem 1.15. *Suppose that $G = \mathrm{Sym}(n)$ and X is the G-conjugacy class of elements of cycle type p^r, where $p \geq 5$ is prime. Let k be the least non-negative integer such that $r/2^k \leq \lfloor p \rfloor$. Then $\mathrm{Diam}(\mathcal{C}_{p'}(G,X)) \leq 5 + k$.*

We conclude our work in Chapter 10, where we present a computational algorithm which makes use of local fusion graphs to produce elements of the centraliser of a given involution. Along with its description, there is experimental data and analysis of how the algorithm performs in practice.

1.1 Preliminary Results

Before diving headlong into the world of local fusion graphs, we set up some notation, and prove some elementary results. For the most part our group-theoretic notation is standard, as found in [38]. At times we shall use Atlas notation [26] to denote finite simple groups and their conjugacy classes of involutions. When investigating a local fusion graph defined on a finite group G, we shall usually denote by X the G-conjugacy class of involutions which is the vertex set of our graph $\mathcal{F}(G, X)$. Often we shall analyse the structure of our graph relative to some fixed involution $t \in X$, and we denote by Y the connected component of $\mathcal{F}(G, X)$ which contains t. When working with matrix groups and their associated projective groups, we use H to denote the matrix group, with G usually reserved for the projective group.

We define the *i-th disc* of $\mathcal{F}(G, X)$ relative to $x \in X$ as

$$\Delta_i(x) = \{y \in X : d(x, y) = i\},$$

where $d(,)$ denotes the usual graph metric. Thus $\Delta_0(x) = \{x\}$, while $\Delta_1(x)$ consists of all the neighbours of t in $\mathcal{F}(G, X)$. The following easy lemma will be of use to us.

Lemma 1.16. *Let Γ be a regular graph with $V(\Gamma) = X$. Let $x \in X$. If $|\Delta_1(x)| > |X|/2$ then Γ is connected and* $\mathrm{Diam}(\Gamma) \leq 2$.

Proof. Since $|\Delta_1(x)| > |X|/2$, the regularity of Γ implies connectedness. Suppose there exists $y \in X$ such that $d(x, y) = 3$. Then $\Delta_1(x) \cap \Delta_1(y) = \emptyset$, since otherwise $d(x, y) \leq 2$. Therefore

$$|\Delta_1(x)| \leq |X| - |\Delta_1(y)| = |X| - |\Delta_1(x)|$$

by regularity. Hence $|\Delta_1(x)| \leq |X|/2$, a contradiction. Thus the diameter of Γ is at most 2. $\square$

At times we will wish to break down the vertex set of $\mathcal{F}(G, X)$ into orbits under the action of $C_G(x)$, where $x \in X$. This is motivated by the following lemma, which is easy to verify.

Lemma 1.17. *Let G be a group with G-conjugacy class of involutions X. Suppose $x, y \in X$ are such that $d(x, y) = k$ in $\mathcal{F}(G, X)$. Then for any $g \in C_G(x)$, $d(x, y^g) = k$.*

We shall also need some results regarding local fusion graphs of direct products and normal subgroups, along with centralisers of involutions.

Lemma 1.18. *Let $G = G_1 \times G_2$, where $G_1, G_2 \leq G$, and suppose $X = X_1 \times X_2$ is a G-conjugacy class of involutions, with X_i a G_i-conjugacy class of involutions for $i = 1, 2$. Then $\mathcal{F}(G, X)$ is connected if, and only if, both $\mathcal{F}(G_1, X_1)$ and $\mathcal{F}(G_2, X_2)$ are connected. Moreover if $\mathcal{F}(G_1, X_1)$ and $\mathcal{F}(G_2, X_2))$ have diameters k_1 and k_2 respectively, then* $\mathrm{Diam}(\mathcal{F}(G, X)) = \max\{k_1, k_2\}$.

Proof. Let $t, x \in X$, and write $t = (t_1, t_2)$ and $x = (x_1, x_2)$, where $t_1, x_1 \in X_1$ and $t_2, x_2 \in X_2$. Suppose $\mathcal{F}(G_1, X_1)$ and $\mathcal{F}(G_2, X_2)$ are connected, so there exists a path

$$t_1 \to x_1^{(1)} \to x_1^{(2)} \to \cdots \to x_1^{(r)} = x_1$$

from t_1 to x_1 in $\mathcal{F}(G_1, X_1)$, and a path

$$t_2 \to x_2^{(1)} \to x_2^{(2)} \to \cdots \to x_2^{(s)} = x_2$$

from t_2 to x_2 in $\mathcal{F}(G_2, X_2)$. Without loss of generality we assume that $s \geq r$. Then the following is a path between t and x in $\mathcal{F}(G, X)$:

$$(t_1, t_2) \to (x_1^{(1)}, x_2^{(1)}) \to \cdots \to (x_1^{(r)}, x_2^{(r)}) \to (x_1^{(r)}, x_2^{(r+1)}) \to \cdots \to (x_1^{(r)}, x_2^{(s)}).$$

Since t and x were chosen arbitrarily, this shows that $\mathcal{F}(G, X)$ is connected. The 'only if' statement is proved similarly. Now suppose that $\mathcal{F}(G_1, X_1)$ and $\mathcal{F}(G_2, X_2)$ have diameters k_1 and k_2 respectively, and without loss assume that $k_1 \geq k_2$. Then the method above shows that we can construct a path of length at most k_1 between any two vertices of $\mathcal{F}(G, X)$. Furthermore, it is clear that that if $x = (x_1, x_2)$ is chosen so that $d(t_1, x_1) = k_1$ in $\mathcal{F}(G_1, X_1)$ then $d(t, x) \geq k_1$ in $\mathcal{F}(G, X)$. Thus we deduce that $\mathrm{Diam}(\mathcal{F}(G, X)) = k_1$. □

Lemma 1.19. *If all the local fusion graphs of a group G are connected, then the local fusion graphs of its normal subgroups are also connected.*

Proof. Let $N \lhd G$, with X' an N-conjugacy class of involutions such that $X' \subseteq X$, where X is a G-conjugacy class of involutions. Since N is normal in G, it must be that X is a union of N-conjugacy classes. Suppose that $X \neq X'$. Then we may write $X = X' \cup X''$, where X'' is a union of N-conjugacy classes such that $X' \cap X'' = \emptyset$. By assumption $\mathcal{F}(G, X)$ is connected, and so there must exist $x \in X'$, $y \in X''$ which are adjacent in $\mathcal{F}(G, X)$, and so have odd order product. But if this is the case, then x and y are conjugate in $\langle x, y\rangle$, and as $x, y \in N$ we have $\langle x, y\rangle \leq N$. This contradicts the assumption that $X' \cap X'' = \emptyset$, and so it must be the case that $X = X'$. It follows immediately that $\mathcal{F}(N, X')$ is connected. $\square$

Lemma 1.20. *Suppose G is a group with G-conjugacy class of involutions X such that $X \nsubseteq O_2(G)$. Let $t \in X$. If $C_G(t)$ is a maximal subgroup of G, then $\mathcal{F}(G, X)$ is connected.*

Proof. Denote by Y the connected component of $\mathcal{F}(G, X)$ which contains t. It is well known that a group G acts primitively on a set Ω if, and only if, $C_G(\alpha)$ is a maximal subgroup of G for some $\alpha \in \Omega$ (see [22], for example). It is certainly the case that G acts on the vertex set of any of its local fusion graphs. Moreover, it is straightforward to see that if $\mathcal{F}(G, X)$ is disconnected, then its connected components form a system of imprimitivity for G. Thus if $t \in X$ and $C_G(t)$ is maximal in G, we must either have $Y = \mathcal{F}(G, X)$, whence $\mathcal{F}(G, X)$ is connected, or $|Y| = 1$, so $\mathcal{F}(G, X)$ is totally disconnected. However, in the latter case Theorem 1.4 implies that $X \subseteq O_2(G)$, a contradiction. $\square$

We conclude this opening chapter by proving an important lemma regarding stabilisers of connected components of π-local fusion graphs. To do so we require the following result.

Lemma 1.21. *Let ϕ be an involutary automorphism of H, a group of odd order, and set $I = \{h \in H | h^\phi = h^{-1}\}$. Then $H = C_H(\phi)I$.*

Proof. See [38], Lemma 10.4.1(i). $\square$

Lemma 1.22. *Suppose G is a finite group, with X a G-conjugacy class of involutions, and π some set of non-negative odd integers. Suppose $t \in X$ and let Y be the connected component of $\mathcal{F}_\pi(G, X)$ which contains t. Set $M = \mathrm{Stab}_G(Y)$.*

(i) For all $y \in Y$, $C_G(y) \leq M$, and in particular $\langle Y\rangle \leq M$.

(ii) $Y = t^M$.

(iii) Let $y \in Y$. *If* H *is a* π*-subgroup of* G *which is normalised by* y*, then* $H \leq M$.

Proof. The proof of (i) is clear. Since Y is, by definition, M-invariant under conjugation, $t^M \subseteq Y$. For $y_1, y_2 \in Y$ which are adjacent, y_1 and y_2 are conjugate in $\langle y_1, y_2 \rangle$. So, as $\langle y_1, y_2 \rangle \leq M$ by (i), y_1 and y_2 are M-conjugate. Hence $t^M = Y$, proving (ii). For the final part, by Lemma 1.21, $H = C_H(y)I$ where $I = \{h \in H | h^y = h^{-1}\}$. For $h \in I$, $\langle y, y^h \rangle$ is a dihedral group of order $2o(h)$. Note that y^h is G-conjugate to y and so $y^h \in X$. Also y and y^h are adjacent in $\mathcal{F}_\pi(G, X)$ and thus $y^h \in Y$. By (i), $\langle y, y^h \rangle \leq M$ and hence $h \in M$. Therefore $H = C_H(y)I \leq M$, proving (iii). $\square$

Chapter 2

Symmetric Groups

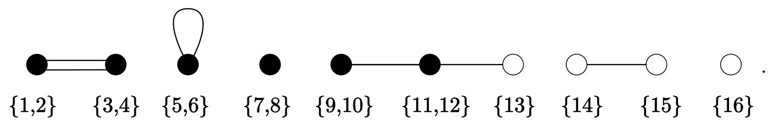
We begin our study by investigating the local fusion graphs of symmetric groups. The conjugacy classes of symmetric groups are of course very well understood, being parametrised by the cycle type of permutations. Also, given two permutations in a symmetric group, the procedure for calculating the product of the permutations is elementary. This being the case, one might hope for relatively complete results on the structure of the local fusion graphs of symmetric groups. These are indeed achievable; however we do require some notation which encapsulates in a diagrammatic form the product of two involutions. This comes in the form of the 'x-graph', which is introduced in Section 2.1. Once in place, this forms the backbone of the proofs of the results in this chapter. In Section 2.2 the diameters of the local fusion graph of the symmetric groups are established, while in Section 2.3 we study in more detail the $C_G(t)$-orbit structure of $\mathcal{F}(G, X)$. Finally, in Section 2.4 we consider the connectedness of various restricted local fusion graphs of symmetric groups. Much of the material in this chapter also appears in [7].

2.1 The x-graph

The concept of the x-graph was first introduced in [10], and the following summary is derived from this source. For the duration of this chapter we let $G = \mathrm{Sym}(n)$, where G acts on $\Omega = \{1, 2, \ldots, n\}$ in the natural way. Let $t = (1, 2)(3, 4) \cdots (m-1, m)$ be an involution in G, and set $X = t^G$. We set

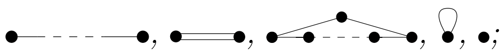
$$\mathcal{V} = \{\{1,2\},\{3,4\},\ldots,\{2m-1,2m\},\{2m+1\},\ldots,\{n\}\}\,.$$

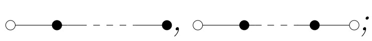
Thus the elements of $\mathcal{V}$ are just the orbits of $\langle t \rangle$ upon Ω. For each $x \in X$, we define the *x-graph (relative to t)*, denoted $\mathcal{G}_x^t$ (or simply $\mathcal{G}_x$ when t is understood), to be the graph with $\mathcal{V}$ as vertex set, and $v_1, v_2 \in \mathcal{V}$ are joined by an edge whenever there exist $\alpha \in v_1$ and $\beta \in v_2$ with $\alpha \neq \beta$ for which $\{\alpha, \beta\}$ is a $\langle x \rangle$-orbit. Additionally the vertices of $\mathcal{G}_x^t$ corresponding to 2-cycles of t will be coloured black ($\bullet$) and the other vertices white ($\circ$). Therefore $\mathcal{G}_x^t$ has m black vertices and $n-2m$ white vertices. Note that the edges in $\mathcal{G}_x^t$ are in one-to-one correspondence with the 2-cycles of x. So the number of edges in $\mathcal{G}_x^t$ is the same as the number of black vertices. As an example, taking $n = 16$, $t = (1,2)(3,4)(5,6)(7,8)(9,10)(11,12)$ and $x = (1,3)(2,4)(5,6)(9,11)(12,13)(14,15)$, $\mathcal{G}_x$ looks like

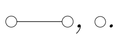


Notice that each black vertex in an x-graph has valency at most two, while a white vertex has valency at most one. From this we have the following result.

Lemma 2.1. *For $x \in X$, the possible connected components of $\mathcal{G}_x$ are*

(i) 

(ii)  *and*

(iii) 

Suppose for $x \in X$ the connected components of $\mathcal{G}_x$ are $C_1, C_2, \ldots, C_l$, and for each such component let x_i and t_i be the corresponding parts of x and t. Observe that for $i \neq j$ both t_i and x_i commute with both t_j and x_j. So in the above example, $l = 6$ with $t_1 = (1,2)(3,4)$, $t_2 = (5,6)$, $t_3 = (7,8)$, $t_4 = (9,10)(11,12)(13)$, $t_5 = (14)(15)$, $t_6 = (16)$, and $x_1 = (1,3)(2,4)$, $x_2 = (5,6)$, $x_3 = (7)(8)$, $x_4 = (9,11)(12,13)(10)$, $x_5 = (14,15)$, $x_6 = (16)$.

The next lemma captures the properties of the x-graph which will be important for our purposes.

Lemma 2.2. *(i) Every graph with b black vertices of valency at most two, $n-2b$ white vertices of valency at most one, and exactly b edges is the x-graph for some $x \in X$.*

(ii) If $x, y \in X$, then x and y are in the same $C_G(t)$-orbit if and only if $\mathcal{G}_x$ and $\mathcal{G}_y$ are isomorphic graphs (where isomorphisms preserve the colour of vertices).

(iii) Let $C_1, C_2, \ldots, C_l$ be the connected components of $\mathcal{G}_x$. Assume that x_i and t_i are the corresponding parts of x and t, and let b_i, w_i and c_i be, respectively, the number of black vertices, white vertices and cycles in C_i. Then

(a) the order of tx is the least common multiple of the orders of t_ix_i, $i = 1, \ldots, l$; and

(b) for $i = 1, \ldots, l$, the order of t_ix_i is $(2b_i + w_i)/(c_i + 1)$.

Proof. The proof may be found in [10]. □

2.2 The diameter of $\mathcal{F}(G, X)$

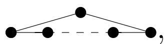
In this section we prove the following:

Theorem 2.3. *Let $G = \mathrm{Sym}(n)$, where $n \geq 5$, and let X be a G-conjugacy class of involutions. Then $\mathcal{F}(G, X)$ is connected, and $\mathrm{Diam}(\mathcal{F}(G, X)) = 2$.*

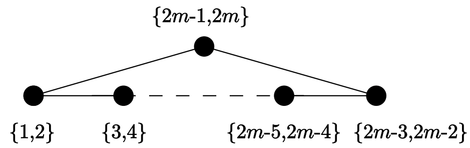
When $n = 2$, $\mathcal{F}(G, X)$ consists of a single vertex, and when $n = 3$, $\mathcal{F}(G, X)$ is the complete graph on 3 vertices. Finally, when $n = 4$ and $X = (1, 2)^G$, $\mathcal{F}(G, X)$ is connected with diameter 2, and when $X = (1, 2)(3, 4)^G$, $\mathcal{F}(G, X)$ is the totally disconnected graph on three vertices.

Theorem 2.3 is perhaps not a surprising result. As the conjugacy classes of symmetric groups are in some sense as 'big as possible', if any family of groups is to have local fusion graphs of low diameter, the family of symmetric groups is the most likely.

Proof of Theorem 2.3. For $n \leq 16$, Magma [18] makes relatively short work of checking that $\mathcal{F}(G, X)$ has diameter two. So we may assume $n > 16$. Let t be a fixed element of X. We proceed by induction on n. Let $x \in X$. We aim to show that $d(t, x) \leq 2$. Since there are plainly $x \in X$ for which $d(t, x) > 1$, this would prove that $\mathrm{Diam}(\mathcal{F}(G, X)) = 2$.

(3.1) If $\mathcal{G}_x$ is , then $d(t, x) \leq 2$.

Assume, without loss of generality, that $t = (1, 2)(3, 4), \ldots, (2m-1, 2m)$. So $\mathcal{G}_x$ has m black vertices. If m is odd, then tx has odd order by Lemma 2.2, and so $d(t, x) \leq 1$. While if m is even, we assume that $\mathcal{G}_x$ is labelled like so



,

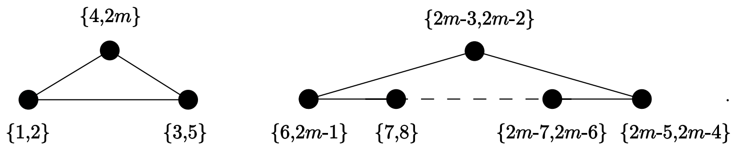
and that

$$x = (1, 2m)(2, 3)(4, 5) \ldots (2m-4, 2m-3)(2m-2, 2m-1).$$

We select

$$y = (1, 2)(3, 5)(4, 2m)(6, 2m-1)(7, 8)(9, 10) \ldots (2m-3, 2m-2).$$

Then $ty = (3, 2m, 6)(4, 5, 2m-1)$, and hence $y \in \Delta_1(t)$. Now $\mathcal{G}_x^y$ is seen to be



.

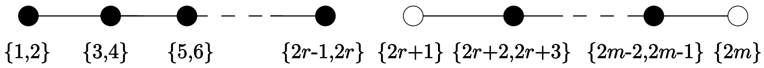
Since the two connected components of $\mathcal{G}_x^y$ have sizes 3 and $m-3$, both of which are odd, Lemma 2.2(iii) implies that yx has odd order. Therefore $x \in \Delta_1(y)$ and so (3.1) holds.

(3.2) If $\mathcal{G}_x$ is , then $d(t, x) = 1$.

Since $\mathcal{G}_x$ is a connected component with one white vertex, (3.2) follows from Lemma 2.2(iii).

(3.3) If $\mathcal{G}_x$ is , then $d(t,x) \leq 2$.

Without loss we may label $\mathcal{G}_x$ as follows



where

$$t = (1,2)(3,4)(5,6)\dots(2r-1,2r)(2r+1)(2r+2,2r+3)\dots(2m-2,2m-1)(2m).$$

We may assume that

$$x = (2,3)(4,5)\dots(2r-2,2r-1)(2r+1,2r+2)\dots(2m-1,2m).$$

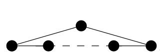
Set $t_0 = (1,2)t$ and $x_0 = x(2m-1,2m)$. Then t_0 and x_0 are H-conjugate (where $H = \mathrm{Sym}(\Omega \setminus \{1,2m\})$). Observing that $\mathcal{G}_{x_0}^{t_0}$ (thinking of t_0, x_0 as involutions in H) has two connected components of type we deduce from Lemma 2.2(iii) that t_0x_0 has odd order. Let $y = (1,2m)t_0$. Then $y \in X$ and

$$ty = (1,2)t_0(1,2m)t_0 = (1,2)(1,2m) = (1,2,2m),$$

whence $y \in \Delta_1(t)$. Also, as t_0 and x_0 fix 1 and $2m$,

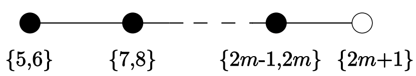
$$\begin{aligned} yx &= (1,2m)t_0x_0(2m-1,2m) \\ &= t_0x_0(1,2m)(2m-1,2m) \\ &= t_0x_0(1,2m-1,2m). \end{aligned}$$

Now $t_0x_0 \in H$ is a product of two disjoint odd cycles of lengths, say, m_1, m_2. If $2m-1$ is in say the latter cycle of t_0x_0, then tx is a disjoint product of an m_1-cycle and an (m_2+2)-cycle. Thus yx has odd order and so $x \in \Delta_1(y)$. Therefore $d(t,x) \leq 2$, which proves (3.3).

Suppose that $\mathcal{G}_x$ contains no connected components of shape . Then by induction and Lemma 2.1 $\mathcal{G}_x$ must be either , or (allowing as a possibility in the latter connected component). Hence $d(t, x) \leq 2$ by (3.1), (3.2) and (3.3). It therefore remains to analyse $\mathcal{G}_x$ when it has connected components of shape . If there are an even number of connected components, then, as the fusion graphs for Sym(8) have diameter two, by pairing them up and using induction we obtain our result. Thus we may assume $\mathcal{G}_x$ contains exactly one connected component. Let $\mathcal{H}_x$ denote the union of all the other connected components of $\mathcal{G}_x$. Also we may assume $t = (1,2)(3,4)t_0$, $x = (1,3)(2,4)x_0$ where t_0 and x_0 are involutions in $H = \mathrm{Sym}(\Omega \setminus \{1,2,3,4\})$.

Let $\mathcal{C}_x$ be a subgraph of $\mathcal{H}_x$, where $\mathcal{C}_x$ is one of , , , , and . Then $t_0 = t_1t_2$, $x_0 = x_1x_2$ where t_1, x_1 are the parts in $\mathcal{C}_x$ and t_2, x_2 the parts in $\mathcal{H}_x \setminus \mathcal{C}_x$. Then t_2 and x_2 are conjugate involutions in some symmetric subgroup of G and the x_2-graph (with respect to t_2) is $\mathcal{H}_x \setminus \mathcal{C}_x$. Since $\mathcal{H}_x$ contains no subgraph we can find y_2 in this conjugacy class such that t_2y_2 and y_2x_2 have odd order. Since y_2 commutes with both $(1,2)(3,4)t_1$ and $(1,3)(2,4)x_1$, without loss we may assume $\mathcal{H}_x = \mathcal{C}_x$. We now work through the possibilities for $\mathcal{H}_x$ making repeated use of Lemma 2.2(iii) to show $d(t, x) \leq 2$. The first three possibilities listed above do not need attention as $n \geq 16$.

If $\mathcal{H}_x$ is



,

then

$$t = (1,2)(3,4)(5,6)(7,8)\ldots(2m-1,2m)(2m+1)$$

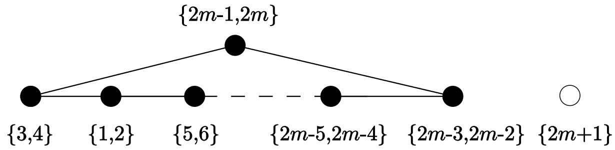
and, without loss of generality,

$$x = (1,3)(2,4)(5)(6,7)(8,9)\ldots(2m,2m+1).$$

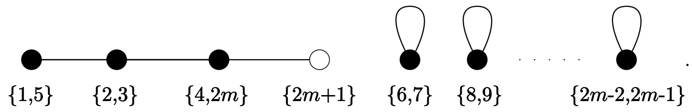
In the case when m is odd, we select

$$y = (1,5)(2,3)(4,2m)(6,7)(8,9)\ldots(2m-2,2m-1)(2m+1),$$

and then $\mathcal{G}_y$ is



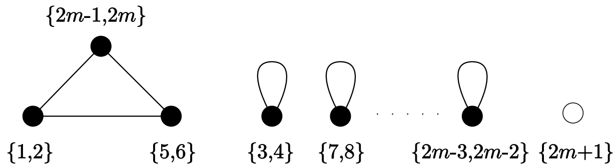
while $\mathcal{G}_x^y$ is



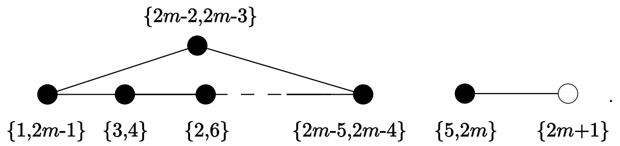
If m were to be even, instead we choose

$$y = (1, 2m - 1)(2, 6)(3, 4)(5, 2m)(7, 8)(9, 10) \dots (2m - 3, 2m - 2)$$

which gives $\mathcal{G}_y$ as

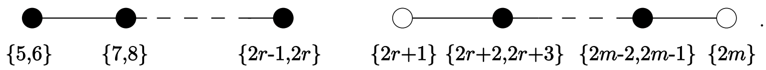


and $\mathcal{G}_x^y$ as



Thus in each case we have $d(t, x) = 2$, as required.

Now we examine the case when $\mathcal{H}_x$ is



So

$$t = (1, 2)(3, 4)(5, 6) \dots (2r - 1, 2r)(2r + 1)(2r + 2, 2r + 3) \dots (2m - 2, 2m - 1)(2m)$$

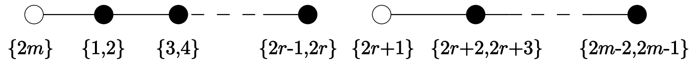
and

$$x = (1, 3)(2, 4)(5)(6, 7)(8, 9) \dots (2r - 2, 2r - 1)(2r)(2r + 1, 2r + 2) \dots (2m - 1, 2m).$$

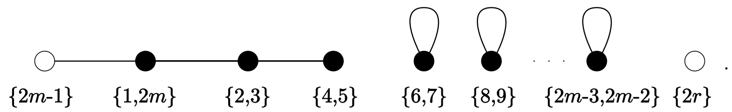
Choosing

$$y = (1, 2m)(2, 3)(4, 5) \dots (2r - 2, 2r - 1)(2r + 1, 2r + 2) \dots (2m - 3, 2m - 2),$$

we observe that $\mathcal{G}_y$ is

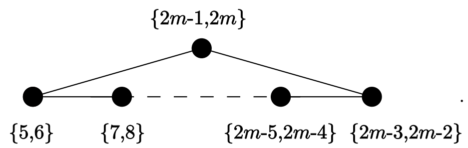


and $\mathcal{G}_x^y$ is



Therefore we again have $d(t, x) = 2$.

Finally, we consider when $\mathcal{H}_x$ is



Thus

$$t = (1, 2)(3, 4)(5, 6)(7, 8) \ldots (2m - 1, 2m)$$

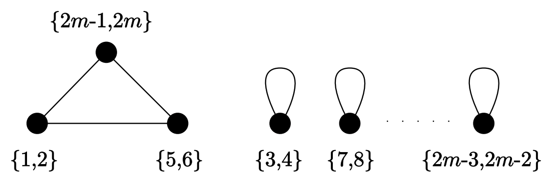
and, without loss,

$$x = (1, 3)(2, 4)(6, 7)(8, 9) \ldots (2m, 5).$$

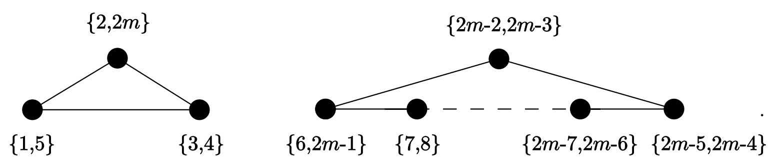
When m is even we select

$$y = (1, 5)(2, 2m)(3, 4)(6, 2m - 1)(7, 8)(9, 10) \ldots (2m - 3, 2m - 2)$$

and as a result $\mathcal{G}_y$ is



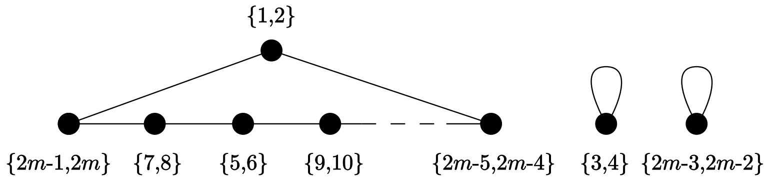
and $\mathcal{G}_x^y$ is



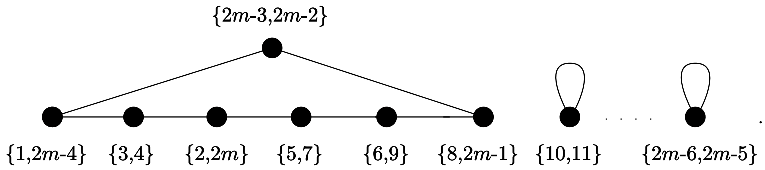
Before dealing with m odd we recall that we are assuming $n(= 2m) \geq 16$. So $2m - 4 > 10$ and therefore the choice we now make gives us an element of X. Take

$$\begin{aligned} y \;=\; & (1, 2m - 4)(2, 2m)(3, 4)(5, 7)(6, 9)(8, 2m - 1)(10, 11)(12, 13) \ldots \\ & \ldots (2m - 6, 2m - 5)(2m - 3, 2m - 2). \end{aligned}$$

Hence $\mathcal{G}_y$ is



and $\mathcal{G}_x^y$ is

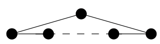


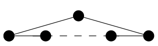
So once more have $d(t, x) = 2$.

Having successfully dealt with all the possibilities for $\mathcal{H}_x$, the proof of Theorem 2.3 is complete. $\square$

2.3 The $C_G(t)$-orbit structure of $\mathcal{F}(G, X)$

Our aim in this section is to obtain an expression for the size of a given $C_G(t)$-orbit in $\Delta_1(t)$. It is relatively straightforward to adapt the methods of [10], where the corresponding goal was achieved for commuting involution graphs. Again, the x-graph lies at the heart of the analysis. The next lemma follows immediately from Lemma 2.2.

Lemma 2.4. *Let $x \in X$. Then $x \in \Delta_1(t) \cup \{t\}$ if and only if each component of $\mathcal{G}_x$ is one of* ○, , *and*  *(where the number of vertices in the final component must be odd).*

Proposition 2.5. *Let $x \in \Delta_1(t)$. Suppose that $\mathcal{G}_x$ contains p components of type* , *labelled $1, \ldots, p$, and q components of type* , *labelled $p+1, \ldots, p+q$. Also assume $\mathcal{G}_x$ has l loops*  *and s single white vertices* ○, *labelled $p+q+1, \ldots, p+q+l$ and $p+q+l+1, \ldots, p+q+l+s$ respectively. For $i = 1, \ldots, p+q$ let m_i be the number of black vertices in component i. Set $M_1 = m$, and write $M_i = m - (m_1 + \cdots + m_{i-1})$. Then the number of elements $\mathcal{O}$ in the $C_G(t)$-orbit of*

x is

$$\mathcal{O} = abcd,$$

where

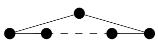
$$a = \prod_{i=1}^{p} \binom{M_i}{m_i} (2m_i - 2)(2m_i - 4)\cdots 2,$$

$$b = \prod_{i=p+1}^{p+q} \binom{M_i}{m_i} (r + p + 1 - i) 2m_i(2m_i - 2)\cdots 2,$$

$$c = \binom{m - (m_1 + \cdots + m_{p+q})}{l}$$

and

$$d = \binom{r - q}{s}.$$

Proof. First consider a component of $\mathcal{G}_x$ of type , where

$$t = (1, 2)(3, 4)\cdots(2m_i - 1, 2m_i).$$

We wish to find an element x with this x-graph. The image of 1 under x cannot be 1 or 2, but anything else is a possible, giving $2m_i - 2$ choices for 1^x. Without loss of generality we may choose $1^x = 3$. Now 3^x cannot be $1, 2, 3$ or 4, but anything else is possible, giving $2m_i - 4$ choices for 3^x. Continuing in this manner, we see there are

$$(2m_i - 2)(2m_i - 4)(2m_i - 6)\cdots 4 \cdot 2$$

choices in total for x.

Now consider a component of $\mathcal{G}_x$ of type , and suppose

$$t = (1, 2)(3, 4)\cdots(2m_i - 1, 2m_i)(2m_i + 1).$$

To get an x-graph of the required type, x must fix exactly one point in $\{1, \ldots, 2m_i\}$. Without loss of generality let this point be 1. Then, arguing as above, there are $2m_i - 2$ choices for 2^x, and so on, which gives

$$2m_i(2m_i - 2)(2m_i - 4)\cdots 4 \cdot 2$$

choices in total.

Next, observe that there are $\binom{m}{m_1}$ choices for the black vertices in the first component, then $\binom{m-m_1}{m_2} = \binom{M_2}{m_2}$ choices for the black vertices in the second component, and so on. When we reach component $p+1$ there are $\binom{M_{p+1}}{m_{p+1}}$ choices for the black vertices, and r choices for the single white vertex, and so on. When we reach loops and single white vertex components we are simply choosing one vertex from those vertices remaining which are, respectively, black and white. Putting all this together gives the desired expression for $|\Delta_1(t)|$. $\square$

2.4 Connectedness when π is restricted

Here we present a proof of a result, due to Peter Rowley, which shows the relatively minor role the set π plays in determining whether or not $\mathcal{F}_\pi(G, X)$ is connected.

Theorem 2.6 (Rowley). *Suppose that $G = \mathrm{Sym}(n)$, X is a G-conjugacy class of involutions and π is a set of odd positive integers. Then $\mathcal{F}_\pi(G, X)$ is either totally disconnected or connected.*

The proof of this theorem makes use of the following classical result due to Jordan (see [47]):

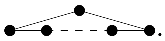
Theorem 2.7 (Jordan). *Let G be a primitive permutation group on a finite set Ω, and suppose that G has a subgroup H which fixes at least one point of Ω and is transitive on* $\mathrm{supp}(H)$. *Then G acts 2-transitively on Ω.*

Proof of Theorem 2.6. We argue by induction on n, with $n = 1$ clearly holding. Assume that $\mathcal{F}_\pi(G, X)$ is not totally disconnected, and let $t \in X$ be such that Y, the connected component of t in $\mathcal{F}_\pi(G, X)$, has $|Y| > 1$. Put $K = \mathrm{Stab}_G(Y)$. If $K = G$, then $Y = X$ and hence $\mathcal{F}_\pi(G, X)$ is connected. So we now suppose $K \neq G$, and argue for a contradiction.

Let $x \in Y$ with $d(t, x) = 1$. Then $z = tx$ has order in the set π, and we have

(5.1) $\langle C_G(t), C_G(x)\rangle \leq K$, and

(5.2) $\mathrm{supp}(t) \cup \mathrm{supp}(x) = \Omega$.

If (5.2) is false, then t and x both fix some $\alpha \in \Omega$. So $t, x \in G_\alpha \cong \mathrm{Sym}(n-1)$. Since t and x are G_α-conjugate and the order of tx is in π, by induction $\mathcal{F}_\pi(G_\alpha, X \cap G_\alpha)$ is connected. Therefore $G_\alpha \leq K$, and so, as $K \neq G$ and G_α is a maximal subgroup of G, $K = G_\alpha$. If t fixes a further element of Ω, say β, then, by (5.1), $(\alpha, \beta) \in C_G(t) \leq K$, contrary to $K = G_\alpha$. So t (and hence also x) fixes only α. Thus $\mathcal{G}_x$ has only one white node (namely $\{\alpha\}$) with the remaining connected components being either  or . Without loss we assume $\alpha = n$.

Suppose that $\mathcal{G}_x$ has  as a component. So, without loss of generality,

$$t = (1,2)(3,4)\cdots(n-2,n-1) = (1,2)t_1$$

and $x = (1,2)x_1$, where $x_1 \in \mathrm{Sym}(\{3,4,\ldots,n-1\})$.If we set $H = \mathrm{Sym}(\{3,4,\ldots,n-1\})$, then $t_1, x_1 \in H$, with t_1 and x_1 being H-conjugate involutions and the order of t_1x_1, being the same as that of tx, lies in π. Using induction again we infer that $\mathcal{F}_\pi(H, X')$ is connected, where $X' = t_1^H$. Hence, in $\mathcal{F}_\pi(H, X')$ there is a path from t_1 to

$$s_1 = (3,4)(5,6)\cdots(n-4,n-3)(n-1,n),$$

say $t_1 = y_0, y_1, \ldots, y_m = s_1$ $(y_i \in X')$. Consequently

$$t = (1,2), t_1 = (1,2)y_0, (1,2)y_1, \ldots, (1,2)y_m = (1,2)s_1$$

is a path in $\mathcal{F}_\pi(G, X)$ from t to

$$(1,2)(3,4)(5,6)\cdots(n-4,n-3)(n-1,n).$$

But then $(n-1, n) \in K$, whereas $K = G_\alpha$. This rules out  as being a connected component of $\mathcal{G}_x$.

Let $t = t_1t_2\cdots t_k$ and $x = x_1x_2\cdots x_k$, where

$$\begin{aligned}
t_1 &= (1,2)\cdots(l_1-1,l_1),\\
t_2 &= (l_1+1,l_1+2)\cdots(l_1+l_2-1,l_1+l_2),\\
&\ \ \vdots
\end{aligned}$$

and

$$\begin{aligned} x_1 &= (2,3)(4,5)\cdots(l_1-2,l_1-1)(1,l_1), \\ x_2 &= (l_1+2,l_1+3)\cdots(l_1+l_2-2,l_1+l_2-1)(l_1+1,l_1+l_2), \\ &\vdots \end{aligned}$$

So $x_1, x_2, \ldots$ correspond to the connected components of $\mathcal{G}_x$. Set $l = l_1$. A calculation gives

$$t_1x_1 = (1,3,5,\ldots,l-1)(l,l-2,\ldots,2),$$

and thus t_1x_1 has order $m = (l-1)/2$. Now the order of $z = tx$ is the least common multiple of the orders of $t_1x_1, t_2x_2, \ldots, t_kx_k$, whence m must be odd. Put

$$w = (n, l-m+1, l-m+3, \ldots, l-m+4, l-m+2).$$

Then w is a cycle of length m, and so of order m. Further (by design) $w^{t_1} = w^{-1}$ and hence

$$y_1 = t_1w = (1,2)(3,4)\cdots(l-m+1,n)\cdots(l-m+2,l-m+3)$$

is conjugate to t_1. Also, of course, $t_1y_1 = w$ has order m. So $y = y_1t_2\cdots t_k \in X$ and the order of ty is the same as that of tx. Therefore $y \in Y$ and hence $(l-m+1,n) \in K$. This contradicts the earlier deduction that $K = G_\alpha$, and with this we have proven (5.2).

(5.3) K acts transitively, but not primitively, on Ω.

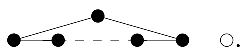
Since $C_G(t)$ and $C_G(x)$ have shape $2^k\mathrm{Sym}(2k)\times\mathrm{Sym}(n-2k)$, where $k = |\mathrm{supp}(t)|/2$, and t and x do not commute, (5.1) and (5.2) imply that K is transitive on Ω. Plainly $C_G(t)$, and hence K, contains transpositions. So, if K were to act primitively, then Theorem 2.7 would force $K = G$, contrary to $K \neq G$. Thus (5.3) holds.

By (5.3) we may choose a nontrivial block Λ for K with $\alpha \in \Lambda \cap \mathrm{supp}(t)$. If $\Lambda \not\subseteq \mathrm{supp}(t)$, then the action of $C_G(t)$ on Ω results in $\Lambda = \Omega$. Thus $\Lambda \subseteq \mathrm{supp}(t)$. Again, using the action of $C_G(t)$ on Ω we deduce that either $\Lambda = \mathrm{supp}(t)$ or $\Lambda = \{\alpha, \beta\}$

where $\beta = \alpha^t$. Since t and x do not commute, we may further assume that $\alpha \in \text{supp}(t)$ is such that $\alpha^x \notin \{\alpha, \beta\}$. So $\alpha \in \text{supp}(x)$ and a similar argument yields that either $\Lambda = \text{supp}(x)$ or $\Lambda = \{\alpha, \alpha^x\}$. In view of (5.2) this then implies that $\Lambda = \Omega$, contrary to Λ being a nontrivial block. With this contradiction the proof is complete. $\square$

The preceding result shows that no matter how small the set π is chosen to be, if there are any edges in $\mathcal{F}_\pi(G, X)$ then the graph is in fact connected. This prompts the following question: to what extent does this statement hold true when the connectivity condition is restricted further? For example, does this hold when we choose to join $t, x \in X$ with an edge if and only if the x-graph is of a particular isomorphism type? The answer, as we shall presently see, is no.

Proposition 2.8. *Let $G = \text{Sym}(n)$, where $n = 2m+1$ and $m \geq 3$ is odd. Let X be the G-conjugacy class of elements with cycle type 2^m. Let $\overline{\mathcal{F}}_{\{m\}}(G, X)$ be the subgraph of $\mathcal{F}_{\{m\}}(G, X)$ given by joining vertices x and y if and only if $\mathcal{G}_x^y$ has type*



Then $\overline{\mathcal{F}}_{\{m\}}(G, X)$ is disconnected, with exactly $2m+1$ connected components.

Proof. Without loss of generality suppose that for $x \in X$ we have

$$\text{supp}(x) = \{1, \ldots, 2m\}.$$

Note that if $d(x, y) = 1$ then $\mathcal{G}_x^y$ must have a single white vertex corresponding to the point $2m+1$, so y must fix $2m+1$. Thus x can be connected only to involutions in $X \cap H$, where $H = \text{Stab}_G(\{2m+1\})$. This implies that $\overline{\mathcal{F}}_{\{m\}}(G, X)$ is disconnected, with at least $2m+1$ connected components. But notice that $\overline{\mathcal{F}}_{\{m\}}(H, H \cap X) \cong \mathcal{F}_{\{m\}}(H, H \cap X)$, and since the latter graph is not totally disconnected, by Theorem 2.6 it must be connected. Thus $\overline{\mathcal{F}}_{\{m\}}(G, X)$ has exactly $2m+1$ components. $\square$

Chapter 3

Linear Groups of Small Dimension

In this chapter we investigate the local fusion graphs of projective special linear groups of dimension 2. As in the case with symmetric groups, we are able to determine the diameter of our graphs in these cases. Our ability to do this relies on the action of such linear groups on the projective line, and the clarity this lends to the group properties which are relevant to our study. We begin by briefly reviewing the definition and some elementary facts about the linear groups, before presenting the results.

3.1 A brief review

Let K be any field. The *general linear group* $GL_n(K)$ is defined to be the group of all invertible $n \times n$ matrices over K. Since K is a field, the requirement that a matrix $A \in \mathbb{M}_n(K)$ be invertible is equivalent to the determinant $\det(A)$ being nonzero. The *special linear group* $SL_n(K)$ is the subgroup of $GL_n(K)$ consisting of all $A \in GL_n(K)$ with $\det(A) = 1$. As this subgroup is the kernel of the determinant homomorphism, $SL_n(K)$ is in fact a normal subgroup of $GL_n(K)$. It is easily seen that the centre of $GL_n(K)$ is precisely the set of scalar matrices in $GL_n(K)$, that is

$$Z(GL_n(K)) = \{\lambda I_n : \lambda \in K^*\}.$$

Thus the centre of $SL_n(K)$ is the subgroup of $Z(GL_n(K))$ consisting of the matrices with determinant equal to 1, so

$$Z(SL_n(K)) = \{\lambda I_n : \lambda^n = 1\}.$$

Since the centre of a group is a normal subgroup, we may form the factor groups

$$PGL_n(K) := GL_n(K)/Z(GL_n(K))$$

and

$$PSL_n(K) := SL_n(K)/Z(SL_n(K)),$$

which we call the *projective general linear group* and *projective special linear group* respectively. It turns out that the latter of these is usually a simple group.

Being matrix groups, $GL_n(K)$ and $SL_n(K)$ act naturally on an n-dimensional vector space $V \cong K^n$. Indeed, given an n-dimensional vector space V over K, the group of invertible linear transformations $GL(V)$ of V is isomorphic to $GL_n(K)$. Since the elements of these groups are linear transformations, $GL_n(K)$ and $SL_n(K)$ also act on the set of all 1-dimensional subspaces of V. When $n = 2$ this set is called the *projective line* over K. If K is a finite field, say $K = \mathbb{F}_q$ where $q = p^r$ for a prime p, the projective line is a finite set which we denote $P(q)$, and consists of the spans of the following vectors:

$$\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}\alpha_2\\1\end{pmatrix}, \ldots, \begin{pmatrix}\alpha_{p-1}\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix},$$

where $\{0, 1, \alpha_2, \ldots, \alpha_{p-1}\}$ is the set of elements of $\mathbb{F}_q$. Hence $|P(q)| = q+1$. We label each span by the upper entry of each representative vector, except in the case of $\binom{1}{0}$ which we label ∞. Thus

$$P(q) = \{0, 1, \alpha_2, \ldots, \alpha_{p-1}, \infty\}.$$

In general, the actions of $GL_2(q)$ and $SL_2(q)$ on the projective line are not faithful. Certainly any scalar matrix in $GL_2(q)$ acts trivially on $P(q)$. Conversely, suppose $A \in GL_2(q)$ fixes every element of $P(q)$. Then in particular both 0 and ∞ are fixed, so A must be a diagonal matrix, say $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, but now since 1 is also fixed we deduce that $a = b$, so A is a scalar matrix. Thus the kernels of the actions of $GL_n(q)$ and $SL_n(q)$ on $P(q)$ are the centres of these respective groups, and consequently we have faithful actions of both $PGL_2(q)$ and $PSL_2(q)$ on $P(q)$. Therefore $PGL_2(q)$ and $PSL_2(q)$ may be considered as permutation groups on $P(q)$.

3.2 The local fusion graphs of $PSL_2(q)$

Our aim is to prove the following result:

Theorem 3.1. *Let $G = PSL_2(q)$, where $q \neq 3$, with X a G-conjugacy class of involutions. Then $\mathcal{F}(G, X)$ is connected, with* $\mathrm{Diam}(\mathcal{F}(G, X)) = 2$.

Given a finite group G with G-conjugacy class of involutions X, the *commuting involution graph* $\mathcal{C}(G, X)$ has X as its vertex set, with $x, y \in X$ joined by an edge if, and only if, $x \neq y$ and x commutes with y. Commuting involutions graphs for the groups $PSL_2(q)$ have been investigated in [13]. This work shall be of particular use to us, as the next result indicates.

Proposition 3.2. *Let G be a finite group containing a unique conjugacy class of involutions X. For $t \in X$ denote by $\Delta_i(t)$ the discs of the local fusion graph $\mathcal{F}(G, X)$, and by $\Delta_i^{\mathcal{C}}(t)$ the discs of the commuting involution graph $\mathcal{C}(G, X)$. Then $\Delta_j^{\mathcal{C}}(t) \subseteq \Delta_1(t)$ for all $j \geq 3$.*

Proof. We prove the contrapositive statement. Let $x \in X$, with $x \neq t$ and $x \notin \Delta_1(t)$. Then $o(tx) = 2^k m$ for some k, m where $k \geq 1$ and m is odd. Consequently, the dihedral group $\langle t, x \rangle$ has order divisible by 4, and thus contains a central involution y. But now $t \to y \to x$ is a path from t to x in $\mathcal{C}(G, X)$ of length 2, which implies $d(t, x) \leq 2$ in $\mathcal{C}(G, X)$. Thus either $x \in \Delta_1^{\mathcal{C}}(t)$ or $x \in \Delta_2^{\mathcal{C}}(t)$. $\square$

In [13], the disc sizes of the commuting involution graphs for $PSL_2(q)$ are calculated. For convenience we now restate Theorem 1.1 of [13].

Theorem 3.3. *Suppose $G = PSL_2(q)$, with X a G-conjugacy class of involutions.*

(i) If q is even, then $\mathcal{C}(G, X)$ consists of $q + 1$ cliques each with $q - 1$ vertices.

(ii) If $q \equiv 3 \bmod 4$, with $q > 3$, then $\mathcal{C}(G, X)$ is connected and $\mathrm{Diam}(\mathcal{C}(G, X)) = 3$. *Furthermore*

$$\begin{aligned} |\Delta_1^{\mathcal{C}}(t)| &= (q+1)/2; \\ |\Delta_2^{\mathcal{C}}(t)| &= (q+1)(q-3)/4; \textit{ and} \\ |\Delta_3^{\mathcal{C}}(t)| &= (q+1)(q-3)/4. \end{aligned}$$

(iii) If $q \equiv 1 \bmod 4$, with $q > 13$, then $\mathcal{C}(G, X)$ is connected and $\mathrm{Diam}(\mathcal{C}(G, X)) = 3$. *Furthermore*

$$\begin{aligned} |\Delta_1^{\mathcal{C}}(t)| &= (q-1)/2; \\ |\Delta_2^{\mathcal{C}}(t)| &= (q-1)(q-5)/4; \textit{ and} \\ |\Delta_3^{\mathcal{C}}(t)| &= (q-1)(q+7)/4. \end{aligned}$$

We can now put this to good use to partially prove Theorem 3.1 with very little effort.

Proposition 3.4. *Let $G \cong PSL_2(q)$, where $q \equiv 1 \bmod 4$. Let X be the unique conjugacy class of involutions of G. Then $\mathcal{F}(G, X)$ is connected and has diameter* 2.

Proof. For $q \leq 13$, we verify using MAGMA. So assume $q > 13$, and let $t \in X$. From [13] we have that $|X| = q(q+1)/2$, and there are clearly elements of X which are not adjacent to t.

By Theorem 3.3(iii) we have that $|\Delta_3^{\mathcal{C}}(t)| = (q-1)(q+7)/4$, and by Proposition 3.2 $\Delta_3^{\mathcal{C}}(t) \subseteq \Delta_1(t)$. Therefore, $|\Delta_1(t)| \geq (q-1)(q+7)/4$. Since $q > 13$, we deduce that $|\Delta_1(t)| > |X|/2$, and so by Lemma 1.16, $\mathcal{F}(G, X)$ is connected and has diameter 2. □

Proposition 3.5. *Let $G \cong PSL_2(q)$, where $q \geq 4$ is even. Let X be the unique conjugacy class of involutions of G. Then $\mathcal{F}(G, X)$ is connected and has diameter* 2.

Proof. For q even, $|X| = q^2 - 1$, and the only elements of even order in G are involutions. Hence, for $t, x \in X$, the order of the product tx is either odd, or t and

x commute. We deduce that the elements of $X - \Delta_1(t)$ are precisely the involutions in $C_G(t)$.

For $PSL_2(q)$ with q even, the centraliser of an involution is a Sylow 2-subgroup, which contains $q-1$ non-identity elements. By our earlier observation, all these elements must be involutions. But now,

$$\begin{aligned} |\Delta_1(t)| &= (q^2-1)-(q-1) \\ &= q^2-q \\ &> (q^2-1)/2 \\ &= |X|/2 \end{aligned}$$

since $q \geq 4$.

Thus, by Lemma 1.16, $\mathcal{F}(G, X)$ is connected and $\mathrm{Diam}(\mathcal{F}(G, X)) \leq 2$. But there are clearly vertices in $\mathcal{F}(G, X)$ which are not adjacent to t, so the result follows. □

Corollary 3.6. *For G, X as above, if $t \in X$ then*

$$|\Delta_1(t)| = q(q-1) \qquad \textit{and} \qquad |\Delta_2(t)| = q-2.$$

Proof. This follows immediately from proof of Proposition 3.5. □

When $q \equiv 3 \bmod 4$, life is not quite so straightforward. However, we can make use of the action of $PSL_2(q)$ on the projective line $P(q)$.

Lemma 3.7. *Let $G \cong PSL_2(q)$, where $q \equiv 3 \bmod 4$. Let X be the unique conjugacy class of involutions of G, with $x, y \in X$. If the product xy fixes points on the projective line, then xy has odd order in G.*

Proof. Since $|G| = q(q-1)(q+1)/2$, and G acts transitively on the $q+1$ points of the projective line, by the Orbit-Stabiliser Theorem we see that a point stabiliser has order $q(q-1)/2$. Since $q \equiv 3 \bmod 4$, this order is odd, and hence xy must have odd order. □

Proposition 3.8. *Let $G \cong PSL_2(q)$, where $q \equiv 3 \bmod 4$, $q > 13$. Let X be the unique conjugacy class of involutions of G. Then $\mathcal{F}(G, X)$ is connected and has diameter 2.*

Proof. We adapt the proof of Theorem 1.1 (ii) in [13]. Let $t, x \in X$ be non-adjacent in $\mathcal{F}(G, X)$. We show there exists $y \in X$ such that both ty and yx fix points on the projective line. Then the result will follow by Lemma 3.7. Consider the elements of G as elements of $SL_2(q)$, acting on V. Without loss of generality let

$$t = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ and } x = \begin{pmatrix} a & b \\ c & -a \end{pmatrix},$$

where $a, b, c \in \mathbb{F}_q$ and $a^2 + bc = -1$. Let

$$y = \begin{pmatrix} 0 & \lambda \\ -1/\lambda & 0 \end{pmatrix},$$

where $\lambda \in \mathbb{F}_q$. Note that both t and y swap the subspaces of V generated by $\binom{1}{0}$ and $\binom{0}{1}$, so ty fixes these points on the projective line, and by Lemma 3.7 t and y are adjacent in $\mathcal{F}(G, X)$. Therefore it suffices to show that yx fixes a subspace generated by some non-zero vector $\binom{\alpha}{\beta}$. Note that

$$yx = \begin{pmatrix} 0 & \lambda \\ -1/\lambda & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & -a \end{pmatrix} = \begin{pmatrix} \lambda c & -\lambda a \\ -a/\lambda & -b/\lambda \end{pmatrix}.$$

Thus we are looking for α, β such that

$$\kappa \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \lambda c & -\lambda a \\ -a/\lambda & -b/\lambda \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \lambda c\alpha - \lambda a\beta \\ -a\alpha/\lambda - b\beta/\lambda \end{pmatrix}$$

for some $\kappa \in \mathbb{F}_q$. Thus we require

$$\kappa\alpha = \lambda c\alpha - \lambda a\beta \tag{3.1}$$

and

$$\kappa\beta = -a\alpha/\lambda - b\beta/\lambda. \tag{3.2}$$

From these we get

$$\frac{\alpha}{\beta} = \frac{-\lambda a}{\kappa - \lambda c} = \frac{-(\kappa\lambda + b)}{a}.$$

We therefore must have that $\kappa \neq \lambda c$ and $\kappa \neq -b/\lambda$. Rearranging the above yields the following quadratic equation in κ:

$$\lambda\kappa^2 + (b - \lambda^2 c)\kappa - \lambda(bc + a^2) = 0.$$

This equation has solutions if and only if its discriminant $\Phi(\lambda)$ is non-zero. Note that $\Phi(\lambda)$ is a quartic equation in $\lambda \neq 0$. Since there are $q-1$ possible values of λ, there are at worst $(q-1)/4$ different values of $\Phi(\lambda)$. Since we disallow $\Phi(\lambda) = 0$ and values resulting from choices of λ which lead to disallowed values of κ, there are at least $(q-1)/4 - 3 = (q-13)/4$ suitable values of $\Phi(\lambda)$. But $q > 13$ by assumption, so there is at least one suitable value of $\Phi(\lambda)$, which yields a suitable value of κ and hence of α/β. Thus y may be chosen so that yx fixes points on the projective line, and the result follows. $\square$

Chapter 4

Finite Coxeter Groups

Let us move on to investigate the local fusion graphs of finite *Coxeter groups*. A Coxeter group of rank n is defined to be a group generated by n involutions, subject only to relations which give the order of the pairwise products of the generators. For example, the symmetric group $\mathrm{Sym}(n)$ is a Coxeter group of rank $n-1$, since

$$\mathrm{Sym}(n) = \langle t_1, \ldots, t_{n-1} : (t_i t_j)^3 = 1 \text{ when } |i-j| = 1, (t_i t_j)^2 = 1 \text{ otherwise} \rangle.$$

This can be seen by setting $t_i = (i, i+1) \in \mathrm{Sym}(n)$ for $1 \leq i \leq n-1$. In view of this, studying the finite Coxeter groups is a natural next step after the work of Chapter 2. Furthermore, two infinite families of finite Coxeter groups will provide us with examples which show that the diameter of local fusion graphs can be arbitrarily large.

4.1 Reflection Groups

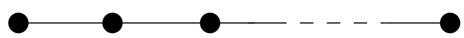
It can be shown that finite Coxter groups are in fact equivalent to finite real *reflection groups* (see [46]). Let V be an n-dimensional Euclidean space, that is the vector space $\mathbb{R}^n$ equipped with an inner product, and let $\{e_1, \ldots, e_n\}$ be an orthonormal basis for V. If $0 \neq x \in V$, notice that x defines a hyperplane $H \subset V$ (a subspace of codimension 1), where H consists of all vectors in V orthogonal to x. The *reflection* ρ_x is a linear map from V to itself which fixes H but negates every vector in V which is orthogonal to H. More precisely,

$$\rho_x(v) = v - 2\frac{\langle x, v\rangle}{\langle x, x\rangle}x$$

for all $v \in V$. A group which is generated by reflections is called a *reflection group*.

The finite real reflection groups were completely classified by Coxeter in [28]. In doing so, Coxeter made use of a particular type of diagram, subsequently referred to as a *Coxeter diagram* or *Coxeter graph*. To define the graph, we must first choose our set of generating reflections in a particular way. Recall that any two reflections ρ_x and ρ_y (indeed, any two involutions) generate a dihedral group of order $2m$, where m is the order of the product $\rho_x\rho_y$. It follows that the angle between the defining vectors x and y is $2k\pi/m$, where k is coprime to m. It is in fact possible to choose our defining vectors so that the angle between any x and y is $\pi - \pi/m$, so as close to parallel as possible. A generating set chosen in this way is called a *fundamental system* of reflections.

Given a fundamental system of n reflections, we can now define the Coxeter graph. It consists of n vertices, each corresponding to a fundamental reflection, with two vertices joined by an edge if the product of the corresponding reflections has order $m \geq 3$. Furthermore, if $m \geq 4$ we label the edge with the integer m. As an example, here is the Coxeter graph for $\mathrm{Sym}(n)$, which has $n-1$ vertices.



Notice that if the Coxeter graph is disconnected, then every reflection in one component commutes with those in another component, so the reflection group which is generated is a direct product of smaller reflection groups. Thus we may restrict our attention to connected Coxeter graphs. Coxeter showed that the only certain such graphs can occur, which we list in Figure 4.1. The resulting reflection groups consist of three infinite families $C(A_n)$, $C(B_n)$ and $C(D_n)$, along with the exceptional groups $C(E_6)$, $C(E_7)$, $C(E_8)$, $C(F_4)$, $C(H_3)$, $C(H_4)$ and $C(I_n)$. The structure of these groups is shown in Table 4.1. For the group $C(H_4)$ in Table 4.1, $SL_2(5) \circ SL_2(5)$ denotes the *central product* of two copies of $SL_2(5)$ (see [38], for example).

Figure 4.1: Finite Irreducible Coxeter Diagrams

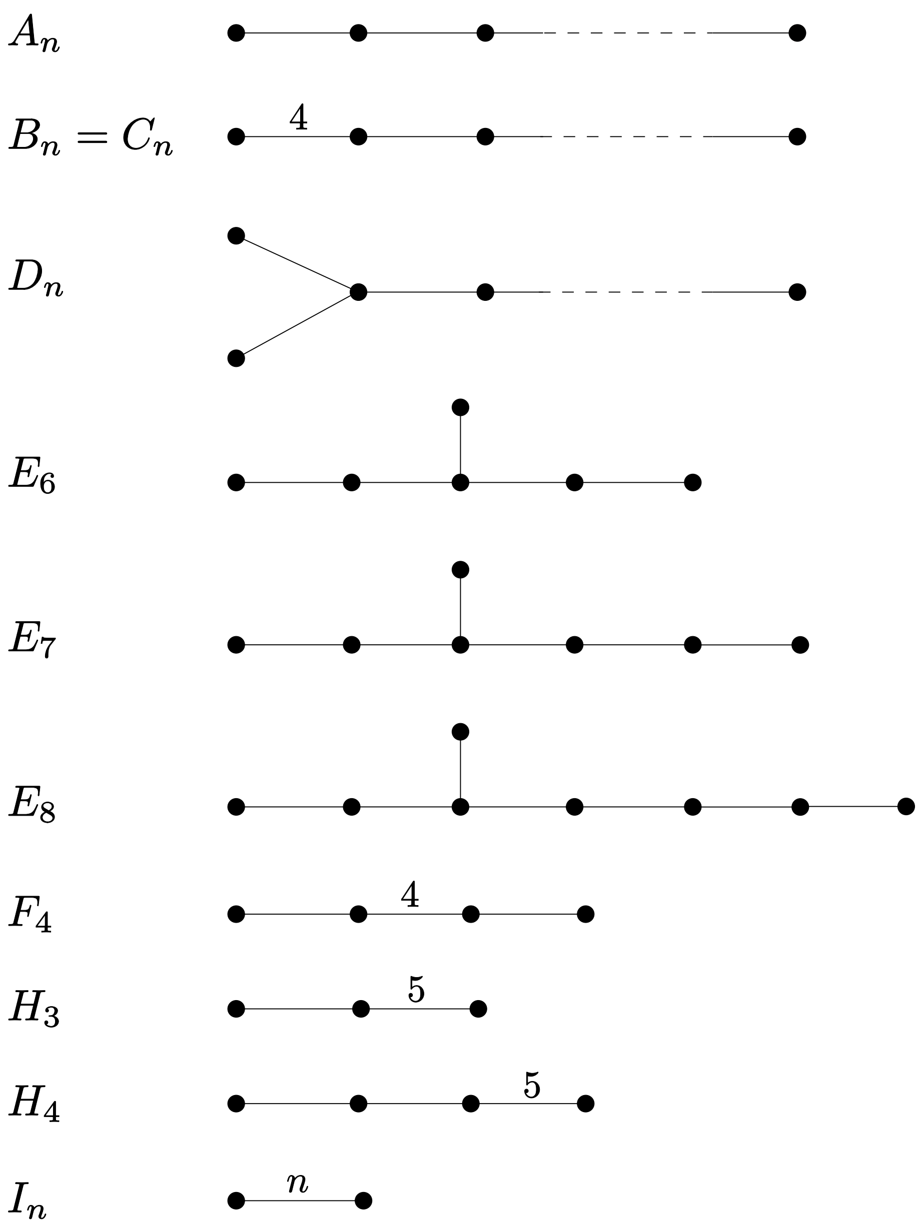


Table 4.1: Structure of the finite irreducible Coxeter groups

$$
\begin{array}{lll}
C(A_n) & \cong \mathrm{Sym}(n+1), & (n \geq 1); \\
C(B_n) & \cong 2^n : \mathrm{Sym}(n), & (n \geq 2); \\
C(D_n) & \cong 2^{n-1} : \mathrm{Sym}(n), & (n \geq 4); \\
C(E_6) & \cong GO_6^-(2); & \\
C(E_7) & \cong O_4^+(3); & \\
C(E_8) & \cong O_8^+(2).2; & \\
C(F_4) & \cong 2_+^{1+4}.3^2.2^2; & \\
C(H_3) & \cong 2 \times \mathrm{Alt}(5); & \\
C(H_4) & \cong (SL_2(5) \circ SL_2(5)) : 2; & \\
C(I_n) & \cong \mathrm{Dih}(2n). &
\end{array}
$$

4.2 The Classical Coxeter Groups

We can now focus on the local fusion graphs of finite Coxeter groups, beginning with the classical groups of types A_n, B_n and D_n. Firstly, we note that the Coxeter groups $C(A_n)$ have already been addressed.

Theorem 4.1. *Let $G = C(A_n)$, where $n \geq 4$, and let X be a G-conjugacy class of involutions. Then $\mathcal{F}(G, X)$ is connected with* $\mathrm{Diam}(\mathcal{F}(G, X)) = 2$.

Proof. Since $C(A_n) \cong \mathrm{Sym}(n+1)$ this is just Theorem 2.3. $\square$

Let us now concentrate on the groups $C(B_n)$ and $C(D_n)$. The Coxeter group $C(B_n)$ may be considered as the group of *signed permutations* of n objects (see [12] or [46]). Let $\mathrm{Sym}(n)$ act on the set $\Omega = \{1, \ldots, n\}$, and define the i-th 'sign change' to be the element which sends i to $-i$ and fixes all other $j \in \Omega$. The set of all such elements generates an elementary abelian group of order 2^n, and $C(B_n)$ is isomorphic to the semidirect product of this group with $\mathrm{Sym}(n)$. If we wish to emphasise the set upon which $C(B_n)$ acts, we may write $C(B_\Omega)$. For $n \geq 4$, $C(D_n)$ is the subgroup of index 2 of $C(B_n)$ generated by $\mathrm{Sym}(n)$ and the elements of the elementary abelian subgroup involving an even number of sign changes. A convenient way of expressing the elements of $C(B_n)$ is to write a permutation in $\mathrm{Sym}(n)$, including 1-cycles, along with a plus or minus sign above each i, and say i is positive or negative respectively, for example

$$z = (\overset{+}{1}, \overset{-}{3}, \overset{+}{2})(\overset{-}{4}) \in C(B_4).$$

By convention we read the sign first, so $z(1) = 3$, $z(2) = 1$, $z(3) = -2$ and $z(4) = -4$. Given a cycle $\rho \in C(B_n)$, we say ρ is *positive* or *negative* depending on whether the number of minus signs above its elements are even or odd, respectively. The *signed cycle type* of an element of $C(B_n)$ is defined to be the cycle type of the element, including 1-cycles, with a plus or minus over each cycle, depending on whether the cycle is positive or negative, respectively.

We can now state the main results we shall prove about the groups $C(B_n)$ and $C(D_n)$.

Theorem 4.2. *Suppose $G = C(B_n)$, $n \geq 2$ and X is a G-conjugacy class of involutions. Write $G = N : H$ where $N \cong 2^n$ and $H \cong \mathrm{Sym}(n)$. If $X \subset N$, then $\mathcal{F}(G, X)$ is totally disconnected, while if $X \not\subset N$ then $\mathcal{F}(G, X)$ is connected, unless $n = 2m$ and $X = t^G$, where*

$$t = (\overset{+}{1}, \overset{+}{2}), (\overset{+}{3}, \overset{+}{4}) \cdots (\overset{+}{2m-1}, \overset{+}{2m}).$$

In the latter case $\mathcal{F}(G, X)$ has exactly two connected components, unless $n = 4$, in which case $\mathcal{F}(G, X)$ is totally disconnected with 12 vertices.

Theorem 4.3. *Suppose $G = C(D_n)$, $n \geq 4$ and X is a G-conjugacy class of involutions. Write $G = N : H$ where $N \cong 2^{n-1}$ and $H \cong \mathrm{Sym}(n)$. If $X \subset N$, then $\mathcal{F}(G, X)$ is totally disconnected, while if $X \not\subset N$ then $\mathcal{F}(G, X)$ is connected.*

Theorem 4.4. *Suppose $G = C(B_n)$, where $n \geq 4$.*

(i) If n is even, then there exists a G-conjugacy class of involutions X such that $\mathrm{Diam}(\mathcal{F}(G, X)) = n - 1$. Moreover, if X' is any other G-conjugacy class of involutions such that $\mathcal{F}(G, X')$ is connected, then

$$\mathrm{Diam}(\mathcal{F}(G, X')) \leq n - 1.$$

(ii) If n is odd, then there exists a G-conjugacy class of involutions X such that $\mathrm{Diam}(\mathcal{F}(G, X)) = n - 2$. Moreover, if X' is any other G-conjugacy class of

involutions such that $\mathcal{F}(G, X')$ is connected, then

$$\mathrm{Diam}(\mathcal{F}(G, X')) \leq n - 2.$$

We shall see from Proposition 4.6 that, with possibly just one exception, the local fusion graphs of $C(D_n)$ are isomorphic to local fusion graphs of $C(B_n)$. Thus Theorem 4.4 also provides bounds on the diameters of the local fusion graphs of $C(D_n)$. As a consequence of our work on $C(B_n)$ we have the following more general result concerning local fusion graphs of finite groups.

Theorem 4.5. *For any given $r, m \in \mathbb{N}$, there exists a finite group G with conjugacy class of involutions X such that $\mathcal{F}(G, X)$ has exactly m connected components, each of which has diameter r.*

Theorems 4.4 and 4.5 contrast with many results concerning the diameter of graphs related to local fusion graphs. For example, in [10] it is shown that for finite symmetric groups the diameter of commuting involution graphs is at most 4, while in [12] it is proved that for any other finite irreducible Coxeter group the diameter of a commuting involution graph is at most 5. Also, in [14], we find analysis of the commuting involutions graphs of the majority of the sporadic simple groups, and it is shown that their diameters are at most 4. For the S_3-involution graphs studied in [30], it is shown that their diameter is 3. And of course, the work of Chapter 2 has shown that for finite symmetric groups almost all local fusion graphs have diameter 2. It is therefore worthwhile to note that Theorem 4.4 demonstrates that no such absolute bounds exist for the diameters of local fusion graphs of finite Coxeter groups.

The following result, found in [23], characterises the conjugacy classes of $C(B_n)$ and $C(D_n)$, and will be important in the proofs throughout this chapter.

Proposition 4.6. *(i) Elements of $C(B_n)$ are conjugate if and only if they have the same signed cycle type.*

(ii) Conjugacy classes in $C(D_n)$ are parameterised by signed cycle type, with one class for each signed cycle type except in the case where the signed cycle type

contains only even length, positive cycles. In the latter case there are two classes for each signed cycle type, distinguished by the number of minus signs modulo 4.

As we are considering $C(D_n)$ as a subgroup of $C(B_n)$, Proposition 4.6 (ii) tells us that for $x \in C(D_n)$ we have $x^{C(D_n)} = x^{C(B_n)}$, unless x has only even length, positive cycles. Let us now establish some notation. Recall that for an element $\sigma \in \mathrm{Sym}(n)$, the *support* of σ is defined to be $\mathrm{supp}(\sigma) = \Omega \setminus \mathrm{fix}(\sigma)$. We now extend this notion to $C(B_n)$. Given $x \in C(B_n)$, we define the *S-support* of x, $\mathrm{supp}_S(x)$, to be the support of the corresponding element of $\mathrm{Sym}(n)$. In addition, we define the *C-support* of x, $\mathrm{supp}_C(x)$, to be $\Omega \setminus \mathrm{fix}(x)$. Here S and C stand for 'symmetric' and 'Coxeter' respectively. To illustrate, if we again take

$$z = (\overset{+}{1}, \overset{-}{3}, \overset{+}{2})(\overset{-}{4}),$$

then $\mathrm{supp}_S(z) = \{1, 2, 3\}$, while $\mathrm{supp}_C(z) = \{1, 2, 3, 4\}$ (since $z(4) = -4$). For brevity, given two elements x and y of $C(B_n)$ we shall write

$$\Delta_{x,y} = \mathrm{supp}_S(x) \cup \mathrm{supp}_S(y).$$

We define the *weight* of x, denoted $w(x)$, to be the number of negative signs in x, and the 1-*weight* of x, denoted $w_1(x)$, is defined to be the number of negative 1-cycles in x. For example, for the element z given above we have $w(z) = 2$ and $w_1(x) = 1$.

We now set $G = C(B_n)$ where $n \geq 3$, and begin to consider the structure of the local fusion graphs of G. Clearly a G-conjugacy of involutions which lies in the elementary abelian normal 2-subgroup of G will yield a totally disconnected local fusion graph. A more interesting collection of local fusion graphs of G are those which have as vertex set a G-conjugacy class of *signed transpositions*, that is, elements of G which contain exactly one 2-cycle. Let X be such a G-conjugacy class. Our next lemma tells us precisely when two elements of X are adjacent in $\mathcal{F}(G, X)$.

Lemma 4.7. *If $x, y \in X$, then x and y are adjacent in $\mathcal{F}(G, X)$ if, and only if, $|\Delta_{x,y}| = 3$ and $w_1(xy) = 0$.*

Proof. Suppose that x and y are adjacent in $\mathcal{F}(G,X)$. Then since x and y contain only one 2-cycle each, the product xy must have order 3, and we must certainly have $|\Delta_{x,y}| = 3$. Furthermore, if $w_1(xy) \geq 1$, then xy must contain negative 1-cycles, and consequently the product order must be divisible by 2. This contradicts xy having order 3.

Now suppose that $|\Delta_{x,y}| = 3$ and $w_1(xy) = 0$. By the latter assumption, any 1-cycle (i) in the product xy, where $i \in \Omega \setminus \Delta_{x,y}$, must be positive, and hence have order 1. So we need only concern ourselves with the 3-cycle of xy. We may without loss of generality assume that, without signs, we have $x = (1,2)(3)$ and $y = (1,3)(2)$. Since x and y are G-conjugate (and the 1-cycles outside $\Delta_{x,y}$ have the same signs), we can apply Proposition 4.6 to deduce that the 1-cycles (3) and (2) must have the same sign.

If the signs of x as in y are identical, we get

$$xy = (\overset{+}{1}, \overset{+}{2}, \overset{+}{3}),$$

which clearly has order 3, so x and y are adjacent in $\mathcal{F}(G,X)$. On the other hand, any other valid signing of x and y will a yield a 3-cycle with two negative signs and one positive, such as $xy = (\overset{-}{1}, \overset{-}{2}, \overset{+}{3})$. An easy check shows that such elements also have order 3. Thus x and y are adjacent in any case. $\square$

An easy consequence of Lemma 4.7 is that the local fusion graphs of $C(B_n)$ corresponding to G-conjugacy classes of signed transpositions are also S_3-involution graphs, as defined in [30]. We now prove a lemma which gives us a lower bound on the distance between two G-conjugate signed transpositions in $\mathcal{F}(G,X)$.

Lemma 4.8. *Suppose that $x, y \in X$, with $x \neq y$. If $w_1(xy) = k$, then $d(x,y) \geq k+1$.*

Proof. We use induction on k. When $k = 0$ the result is clear, and when $k = 1$ the result follows by Lemma 4.7. So assume $w_1(xy) = k$ where $k \geq 2$, and let γ be a shortest path from x to y in $\mathcal{F}(G,X)$. By Lemma 4.7, there must exist $z \in \gamma$ such that $w_1(xz) = k-1$. Now by induction we have $d(x,z) \geq k$. Since γ was chosen arbitrarily, and $d(z,y) \geq 1$, we see that $d(x,y) \geq k+1$ as required. $\square$

Given $x, y \in X$, then since $|\mathrm{supp}_S(x)| = |\mathrm{supp}_S(y)| = 2$, it must be the case that $|\Delta_{x,y}| = 2$, 3 or 4. The following two lemmas examine each of these possibilities, and provide us with straightforward expressions for the distance between x and y in $\mathcal{F}(G, X)$ in terms of the 1-weight of the product xy.

Lemma 4.9. *Suppose $x, y \in X$, where $x \neq y$ and $|\Delta_{x,y}| = 2$ or 3. Then $d(x, y) = w_1(xy) + 1$, unless $|\Delta_{x,y}| = 2$ and $w_1(xy) = 0$, in which case $d(x, y) = 2$.*

Proof. First suppose that $|\Delta_{x,y}| = 2$, and that $w_1(xy) = k$. Note that Proposition 4.6 implies that k must be even, so write $k = 2m$. If $m = 0$, then since $x \neq y$ without loss of generality the 2-cycles of x and y must be $(\overset{+}{1}, \overset{+}{2})$ and $(\overset{-}{1}, \overset{-}{2})$, and using Lemma 4.7 we may easily find an element which is adjacent to both x and y in $\mathcal{F}(G, X)$. So assume that $m \geq 1$, and consequently we must have $n \geq 4$. If x and y agree on any signed 1-cycles, then in the product xy these will be positive 1-cycles, which have order 1. It therefore suffices to ignore these 1-cycles and consider x and y as elements of $C(B_\Sigma)$ where $\Sigma = \Delta_{x,y} \cup \mathrm{supp}_C(xy)$, and prove the result in this context. So, without loss of generality we assume that $n = |\Delta_{x,y}| + w_1(xy)$. Using the vertex-transitivity of G on $\mathcal{F}(G, X)$, and Proposition 4.6, we may assume that x and y are labelled so that

$$x = (\overset{+}{1}, \overset{+}{2})(\overset{-}{3})(\overset{-}{4}) \ldots (m \overset{-}{+} 2)(m \overset{+}{+} 3) \ldots (2m \overset{+}{+} 2)$$

and

$$y = (\overset{\epsilon}{1}, \overset{\epsilon}{2})(\overset{+}{3})(\overset{+}{4}) \ldots (m \overset{+}{+} 2)(m \overset{-}{+} 3) \ldots (2m \overset{-}{+} 2),$$

where $\epsilon \in \{+, -\}$. By Lemma 4.8, $d(x, y) \geq 2m + 1$. To show that this is in fact an equality, we construct a path from x to y in $\mathcal{F}(G, X)$ as follows, using Lemma 4.7 to verify adjacency at each step:

$$\begin{aligned}
x &= (\overset{+}{1},\overset{+}{2})(\overset{-}{3})(\overset{-}{4})\dots(\overset{-}{m+2})(\overset{+}{m+3})\dots(\overset{+}{2m+2}),\\
z_1 &= (\overset{+}{1},\overset{+}{m+3})(\overset{+}{2})(\overset{-}{3})(\overset{-}{4})\dots(\overset{-}{m+2})(\overset{+}{m+4})\dots(\overset{+}{2m+2}),\\
z_2 &= (\overset{+}{1},\overset{+}{3})(\overset{+}{2})(\overset{-}{4})\dots(\overset{-}{m+3})(\overset{+}{m+4})\dots(\overset{+}{2m+2}),\\
z_3 &= (\overset{+}{1},\overset{+}{m+4})(\overset{+}{2})(\overset{+}{3})(\overset{-}{4})\dots(\overset{-}{m+3})(\overset{+}{m+5})\dots(\overset{+}{2m+2}),\\
z_4 &= (\overset{+}{1},\overset{+}{4})(\overset{+}{2})(\overset{+}{3})(\overset{-}{5})\dots(\overset{-}{m+4})(\overset{+}{m+5})\dots(\overset{+}{2m+2}),\\
&\vdots\\
z_{2m} &= (\overset{+}{1},\overset{+}{m+2})(\overset{+}{2})(\overset{+}{3})\dots(\overset{+}{m+1})(\overset{-}{m+3})\dots(\overset{-}{2m+2}),\\
y &= (\overset{\epsilon}{1},\overset{\epsilon}{2})(\overset{+}{3})(\overset{+}{4})\dots(\overset{+}{m+2})(\overset{-}{m+3})\dots(\overset{-}{2m+2}).
\end{aligned}$$

Since this path has length $2m+1$, we deduce that $d(x,y) = 2m+1$.

Now assume that $|\Delta_{x,y}| = 3$ and $w(xy) = k$. Here it need not be the case that k is even. If $k = 0$ the result follows by Lemma 4.7, so assume that $k \geq 1$. Thus $n \geq 4$. Using vertex-transitivity and Proposition 4.6 we see that, up to relabelling, there are the following possibilities for x and y:

(i) $k = 2m$,

$$x = (\overset{+}{1},\overset{+}{2})(\overset{\delta}{3})(\overset{-}{4})\dots(\overset{-}{m+3})(\overset{+}{m+4})\dots(\overset{+}{2m+3})$$

and

$$y = (\overset{\epsilon}{1},\overset{\epsilon}{3})(\overset{\delta}{2})(\overset{+}{4})\dots(\overset{+}{m+3})(\overset{-}{m+4})\dots(\overset{-}{2m+3});$$

(ii) $k = 2m+1$,

$$x = (\overset{+}{1},\overset{+}{2})(\overset{\delta}{3})(\overset{-}{4})\dots(\overset{-}{m+3})(\overset{-\delta}{m+4})(\overset{+}{m+5})\dots(\overset{+}{2m+4})$$

and

$$y = (\overset{\epsilon}{1},\overset{\epsilon}{3})(\overset{-\delta}{2})(\overset{+}{4})\dots(\overset{+}{m+3})(\overset{\delta}{m+4})(\overset{-}{m+5})\dots(\overset{-}{2m+4}),$$

where $\epsilon, \delta \in \{+,-\}$. In case (i), Lemma 4.8 implies that $d(x,y) \geq 2m+1$, while in case (ii), Lemma 4.8 implies that $d(x,y) \geq 2m+2$. However, we may construct paths from x to y in $\mathcal{F}(G,X)$ of length $2m+1$ and $2m+2$, in each case respectively.

Since the method used to construct these paths is very similar in each case, we simply illustrate case (ii) where $\delta = +$. Here a suitable path is

$$\begin{aligned}
x &= (\overset{+}{1},\overset{+}{2})(\overset{+}{3})(\overset{-}{4})\ldots(\overset{-}{m+4})(\overset{+}{m+5})\ldots(\overset{+}{2m+4}),\\
z_1 &= (\overset{+}{1},\overset{+}{4})(\overset{-}{2})(\overset{+}{3})(\overset{-}{5})\ldots(\overset{-}{m+4})(\overset{+}{m+5})\ldots(\overset{+}{2m+4}),\\
z_2 &= (\overset{+}{1},\overset{+}{m+5})(\overset{-}{2})(\overset{+}{3})(\overset{+}{4})(\overset{-}{5})\ldots(\overset{-}{m+4})(\overset{+}{m+6})\ldots(\overset{+}{2m+4}),\\
z_3 &= (\overset{+}{1},\overset{+}{5})(\overset{-}{2})(\overset{+}{3})(\overset{+}{4})(\overset{-}{6})\ldots(\overset{-}{m+5})(\overset{+}{m+6})\ldots(\overset{+}{2m+4}),\\
z_4 &= (\overset{+}{1},\overset{+}{m+6})(\overset{-}{2})(\overset{+}{3})(\overset{+}{4})(\overset{+}{5})(\overset{-}{6})\ldots(\overset{-}{m+6})(\overset{+}{m+7})\ldots(\overset{+}{2m+4}),\\
&\vdots\\
z_{2m} &= (\overset{+}{1},\overset{+}{2m+4})(\overset{-}{2})(\overset{+}{3})\ldots(\overset{+}{m+3})(\overset{-}{m+4})\ldots(\overset{-}{2m+4}),\\
z_{2m+1} &= (\overset{+}{1},\overset{+}{m+4})(\overset{-}{2})(\overset{+}{3})\ldots(\overset{+}{m+3})(\overset{-}{m+5})\ldots(\overset{-}{2m+4}),\\
y &= (\overset{\epsilon}{1},\overset{\epsilon}{3})(\overset{-}{2})(\overset{+}{4})\ldots(\overset{+}{m+4})(\overset{-}{m+5})\ldots(\overset{-}{2m+4}).
\end{aligned}$$

□

Lemma 4.10. *Suppose $x, y \in X$ with $|\Delta_{x,y}| = 4$. Then $d(x,y) = w_1(xy) + 2$.*

Proof. Let $w_1(xy) = k$. We proceed by induction on k. When $k = 0$ then the result may be easily verified, either by hand or using MAGMA [18], so assume that $k \geq 1$. This implies that $n \geq 5$. By Lemma 4.8 we have $d(x,y) \geq k+1$. Using Lemma 4.7, it is clear that y is adjacent to some element $y' \in X$ where $|\Delta_{x,y'}| = 3$, and so by Lemma 4.9 there exists a path from x to y in $\mathcal{F}(G,X)$. So let γ be a shortest path from x to y in $\mathcal{F}(G,X)$, and suppose that $z \in \gamma$ is adjacent to y. Using Lemma 4.7 we see that $|\Delta_{x,z}| = 3$ or 4. If $|\Delta_{x,z}| = 3$ it must also be that $w_1(xz) = w_1(xy)$, and so Lemma 4.9 implies that $d(x,z) = w_1(xz) + 1 = k + 1$. Since γ was chosen arbitrarily, we have $d(x,y) = (k+1) + 1 = k + 2$, as required. Now suppose that $|\Delta_{x,z}| = 4$. If $w_1(xz) = w_1(xy)$, then z and y will lie in the same $C_G(x)$-orbit, which provides a contradiction using Lemma 1.17. So it must be that $w_1(xz) = w_1(xy) - 1$. By induction we have $d(x,z) = w_1(xz) + 2 = k + 1$, and so by the arbitary choice of γ we again have $d(x,y) = (k+1) + 1 = k + 2$. □

Notice that the constructive nature of Lemmas 4.9 and 4.10 shows that the local fusion graphs of $C(B_n)$ which arise from conjugacy classes of signed transpositions are connected. We can now prove the following result regarding the diameters of these local fusion graphs.

Theorem 4.11. *Let $G = C(B_n)$, where $n \geq 4$.*

(i) If n is even, then there exist G-conjugacy classes of signed transpositions X_1 and X_2 such that $\mathrm{Diam}(\mathcal{F}(G, X_1)) = n - 1$ *and* $\mathrm{Diam}(\mathcal{F}(G, X_2)) = n - 2$. *Moreover, if Y is any other G-conjugacy class of signed transpositions, then* $\mathrm{Diam}(\mathcal{F}(G, Y)) \leq n - 1$.

(ii) If n is odd, then there exists a G-conjugacy class of signed transpositions X_3 such that $\mathrm{Diam}(\mathcal{F}(G, X_3)) = n - 2$. *Moreover, if Y' is any other G-conjugacy class of signed transpositions, then* $\mathrm{Diam}(\mathcal{F}(G, Y')) \leq n - 2$.

Proof. Suppose that n is even, and write $n = 2m$. Set $X_1 = x_1^G$, where

$$x_1 = (\overset{+}{1}, \overset{+}{2})(\overset{+}{3})(\overset{+}{4})(\overset{-}{5}) \cdots (\overset{-}{m+2})(\overset{+}{m+3}) \cdots (\overset{+}{2m}).$$

If we now let

$$y_1 = (\overset{+}{1})(\overset{+}{2})(\overset{+}{3}, \overset{+}{4})(\overset{+}{5}) \cdots (\overset{+}{m+2})(\overset{-}{m+3}) \cdots (\overset{-}{2m}),$$

then $w_1(xy) = 2m - 4$, so Lemma 4.10 tells us that

$$d(x_1, y_1) = 2m - 2 = n - 2.$$

Since it is impossible to choose $y_1' \in X_1$ where $w_1(x_1 y_1') > w_1(x_1 y_1)$, Lemmas 4.9 and 4.10 show that this distance is maximal in $\mathcal{F}(G, X_1)$, whence $\mathrm{Diam}(\mathcal{F}(G, X_1)) = n - 2$.

Next, set $X_2 = x_2^G$, where

$$x_2 = (\overset{+}{1}, \overset{+}{2})(\overset{-}{3}) \cdots (\overset{-}{m+1})(\overset{+}{m+2}) \cdots (\overset{+}{2m}).$$

Then

$$y_2 = (\overset{+}{1}, \overset{+}{2})(\overset{+}{3}) \cdots (\overset{+}{m+1})(\overset{-}{m+2}) \cdots (\overset{-}{2m})$$

is an element at maximal distance from x_2 in $\mathcal{F}(G, X_2)$, and since $w_1(x_2 y_2) = 2m - 2$ we have $d(x_2, y_2) = n - 1$ by Lemma 4.9. Thus $\mathrm{Diam}(\mathcal{F}(G, X_2)) = n - 1$. To see the final statement of (i), note that if x' and y' are signed transpositions in any other G-conjugacy class of signed transpositions Y, then $w_1(x'y') < 2m-2$, so by Lemmas 4.9 and 4.10 we have $d(x', y') \leq 2m-1 = n-1$.

Finally, suppose that $n = 2m+1$ and set $X_3 = x_3^G$, where

$$x_3 = (\overset{+}{1}, \overset{+}{2})(\overset{+}{3})(\overset{-}{4})(\overset{-}{5}) \cdots (\overset{-}{m+2})(\overset{+}{m+3}) \cdots (\overset{+}{2m+1}).$$

Then

$$y_3 = (\overset{+}{1})(\overset{+}{2})(\overset{+}{3}, \overset{+}{4})(\overset{+}{5}) \cdots (\overset{+}{m+2})(\overset{-}{m+3}) \cdots (\overset{-}{2m+1})$$

is at maximal distance from x_3 in $\mathcal{F}(G, X)$, and by Lemma 4.10 we have

$$d(x_3, y_3) = 2m-1 = n-2,$$

which yields $\mathrm{Diam}(\mathcal{F}(G, X_3)) = n-2$. For the final statement of (ii), notice that for x' and y' in any other G-conjugacy class of signed tranpositions Y', then either $w_1(x'y') \leq n-4$, or $w_1(x'y') = n-3$ and $|\Delta_{x',y'}| = 2$ or 3. In both cases, by Lemmas 4.9 and 4.10 we have $\mathrm{Diam}(\mathcal{F}(G, Y')) \leq n-2$. $\square$

The case where $n = 3$ is excluded from Theorem 4.11 since for $G = C(B_3)$ and $X = x^G$, where $x = (\overset{+}{1}, \overset{+}{2})(\overset{+}{3})$ or $(\overset{+}{1}, \overset{+}{2})(\overset{-}{3})$, we have $\mathrm{Diam}(\mathcal{F}(G, X)) = 2$. Note that Theorem 4.11 partially proves Theorem 4.5, by showing the existence of local fusion graphs with diameter r for all $r \geq 3$. Since the existence of local fusion graphs with diameters 1 and 2 is clear, to complete the proof of Theorem 4.5, we just need to show that any number of connected components is possible. This is resolved by our next result.

Lemma 4.12. *Let H be a finite group, with X an H-conjugacy class of involutions, and suppose $\mathcal{F}(H, X)$ is connected. Let $L = H \wr \mathrm{Sym}(m)$. Then there exists an L-conjugacy class of involutions Y such that $\mathcal{F}(L, Y)$ has exactly m connected components.*

Proof. The wreath product $L = H \wr \mathrm{Sym}(m)$ has base group $H_1 \times \cdots \times H_m$, where $H_i \cong H$ for $1 \leq i \leq m$. Let Y be the L-conjugacy class which contains the canonical image of X in H_1. Since $\mathrm{Sym}(m)$ acts transitively on the components of the base group, Y can be considered as a direct product of m copies of X. Since elements of Y from distinct components commute, they can never be adjacent in $\mathcal{F}(L, Y)$. It follows that $\mathcal{F}(L, Y)$ has m connected components, each of which is isomorphic to $\mathcal{F}(H, X)$. □

Combining Lemma 4.12 with Theorem 4.11 now yields Theorem 4.5. Having considered the case of signed transpositions, we now move to the opposite extreme, those conjugacy classes of involutions which have at most one 1-cycle. First we collect together some data for cases when the rank n is small, which will be used in proving the more general results which follow.

Lemma 4.13. *Suppose $G = C(B_n)$, where $5 \leq n \leq 10$.*

(i) If $n = 2m$, set $X = t^G$ where

$$t = (\overset{+}{1}, \overset{+}{2}) \ldots (\overset{+}{2m-1}, \overset{+}{2m}).$$

Then $\mathcal{F}(G, X)$ has exactly two connected components. When $n = 8$ these components have diameter 3, while if $n = 6$ or 10 this diameter is 2.

(ii) If $n = 2m+1$, set $X = t_\epsilon^G$ where

$$t_\epsilon = (\overset{+}{1}, \overset{+}{2}) \ldots (\overset{+}{2m-1}, \overset{+}{2m})(\overset{\epsilon}{2m+1})$$

and $\epsilon \in \{+, -\}$. Then $\mathcal{F}(G, X)$ is connected, and $\mathrm{Diam}(\mathcal{F}(G, X)) = 2$.

Proof. Since these local fusion graphs have relatively small vertex sets, it is straightforward to explicitly construct them using Magma [18]. □

Lemma 4.14. *Let $G = C(B_n)$, and suppose $\sigma \in G$ is a signed cycle. Then σ has odd order if, and only if,*

(i) the length of σ is odd; and

(ii) the weight of σ is even.

Proof. Without loss of generality suppose that, without signs, $\sigma = (1, 2, \ldots, k)$. It is clearly the case that σ either has order k or $2k$. Thus for σ to have odd order it is necessary that (i) holds, so suppose that k is odd. If $w(\sigma) = 0$ then certainly σ has odd order k. Suppose that $w(\sigma) = 0$, and let σ_1 be equal to σ multiplied by a single negative 1-cycle, say

$$\sigma_1 = (\bar{i})\sigma,$$

where $i \in \{1, \ldots, k\}$. Then $w(\sigma_1) = 1$. Moreover, we have

$$\sigma_1^k = (\bar{1})(\bar{2}) \cdots (\bar{k}),$$

and so σ_1 has order $2k$. If we now multiply σ_1 by a negative 1-cycle, say

$$\sigma_2 = (\bar{j})\sigma_1,$$

where $j \in \{1, \ldots, k\}$, then we have $w(\sigma_2) = 0$ or 2, and we get

$$\sigma_2^k = (\bar{1})(\bar{2}) \cdots (\bar{k})(\bar{1})(\bar{2}) \cdots (\bar{k}) = 1,$$

so σ_2 has order k. More generally, if we multiply σ by an odd number of negative 1-cycles, the resulting product will have odd weight and order $2k$, while if we multiply σ by an even number of negative 1-cycles, the resulting product will have even weight and product order k. Since it is possible to reach any signed k-cycle in G by multiplying a k-cycle of zero weight by a number of negative 1-cycles, we deduce that if $w(\sigma)$ is even the order of σ is k, and if $w(\sigma)$ is odd the order of σ is $2k$. $\square$

Lemma 4.15. *Suppose $H = \mathrm{Sym}(2m)$ acts naturally on Ω, and set $X = x^H$, where*

$$x = (1, 2)(3, 4) \cdots (2m - 1, 2m).$$

If $y \in X$, then y is adjacent to x in $\mathcal{F}(H, X)$ if, and only if,

$$xy = \sigma_{1,1}\sigma_{1,2}\sigma_{2,1}\sigma_{2,2} \cdots \sigma_{s,1}\sigma_{s,2}$$

is a product of disjoint cycles, where for $1 \leq r \leq s$ the cycles $\sigma_{r,1}$ and $\sigma_{r,2}$ have the same odd length. Moreover, if $i, j \in \Omega$ lie in the same transposition of y, then we can label the cycles of xy so that $i \in \sigma_{1,1}$ and $j \in \sigma_{1,2}$.

Proof. This follows from Proposition 2.2 of [10]. □

We now consider $C(B_n)$ for arbitrary rank $n \geq 3$, and address the connectedness and diameter of those local fusion graphs which have as vertices involutions which contain at most one 1-cycle. In preparation we introduce another piece of notation. Given $g \in C(B_n)$, we denote by $\overline{g}$ the element of $\mathrm{Sym}(n)$ we get by ignoring all signs of g. For example, if $g \in C(B_6)$ and

$$g = (\overset{+}{1}, \overset{-}{2}, \overset{+}{3})(\overset{-}{4}, \overset{-}{5})(\overset{+}{6}),$$

then

$$\overline{g} = (1, 2, 3)(4, 5)(6).$$

Lemma 4.16. *Suppose $G = C(B_{2m})$, where $m \geq 3$, and let*

$$t = (\overset{+}{1}, \overset{+}{2})(\overset{+}{3}, \overset{+}{4}) \ldots (\overset{+}{2m-1}, \overset{+}{2m}),$$

with $X = t^G$. Then $\mathcal{F}(G, X)$ has exactly two connected components, one containing all $x \in X$ with $w(x) \equiv 0$ mod 4, the other containing all $x \in X$ with $w(x) \equiv 2$ mod 4. Furthemore, the diameter of each component is at most 5.

Proof. Proposition 4.6 implies that all elements of X have even weight. Let $\overline{G} = \mathrm{Sym}(2m)$, and denote by $\overline{X}$ the $\overline{G}$-conjugacy class which contains the element $\overline{t}$ which corresponds to t. By Lemma 4.15, $\overline{x}$ is adjacent to $\overline{t}$ in $\mathcal{F}(\overline{G}, \overline{X})$ if, and only if, the product $\overline{tx}$ consists of a disjoint product of pairs of odd-length cycles. There is an associated product of pairs of odd-length cycles of tx, and by Lemma 4.14 each of these cycles must have even weight. But if $(\overset{-}{i}, \overset{-}{j})$ is a transposition in x, then using Lemma 4.15 we see that $\overset{-}{i}$ and $\overset{-}{j}$ lie in disjoint cycles of tx. We deduce that $w(x) \equiv w(t)$ mod 4. Since G acts vertex-transitively on $\mathcal{F}(G, X)$ we have that every element of the connected component of $\mathcal{F}(G, X)$ which contains t has the same weight as t modulo 4.

Now suppose that $x \in X$ with $w(x) \equiv w(t)$ mod 4. Since Lemma 4.13 completes the proof for $m < 6$, we may assume that $m \geq 6$. By Theorem 1.1 of [7], $\mathcal{F}(\overline{G}, \overline{X})$

has diameter 2, so there exists some element $z \in X$ where $\overline{x} = \overline{z}$, and $d(t, z) \leq 2$. We may arrange the 2-cycles of x and z so that

$$x = x^{(1)}x^{(2)} \cdots x^{(r)}$$

and

$$z = z^{(1)}z^{(2)} \cdots z^{(r)},$$

and the following conditions are satisfied:

(i) the $x^{(i)}$ are (disjoint) products of three signed 2-cycles, except for possibly $x^{(r)}$ which may be a (disjoint) product of four or five signed 2-cycles;

(ii) $\overline{x^{(i)}} = \overline{z^{(i)}}$ for each i; and

(iii) $w(x^{(i)}) \equiv w(z^{(i)}) \bmod 4$, for each i.

Considering each pair $x^{(i)}, z^{(i)}$ as elements of $C(B_6)$ (or possibly $C(B_8)$ or $C(B_{10})$ for the final pair), we now apply Lemma 4.13 to see that for each i there exist paths from $z^{(i)}$ to $x^{(i)}$ of length at most 3, in the relevant local fusion graphs of $C(B_6)$, $C(B_8)$ or $C(B_{10})$. Since both $x^{(i)}$ and $z^{(i)}$ are disjoint from all other $x^{(j)}$, $z^{(j)}$ (where $i \neq j$), by taking products of suitable elements from each such path, we may construct a path of length at most 3 from z to x in $\mathcal{F}(G, X)$. Thus we have a path from t to x of length at most 5. It follows that the elements of X with weight congruent to 0 modulo 4 form a connected component of $\mathcal{F}(G, X)$. Since this accounts for exactly half the elements of X, by the vertex-transitivity of $\mathcal{F}(G, X)$ we deduce that there are exactly two connected components, the second of which must consist of the elements of X with weight congruent to 2 modulo 4. □

Lemma 4.17. *Suppose $G = C(B_{2m+1})$, where $m \geq 2$, and let*

$$t = (\overset{+}{1}, \overset{+}{2})(\overset{+}{3}, \overset{+}{4}) \ldots (\overset{+}{2m-1}, \overset{+}{2m})(\overset{\epsilon}{2m+1}),$$

where $\epsilon \in \{+, -\}$, with $X = t_\epsilon^G$. Then $\mathcal{F}(G, X)$ is connected, and

$$\mathrm{Diam}(\mathcal{F}(G, X)) \leq 4.$$

Proof. Our argument here is similar to that of the previous proof, and we adopt the same 'bar' notation. Let $x \in X$. By Theorem 2.3, $\mathcal{F}(\overline{G}, \overline{X})$ has diameter 2, so there exists some element $z \in X$ where $\overline{x} = \overline{z}$, and $d(t, z) \leq 2$. We may arrange the cycles of x and z so that

$$x = x^{(1)} x^{(2)} \cdots x^{(r)}$$

and

$$z = z^{(1)} z^{(2)} \cdots z^{(r)},$$

and the following conditions are satisfied:

(i) the $x^{(i)}$ are (disjoint) products of three signed 2-cycles, except for $x^{(r)}$ which is a (disjoint) product of two, three or four signed 2-cycles with a signed 1-cycle;

(ii) $\overline{x^{(i)}} = \overline{z^{(i)}}$ for each i; and

(iii) $w(x^{(i)}) \equiv w(z^{(i)}) \bmod 4$, for each $i < r$.

For $1 \leq i < r$, we may now consider each pair $x^{(i)}, z^{(i)}$ as elements of $C(B_6)$, while the pair $x^{(r)}, z^{(r)}$ may be considered as elements of $C(B_5)$, $C(B_7)$ or $C(B_9)$. Using Lemma 4.13 we now have $d(z, x) \leq 2$, and consequently there exists a path from t to x in $\mathcal{F}(G, X)$ of length at most 4. □

We can now say something about the local fusion graphs of the remaining involution classes of $C(B_n)$.

Theorem 4.18. *Let $G = C(B_n)$, where $n \geq 4$, and let X be a G-conjugacy class of involutions where the elements of X contain at least one 1-cycle. Then $\mathcal{F}(G, X)$ is connected, with*

$$\mathrm{Diam}(\mathcal{F}(G, X)) \leq n - 1$$

if n is even, and

$$\mathrm{Diam}(\mathcal{F}(G, X)) \leq n - 2$$

if n is odd.

Proof. When $n < 10$ this can be verified computationally using MAGMA, so assume $n \geq 10$. Suppose $t, x \in X$, and without loss of generality assume that

$$x = (\overset{+}{1}, \overset{+}{2}) \cdots (2\overset{+}{r} - 1, \overset{+}{2r})(2r \overset{-}{+} 1) \cdots (\overset{-}{s})(s \overset{+}{+} 1) \cdots (\overset{+}{n}).$$

Since we have dealt with signed transpositions in Theorem 4.11, we may assume that $r \geq 2$. By Theorem 1.1 of [7] there exists some $y \in X$ such that $d(t, y) \leq 2$ and $\overline{y} = \overline{x}$, which without loss of generality we may label so that

$$y = (1, 2) \cdots (2r - 1, 2r)(2r \overset{\epsilon_{2r+1}}{+} 1) \cdots (\overset{\epsilon_s}{s})(s \overset{\epsilon_{s+1}}{+} 1) \cdots (\overset{\epsilon_n}{n}),$$

where $\epsilon_i \in \{+, -\}$ for $i \in \{2r+1, \ldots, n\}$, and we make no assumption on the signs of the 2-cycles of y. Note that $w_1(xy)$ must be even by Proposition 4.6. Suppose that x and y differ by $2k$ signed 1-cycles. Since $r \geq 2$ it must be that $2k \leq n - 4$.

If $k = 0$ then, by ignoring all but one 1-cycle of x and y, we may apply Lemma 4.17 to see that $d(y, x) \leq 4$, and so $d(t, x) \leq 2+4 = 6$, which suffices since we have assumed $n \geq 10$.

Next, suppose that $k = 1$. If we ignore all 2-cycles of x and y except $(1, 2)$, we can consider the resulting elements $\tilde{x}$ and $\tilde{y}$ as signed transpositions in $K = C(B_\Sigma)$, where $\Sigma = \Omega \setminus \{3, \ldots, 2r\}$. By Lemma 4.9, there exists a path in $\mathcal{F}(K, \tilde{X})$ from $\tilde{y}$ to $\tilde{x}$ (where $\tilde{X}$ is the K-conjugacy class which contains $\tilde{x}$), which has length 3. This induces a path of length 3 in $\mathcal{F}(G, X)$ from y to an element $z \in X$, where $\overline{z} = \overline{x}$, and z and x agree on all signed 1-cycles. Now, since elements of X contain at least one 1-cycle, Lemma 4.17 implies that $d(z, x) \leq 4$, and so $d(t, x) \leq 2 + 3 + 4 = 9$, and again the result holds.

Now assume that $k \geq 2$. Since $r \geq 2$ we may also assume that both x and y contain the 2-cycles $(1, 2)$ and $(3, 4)$. We may partition $\text{supp}_C(xy) \setminus \Delta_{x,y}$ into two subsets A and B, such that the following conditions hold:

(i) $|A| = |B| = k$, or $|A| = k + 1$ and $|B| = k - 1$;

(ii) if we write $K_1 = C(B_{\Sigma_1})$ and $K_2 = C(B_{\Sigma_2})$, where $\Sigma_1 = \{1, 2\} \cup A$ and $\Sigma_2 = \{3, 4\} \cup B$, and for $i = 1, 2$ let $\tilde{x}_i, \tilde{y}_i \in K_i$ be the elements of K_i we get by ignoring all cycles of x and y respectively which fix Σ_i pointwise, then $\tilde{x}_i$ and $\tilde{y}_i$ are K_i-conjugate.

In view of Proposition 4.6, condition (ii) above is equivalent to requiring $w_1(\tilde{x}_i) = w_1(\tilde{y}_i)$. By Lemma 4.9, there exist paths in $\mathcal{F}(K_i, \tilde{X}_i)$ from $\tilde{y}_i$ to $\tilde{x}_i$ (where $\tilde{X}_i$ is the K_i-conjugacy class which contains $\tilde{x}_i$, for $i = 1, 2$). Since for each i we have $w_1(\tilde{x}_i\tilde{y}_i) \leq k+1$, these paths will be of length at most $k+2$. Since all elements of $\tilde{X}_1$ fix Σ_2 pointwise, and all elements of $\tilde{X}_2$ fix Σ_1 pointwise, we may multiply elements from these paths together to yield a path in $\mathcal{F}(G, X)$ of length at most $k+2$, between y and an element $z \in X$ such that $\overline{z} = \overline{x}$, and z and x agree on all signed 1-cycles. By Lemma 4.17, $d(z, x) \leq 4$, so

$$d(t, x) \leq 2 + (k + 2) + 4 = k + 8.$$

First assume that $r \geq 4$. Then $2k \leq n - 8$, and hence $k \leq n/2 - 4$. This yields

$$d(t, x) \leq n/2 + 4.$$

Now assume that $r = 2$ or 3. Here we may apply Lemma 4.13 to show that $d(z, x) \leq 2$, and so in this case we have

$$d(t, x) \leq 2 + (k + 2) + 2 = k + 6.$$

But $r \geq 2$, and so $2k \leq n - 4$ which implies $k \leq n/2 - 2$. Consequently,

$$d(t, x) \leq n/2 + 4$$

in this case also. Since $n \geq 10$, and $d(t, x)$ must be an integer, we have that $d(t, x) \leq n - 1$ when n is even, and $d(t, x) \leq n - 2$ when n is odd, as required. □

Notice that the establishment of Theorem 4.18 completes the proofs of Theorems 4.2 and 4.4. We also have the following corollary, which completes the proof of Theorem 4.3.

Corollary 4.19. *Let $G = C(D_n)$, with X a G-conjugacy class of involutions whose elements contain at least one 2-cycle. Then $\mathcal{F}(G, X)$ is connected, with $\mathrm{Diam}(\mathcal{F}(G, X)) \leq n - 1$ if n is even, and $\mathrm{Diam}(\mathcal{F}(G, X)) \leq n - 2$ if n is odd.*

Proof. This follows from Theorems 4.11 and 4.18, along with Lemma 4.16 and Proposition 4.6, which tells us that the conjugacy class X of $C(B_n)$ for which the local fusion graph has two connected components splits into two classes in G, with local fusion graphs isomorphic to a connected component of the $C(B_n)$ graph. □

4.3 The Exceptional Coxeter Groups

We conclude by examining the local fusion graphs of the finite, exceptional Coxeter groups. The cases when $G = C(I_n)$ (the dihedral groups) are covered by the following easy lemma.

Lemma 4.20. *Let $G = C(I_n)$. If n is odd then there is exactly one conjugacy class of involutions, and the local fusion graph is the complete graph on n vertices. If n is even then G has a central involution, and precisely two further conjugacy classes of involutions. If we write $n = 2^k m$, where m is odd, then each of these local fusion graphs has $n/2$ vertices, with k connected components, each component being a copy of the complete graph on m vertices.*

When $G = C(E_6)$, $C(E_7)$, $C(E_8)$, $C(F_4)$, $C(H_3)$ and $C(H_4)$, we proceed computationally. Representations of these groups are stored in MAGMA [18], and all are small enough to make explicit calculation of their local fusion graphs straightforward. Table 4.2 list the disc sizes for each local fusion graph of each group, along with representative involutions from each conjugacy class, given as words in the generators stored by MAGMA.

Table 4.2: Disc sizes for exceptional Coxeter groups

Group	Representative	Class size	$\lvert\Delta_1(t)\rvert$	$\lvert\Delta_2(t)\rvert$	$\lvert\Delta_3(t)\rvert$
$C(E_6)$	w_1	36	20	15	–
$C(E_6)$	w_0	45	32	12	–
$C(E_6)$	w_1w_2	270	128	141	–
$C(E_6)$	$w_1w_2w_6$	540	212	327	–
$C(E_7)$	w_0	1	–	–	–
$C(E_7)$	w_1	63	32	30	–
$C(E_7)$	w_0w_1	63	32	30	–
$C(E_7)$	$w_2w_5w_7$	315	128	186	–
$C(E_7)$	$w_0w_2w_5w_7$	315	128	186	–
$C(E_7)$	w_1w_2	945	416	528	–
$C(E_7)$	$w_0w_1w_2$	945	416	528	–
$C(E_7)$	$w_0w_1w_2w_5w_7$	3780	1568	2211	–
$C(E_7)$	$w_1w_2w_5w_7$	3780	1568	2211	–
$C(E_8)$	w_0	1	–	–	–
$C(E_8)$	w_1	120	56	63	–
$C(E_8)$	w_0w_1	120	56	63	–
$C(E_8)$	$(w_2w_3w_4w_5)^3$	3150	512	2588	49
$C(E_8)$	w_1w_2	3780	1472	2307	–
$C(E_8)$	$w_0w_1w_2$	3780	1472	2307	–
$C(E_8)$	$w_1w_2w_5$	37800	12344	25455	–
$C(E_8)$	$w_0w_1w_2w_5$	37800	12344	25455	–
$C(E_8)$	$w_1w_2w_5w_7$	113400	25280	88118	1
$C(F_4)$	w_0	1	–	–	–
$C(F_4)$	w_1	12	8	3	–
$C(F_4)$	w_0w_1	12	8	3	–
$C(F_4)$	w_3	12	8	3	–
$C(F_4)$	w_0w_3	12	8	3	–
$C(F_4)$	$(w_2w_3)^2$	18	–	–	–
$C(F_4)$	w_1w_3	72	24	46	1
$C(H_3)$	w_0	1	–	–	–
$C(H_3)$	w_1	15	12	2	–
$C(H_3)$	w_0w_1	15	12	2	–
$C(H_4)$	w_0	1	–	–	–
$C(H_4)$	w_1	60	44	15	–
$C(H_4)$	w_0w_1	60	44	15	–
$C(H_4)$	w_1w_3	450	168	280	1

Chapter 5

Sporadic Simple Groups

In this chapter we investigate the local fusion graphs of the sporadic simple groups. Recall from the Classification of Finite Simple Groups that these are as follows:

- M_{11}, M_{12}, M_{22}, M_{23}, M_{24} (the Mathieu groups);
- Co_1, Co_2, Co_3, McL, HS, Suz, J_2 (the Leech lattice groups);
- Fi_{22}, Fi_{23}, Fi'_{24} (the Fischer groups);
- $\mathbb{M}$, $\mathbb{B}$, Th, HN, He (the 'Monstrous' groups);
- J_1, J_3, J_4, $O'N$, Ru, Ly (the 'pariahs').

Our naming of the collections of sporadics follows Wilson in [65]. Much of the summary material in this chapter is also derived from this source.

As touched upon in Chapter 1, our approach to dealing with the sporadic groups is largely computational. This is made possible by the fact that the complex character tables of the sporadics are known, and can be found in the Atlas [26], or stored in Magma [18] or GAP [36]. Let us now explain why this is of use to us. Suppose G is a finite group, with conjugacy classes $\mathcal{K}_1, \ldots, \mathcal{K}_l$, and let $K_1, \ldots, K_l$ be the corresponding class sums in the group algebra $\mathbb{C}G$. Let a_{ijk} be the integers defined by

$$K_i K_j = \sum_{k=1}^{l} a_{ijk} K_k.$$

These integers are known as the *class structure constants*. Now let $\{g_1, \ldots, g_l\}$ be a complete set of conjugacy class representatives for G. Then we have

$$a_{ijk} = \frac{|\mathcal{K}_i||\mathcal{K}_j|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_i)\chi(g_j)\overline{\chi(g_k)}}{\chi(1)}.$$

The integers a_{ijk} are therefore determined by the character table of G. For further details on class structure constants we refer the reader to [38].

Note that a_{ijk} is precisely the number of pairs of elements (x, y), where $x \in \mathcal{K}_i$, $y \in \mathcal{K}_j$, such that $xy = z$, where z is some fixed element of $\mathcal{K}_k$. Thus if t is a fixed involution in a conjugacy class K_i, then

$$|\Delta_1(t)| = \sum_j a_{iji},$$

where the sum is over all j such that the conjugacy class $\mathcal{K}_j$ contains elements of odd order (excluding the conjugacy class of the identity element). Therefore, given the character table of a group, it is a relatively easy calculation to find the sizes of the first discs of the relevant local fusion graphs.

In fact, these first disc sizes tell us more than at first glance. For suppose a local fusion graph $\mathcal{F}(G, X)$ is disconnected, with m connected components. Then since G acts on the set of connected components, there is a homomorphism $\phi : G \to \mathrm{Sym}(m)$. If G is a simple group, then of course ϕ must be injective. However, a comparison between conjugacy class and first disc sizes for each local fusion graph of each sporadic group indicates that, in all cases, m is far too small for ϕ to possibly be injective. We deduce the following:

Theorem 5.1. *Let G be a sporadic finite simple group, with X a G-conjugacy class of involutions. Then the local fusion graph $\mathcal{F}(G, X)$ is connected.*

In fact, for many of the sporadic groups we can make use of additional methods to deduce further structural properties of their local fusion graphs. For the remainder of this chapter we give details of the computational techniques involved in each case, along with tables of the disc sizes of the local fusion graphs, where known.

5.1 The Mathieu Groups

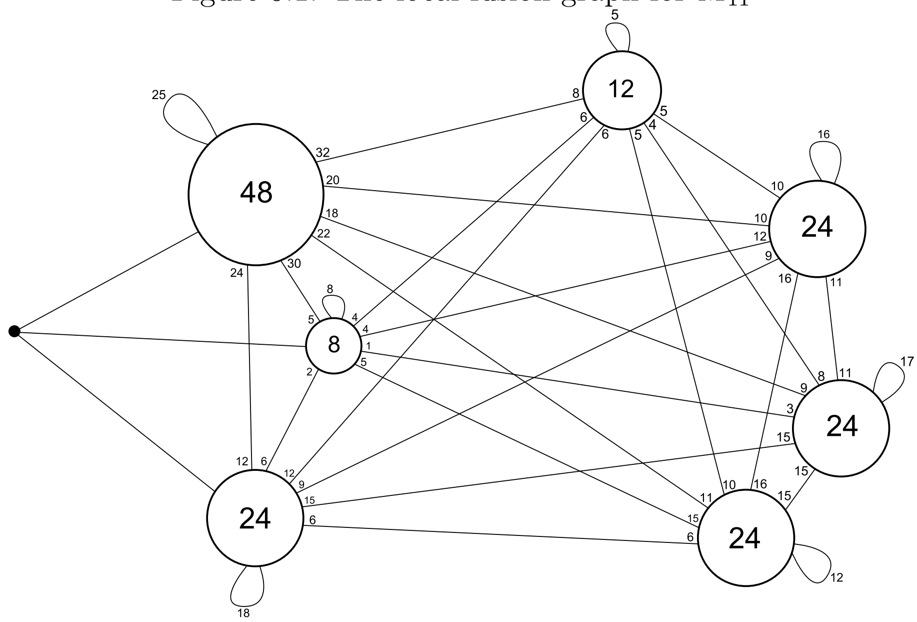
The first family of sporadic simple groups we encounter are the *Mathieu groups*, which were discovered by Emile Mathieu in the 19th century (see [51] and [52]). The largest Mathieu group M_{24} may be viewed as the automorphism group of the *(extended binary) Golay code*, a certain 12-dimensional subspace V of a 24-dimensional $\mathbb{F}_2$-vector space which M_{24} acts upon. Further details of how to work with M_{24} in practice using the 'Miracle Octad Generator' may be found in [29]. The group M_{23} is defined to be the stabiliser in M_{24} of a point, while M_{22} is defined to be the (pointwise) stabiliser in M_{24} of two points. Thus these groups can be realised as permutation groups on 24, 23 and 22 points respectively. The group M_{12} is defined as the stabiliser of a vector of weight 12 in V (a *dodecad*), and M_{11} is the stabiliser in M_{12} of a point.

We now give the disc sizes for the local fusion graphs of the Mathieu groups. These were calculated using Magma, with the natural permutation representations for each group, as mentioned above, taken from the online Atlas [1]. As noted previously, the size of the first disc may be easily calculated using the character table, or otherwise. The groups M_{11} and M_{12} are sufficiently small that, for each conjugacy class of involutions, the local fusion graph may be constructed explicitly via direct calculation. However, this method proves impractical for the larger Mathieu groups. In these cases we construct a complete set of double coset representatives of $C_G(t)$ in G using the Magma command `DoubleCosetRepresentatives`. We then partition this set into two parts A and B, with $x \in A$ if and only if tt^x has odd order. Thus conjugating t be the elements of A yields precisely representatives of the $C_G(t)$-orbits of $\Delta_1(t)$, plus t itself. Now for each $x \in B$ we take random $C_G(t)$-conjugates of t^x, using the Magma command `Random`, until we find t^{xg} such that $t^a t^{xg}$ has odd order for some $a \in A$. Then $t \to t^{ag^{-1}} \to t^x$ is a path of length 2 from t to t^x in $\mathcal{F}(G, X)$. This demonstrates that the local fusion graph has diameter 2, and since we know the size of the first disc, the size of the second disc follows. These disc sizes are given in Table 5.1, while Figure 5.1 shows the (unique) local fusion of M_{11}, where each $C_G(t)$-orbit has been collapsed to a point.

Table 5.1: Disc sizes for the Mathieu groups

Group	Class	Class size	$\lvert\Delta_1(t)\rvert$	$\lvert\Delta_2(t)\rvert$
M_{11}	2A	165	80	84
M_{12}	2A	396	180	215
M_{12}	2B	495	176	318
M_{22}	2A	1155	576	578
M_{23}	2A	3795	1344	2450
M_{24}	2A	11385	2816	8568
M_{24}	2B	31878	10880	20997

Figure 5.1: The local fusion graph for M_{11}



5.2 The Leech Lattice Groups

The *Leech Lattice* is closely connected to the Golay code. It may be defined as the set Λ of integral vectors $(x_1, \ldots, x_{24})$ which satisfy the following conditions:

- $x_i \equiv m \bmod 2$, for $1 \leq i \leq 24$;
- $\sum_{i=1}^{24} x_i \equiv 4m \bmod 8$; and
- for each k, the set $\{i : x_i \equiv k \bmod 4\}$ is in the Golay code.

The automorphism group of Λ may be considered as a group of 24-dimensional matrices. It has a central involution (namely $-I_{24}$), but after factoring this out we have a simple group, Co_1. The Leech Lattice may be equipped with a norm $\frac{1}{8}\sum_{i=1}^{24} x_i^2$. Then the stabilisers in Co_1 of vectors of norms 4 and 6 are also simple groups, denoted Co_2 and Co_3 respectively.

Once more we proceed computationally using Magma, and the double coset procedure described previously, using matrix representations from the online Atlas. This is straightforward in the majority of cases; however, for the largest group Co_1 Magma's inbuilt command `DoubleCosetRepresentatives` fails as the index $[G : C_G(t)]$ is too large. Fortunately, explicit matrix representatives for the $C_G(t)$-orbits of Co_1 have been calculated by Bates and Rowley in [15].

Table 5.2: Disc sizes for the Leech lattice groups

Group	Class	Class size	$\|\Delta_1(t)\|$	$\|\Delta_2(t)\|$
Co_3	2A	170775	59264	111510
Co_3	2B	2608200	904112	1704087
Co_2	2A	56925	14336	42588
Co_2	2B	1024650	379904	644745
Co_2	2C	28690200	5084672	23605527
Co_1	2A	46621575	13451264	33170311
Co_1	2B	2065694400	902774912	1162919488
Co_1	2C	10680579000	3014586368	7665992632
J_2	2A	315	224	90
J_2	2B	2520	1212	1307
HS	2A	5775	2304	3470
HS	2B	15400	7152	8247
McL	2A	22275	10304	11970
Suz	2A	135135	69632	65502
Suz	2B	2779920	1454432	1325487

5.3 The Fischer Groups

The groups Fi_{22}, Fi_{23} and Fi'_{24} were discovered by Bernd Fischer in the 1970s [35], as a result of his study of 3-*transposition groups*. These were defined to be finite groups G such that $G = \langle X \rangle$, where X is a G-conjugacy class of involutions, such that the product of any two elements of X has order at most 3. Additionally, it was required that $G' = G''$ and any normal 2- or 3-subgroup of G is central. Fischer's original construction of his simple groups effectively made use of the commuting involution graph $\mathcal{C}(G,X)$, in the sense that he built a graph $\mathcal{G}$ with vertices corresponding to the elements of X, with distinct $x, y \in X$ joined by an edge if and only if x and y commute. He then showed that the derived group G' of $G := \mathrm{Aut}(\mathcal{G})$ was simple. Notice that since X consists of 3-transpositions, one can equivalently use the local fusion graph $\mathcal{F}(G,X)$ to define the Fischer groups, as in this case $\mathcal{F}(G,X)$ is simply the complementary graph of $\mathcal{C}(G,X)$. It should be emphasised that this construction presented a considerable challenge, since in effect Fischer had to construct $\mathcal{C}(G,X)$ and its automorphism group whilst assuming very little prior knowledge of the group G.

The size of the Fischer groups presents some difficulty in attempting to determine the disc sizes of their local fusion graphs computationally. For two involution classes of Fi_{22}, and one of Fi_{23} (including the class of 3-transpositions of each group) the diameter and disc sizes have been calculated using the double coset procedure described previously. However, for the remaining graphs we are content to calculate the size of the first disc in each case, and deduce that the graph is connected.

Table 5.3: Disc sizes for the Fischer groups

Group	Class	Class size	$\lvert\Delta_1(t)\rvert$	$\lvert\Delta_2(t)\rvert$
Fi_{22}	2A	3510	2816	693
Fi_{22}	2B	1216215	484352	731862
Fi_{22}	2C	36468450	12015872	
Fi_{23}	2A	31671	28160	3510
Fi_{23}	2B	55582605	15234560	
Fi_{23}	2C	12839581755	3308650496	
Fi'_{24}	2A	4860485028	1504701440	
Fi'_{24}	2B	7819305288795	3351534645248	

5.4 The Monstrous Groups

The Monster group, $\mathbb{M}$, is the largest of the sporadic simple groups, with order

$$|\mathbb{M}| = 808017424794512875886459904961710757005754368000000000.$$

Although predicted to exist by Fischer, it was first constructed by Griess in 1981 [40]. We make no attempt to describe this construction here, but simply note that the smallest real representation of $\mathbb{M}$ is in 196883 dimensions. Of the sporadic simple groups, 20 are 'involved' in some way in the Monster. In particular, it contains, as quotients of subgroups, the other sporadic simple groups we address in this section, namely the 'Baby Monster' $\mathbb{B}$, the Thompson group Th, the Harada-Norton group HN, and the Held group He.

Despite its enormous size, the complex character table of $\mathbb{M}$ is known, and stored in GAP. It is therefore straightforward to calculate the sizes of the first discs of its local fusion graphs. This is similarly achievable for $\mathbb{B}$ and HN. For He and Th we can go further, and determine diameters and all disc sizes. This is done using the standard double coset procedure in the case of He, while for Th we make use of explicit double coset representatives calculated by Rowley and Taylor in [56].

Table 5.4: Disc sizes for the Monstrous groups

Group	Class	Class size	$\|\Delta_1(t)\|$	$\|\Delta_2(t)\|$
He	2A	24990	4992	19997
He	2B	187425	119552	67872
Th	2A	976841775	377298944	599542830
HN	2A	1539000	391424	
HN	2B	74064375	26906624	
$\mathbb{B}$	2A	13571955000	2370830336	
$\mathbb{B}$	2B	11707448673375	4010408935424	
$\mathbb{B}$	2C	156849238149120000	56546114902065210	
$\mathbb{B}$	2D	355438141723665100	94228887171498040	
$\mathbb{M}$	2A	97239461142009240000	30528114911948600000	
$\mathbb{M}$	2B	5791748068511982000000000000	1486325429210110000000000000	

5.5 The Pariahs

The six sporadic simple groups we have not encountered so far have been referred to as the 'pariahs', due to the fact that they are not involved in the Monster. These are the Rudvalis group Ru, the O'Nan group $O'N$, the Lyons group Ly, and three of the Janko groups, J_1, J_3 and J_4. Again, we make no attempt here to describe their constructions.

The groups J_1 and J_3 are relatively small, having orders 175560 and 50232960 respectively, and as such we may explicitly calculate their local fusion graphs in MAGMA or GAP. For Ru, we can determine the diameter and disc sizes of its local fusion graphs using the double coset procedure. This data can also be determined for J_4. For its involution class $2A$ we use explicit double coset representatives calculated by Rowley and Taylor in [57], while for the class $2B$ the size of the first disc implies diameter 2 by Lemma 1.16. This latter situation also occurs for the local fusion graph of Ly. For the group $O'N$ we have not determined the diameter of the local fusion graph, but have calculated the size of the first disc using GAP, and deduced that the graph is connected.

Table 5.5: Disc sizes for the pariahs

Group	Class	Class size	$\|\Delta_1(t)\|$	$\|\Delta_2(t)\|$
J_1	2A	1463	1072	390
J_3	2A	26163	16832	9330
J_4	2A	3980549947	1112555520	2867994426
J_4	2B	47766599364	26545360896	21221238467
Ru	2A	593775	149504	444270
Ru	2B	1252800	570752	682047
Ly	2A	1296826875	659509424	637317450
$O'N$	2A	2857239	1079168	

Chapter 6

A Review of Finite Groups of Lie-Type

The purpose of this chapter is to briefly review the construction, and various well known properties, of the finite groups of Lie-type. This will stand us in good stead for the following two chapters, where we study the local fusion graphs of such groups. Many familiar groups are finite groups of Lie-type, including the classical matrix groups, and the projective groups associated to these, and can be defined explicitly in various different ways. However, to fully appreciate the connection between such groups, and to gain a deeper understanding of their structure, it is necessary to view them in the framework of a more general theory. One such approach, which we shall now summarise, is to first study *algebraic groups*.

6.1 Algebraic Group Theory

Here we shall briefly summarise some of the basic theory of algebraic groups. As our aim is to quickly familiarise the reader with the objects and results we shall use in subsequent chapters, we shall often not give detailed definitions or proofs. For an in-depth introduction to the subject we refer the reader to [37].

Let k be an algebraically closed field, and consider the set of n-tuples k^n. If a subset $V \subseteq k^n$ can be defined as the vanishing set of a finite set of polynomials over

k, we say that V is an *affine variety.* If V also carries the structure of a group, and the multiplication

$$\mu : V \times V \to V$$

and inverse operation

$$\iota : V \to V$$

are morphisms of affine varieties, then we write $G = V$ and say that G is an *affine algebraic group.* We can define a topology on G, known as the *Zariski topology*, by defining the closed sets in the topology to be the subvarieties of G.

The standard example of an affine algebraic group is the special linear group $SL_n(k)$, which may be described as

$$SL_n(k) = \{(a_{ij}) \in k^{n^2} : \det(a_{ij}) - 1 = 0\}.$$

The general linear group $GL_n(k)$ can also be shown to be an affine algebraic group. Since any closed subgroup of $GL_n(k)$ will itself satisfy the conditions to be an affine algebraic group, we now have a plentiful supply of examples by considering the closed subgroups of $GL_n(k)$. Such groups are known as *linear algebraic groups.* In fact, it can be shown that every affine algebraic group is also linear. In light of this, henceforth we shall simply use the term 'algebraic group' to describe a linear or affine algebraic group. Additionally, this allows us to use properties of matrices when considering elements of algebraic groups.

6.2 Subgroups of Algebraic Groups

Let V be a finite dimensional vector space over an algebraically closed field k. An element $x \in \mathrm{End}(V)$ is called *semisimple* if is diagonalisable, and is called *unipotent* if its only eigenvalue is 1. The *(multiplicative) Jordan decomposition* is a fundamental result regarding such elements, and runs as follows:

Theorem 6.1. *Let V be a vector space over an algebraically closed field, and suppose $x \in \mathrm{End}(V)$. Then x can be expressed uniquely as $x = x_s x_u$, where x_s is semisimple, x_u is unipotent, and x_s and x_u commute.*

Since any (linear) algebraic group G is a subgroup of $GL(V)$ for some V, it makes sense to talk about semisimple and unipotent elements of G. The *radical* of an algebraic group G is defined to be the (unique) subgroup $R(G)$ generated by all closed, connected, soluble, normal subgroups of G. The subgroup of $R(G)$ consisting of all its unipotent elements is called the *unipotent radical* of G, denoted $R_u(G)$. If $R_u(G) = 1$ we say G is *reductive*, while if $R(G) = 1$ then G is called *semisimple*. An algebraic group is said to be *simple* if it has no proper, closed, connected, normal subgroups.

A subgroup $T \leq G$ such that $T \cong k^* \times \cdots \times k^*$ is called a *torus* of G, and consists of semisimple elements. Conversely, any semisimple element of G lies in a torus of G. A *Borel subgroup* of G is a maximal, closed, connected, soluble subgroup of G. The following theorem collects together some important results regarding tori and Borel subgroups:

Theorem 6.2. *Let G be an algebraic group defined over an algebraically closed field. Then the following hold:*

(i) All maximal tori in G are G-conjugate;

(ii) Any maximal torus lies in some Borel subgroup of G;

(iii) Any two Borel subgroups of G are G-conjugate;

(iv) If B is a Borel subgroup of G, then $N_G(B) = B$.

Proof. See [37]. □

6.3 Groups with a BN-pair

The notion of groups with a 'BN-pair' was introducted by Tits in [63], and is of fundamental importance in the study of groups of Lie-type. We first give the abstract definition, before explaining the relevance to algebraic groups.

Definition 6.3. Let G be a group, with B and N subgroups of G. Then B and N are said to form a *BN-pair* in G if the following conditions hold:

(i) $G = \langle B, N \rangle$;

(ii) $B \cap N \lhd N$;

(iii) $N/(B \cap N) = W$ is a finite group generated by a set S of involutions;

(iv) If $n_s \in N$ maps canonically to $1 \neq s \in W$, then $n_s B n_s \neq B$;

(v) $n_s B n \subseteq B n_s n B \cup BnB$ for any $s \in S$ and $n \in N$.

The group W in the definition above is called the *Weyl group* of G. Weyl groups are particular examples of Coxeter groups, as seen in Chapter 4. Now let G be an algebraic group. We say that G possesses a *split* BN-pair if the groups B and N satisfy the following conditions, in addition to those in the definition above:

(i) B and N are closed subgroups of G;

(ii) We may write $B = U(B \cap N)$, a semidirect product of a closed, normal, unipotent group U and a closed, commutative subgroup $B \cap N$ consisting of semisimple elements;

(iii) $\bigcap_{n \in N} nBn^{-1} = B \cap N$.

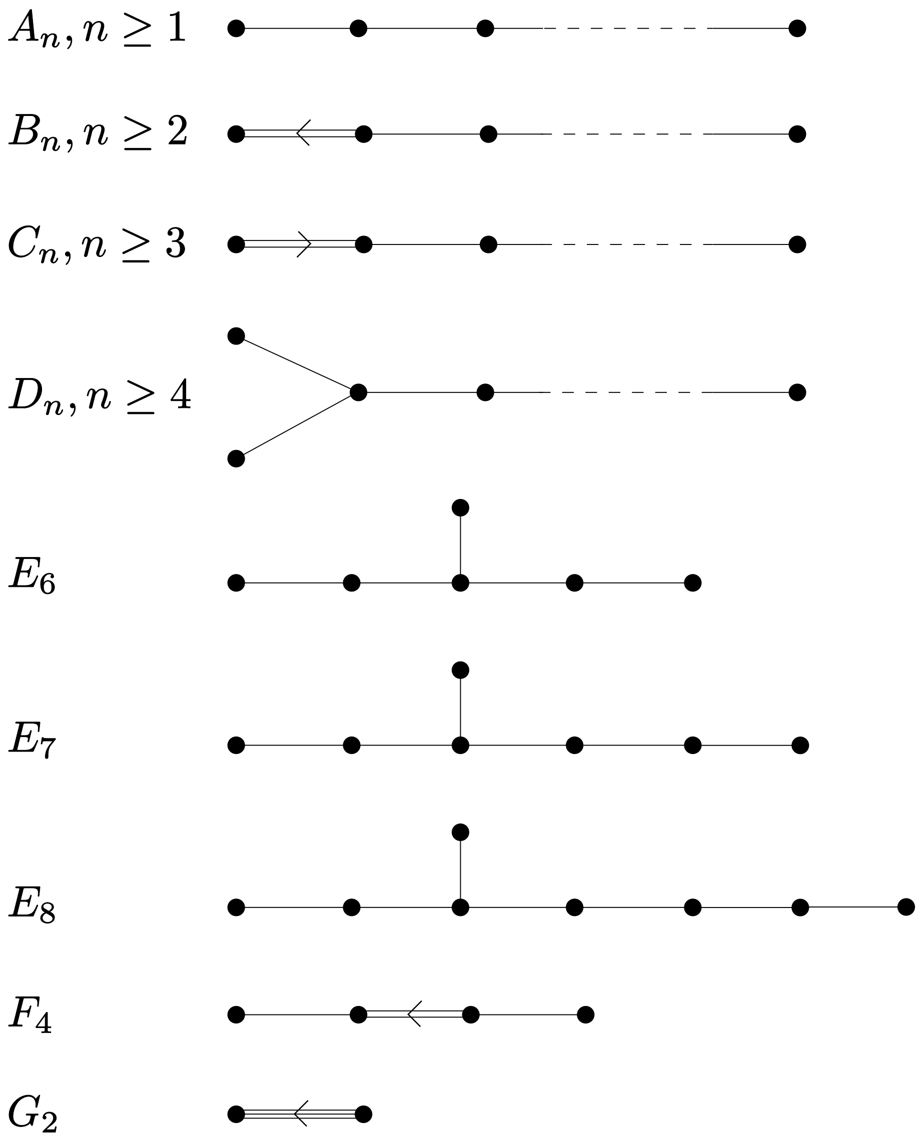
It can be shown (see [37], for example) that a connected reductive group G has a split BN-pair. If T is a maximal torus of G contained in a Borel subgroup B, then $B \cap N = T$ and $B = UT$, where $U = R_u(B)$.

To illustrate, suppose $G = SL_n(k)$. Then a Borel subgroup B of G is the group of upper triangular matrices. T is then the subgroup of diagonal matrices, U is the subgroup of upper uni-triangular matrices, and N is the group of monomial matrices.

6.4 Classification of Simple Algebraic Groups

The simple algebraic groups have been classified. To each connected, reductive algebraic group G there is an associated *Dynkin diagram.* Such diagrams describe the *root lattice* which G acts upon, and are closely related to the Coxeter diagrams described in Chapter 4. For G to be a simple algebraic group, its Dynkin diagram

Figure 6.1: Connected Dynkin diagrams



must be connected, and of one of the types listed in Figure 6.1. While G uniquely determines its Dynkin diagram, it is not necessarily the case that the Dynkin diagram uniquely determines G. For example, the Dynkin diagram of type A_n gives rise to both $SL_{n+1}(k)$ and $PGL_{n+1}(k)$. However, it can be shown that there are only finitely many simple algebraic groups with a given Dynkin diagram, and additional information regarding the action of of the Weyl group W on the root lattice uniquely determines the group. Further details on this process may be found in [25].

6.5 Finite Groups of Lie-Type

Thus far we have only considered algebraic groups over an algebraically closed field. However, we shall be primarily concerned with finite groups of Lie-type, so must explain how these arise.

Let $p > 0$ be a prime, and assume that k is an algebraic closure of the finite field $\mathbb{F}_p$. Let G be an algebraic group over k, and consider G as a closed subgroup of $GL_n(k)$. Let $q = p^r$ for some $r \geq 1$, and define a map $F_q : GL_n(k) \to GL_n(k)$ by

$$F_q : (a_{ij}) \mapsto (a_{ij}^q).$$

A homomorphism $F : G \to G$ is called a *standard Frobenius map* if there exists an injective homomorphism $i : G \to GL_n(k)$ for some n, such that

$$i(F(g)) = F_q(i(g))$$

for some $q = p^r$ and all $g \in G$. A homomorphism $F : G \to G$ is called a *Frobenius map* if some power of F is a standard Frobenius map.

Given a Frobenius map $F : G \to G$, the fixed point set

$$G^F = \{g \in G : g^F = g\}$$

is a finite subgroup of G. When G is a connected reductive algebraic group, then the groups G^F which arise are called *finite groups of Lie-type*. The classification of simple algebraic groups leads to a classification of the finite, simple groups of Lie-type. However, when the field is finite, additional simple groups arise through graph automorphisms of Dynkin diagrams. In this way, all the finite, simple groups of Lie-type listed in Theorem 1.6 can be realised.

The finite groups of Lie-type inherit many structural properties from the algebraic overgroup. In particular it can be shown that every group G^F has a split BN-pair. A Borel subgroup of G^F is defined to be a subgroup of the form B^F, where B is a Borel subgroup of G which is stable under the action of F. Similarly, a maximal torus of G^F is defined to be T^F, where T is an F-stable maximal torus of G which lies in an

F-stable Borel subgroup B^F. For such a torus T^F, $N = N_G(T^F)$ can also be shown to be F-stable, and then B^F and N^F form a split BN-pair for G^F.

Despite these nice properties, we must exercise caution when dealing with finite groups of Lie-type, since many results which hold in G may not necessarily hold in G^F. We first note that in a finite group of Lie-type G^F, an element $x \in G^F$ is defined to be *semisimple* if its order is coprime to the defining charactersitic p, and *unipotent* if its order is a power of p. Another point to note is that it is not always true that an F-stable maximal torus of G lies inside an F-stable Borel subgroup of G, and hence not every maximal torus of G^F lies inside a Borel subgroup of G^F. An F-stable maximal torus of G which does lie in an F-stable Borel subgroup of G is called *maximally split*, while a maximal split torus of G^F is defined to be a torus of the form T^F, where T is a maximal split torus of G.

The following result collects together some properties of Borel subgroups and maximal tori of finite groups of Lie-type:

Theorem 6.4. *Let G^F be a finite group of Lie-type. Then the following hold:*

(i) Any two Borel subgroups of G^F are G^F-conjugate;

(ii) Any two maximal tori which lie in B^F are B^F-conjugate;

(iii) Any two maximal split tori of G^F are G^F-conjugate.

Proof. See [37]. □

6.6 Classical Groups

As previously mentioned, the classical groups are groups of Lie-type, and as such arise through the constructions summarised so far in this chapter. However, they can also be defined in a more familiar way, via their action on vector spaces. We have already seen this when we defined the linear groups in Chapter 3. This natural geometric structure is a powerful tool in their study.

Let V be a vector space over a field k, and assume that $\dim V \geq 3$. The *projective geometry* $\mathcal{P}(V)$ is the set of all subspaces of V, partially ordered by inclusion. A *correlation* of $\mathcal{P}(V)$ is a bijection from $\mathcal{P}(V)$ to $\mathcal{P}(V)$ which reverses inclusion. A *polarity* of $\mathcal{P}(V)$ is a correlation of order 2, and the pair $(\mathcal{P}(V), \pi)$ is called a *polar geometry.*

Theorem 6.5 (Birkhoff-von Neumann)**.** *If π is a polarity of $\mathcal{P}(V)$, then π arises from a non-degenerate, reflexive form β of one of the following types:*

(i) Alternating, so $\beta(v, v) = 0$ for all $v \in V$;

(ii) Symmetric, so $\beta(u, v) = \beta(v, u)$ for all $u, v \in V$;

(iii) Hermitian, so $\beta(u, v) = \tau(v, u)$ for all $u, v \in V$, where τ is an involutory automorphism of the field k.

Proof. See Theorem 7.1 of [62]. □

We refer to the polar geometry as *symplectic*, *orthogonal* or *unitary* when (i), (ii) and (iii) hold and β is bilinear in cases (i) and (ii), and τ-sesquilinear in case (iii), respectively. Using these forms we may define the majority of the classical groups. However, to get the complete set there is a fourth type of form we must introduce, namely a *quadratic form*, $Q : V \to k$. For Q to be a quadratic form, by definition we must must have that

$$Q(av) = a^2 Q(v)$$

for all $a \in k$, and that $\beta : V \times V \to k$ defined by

$$\beta(u, v) := Q(u + v) - Q(u) - Q(v)$$

for all $u, v \in V$, is a bilinear form.

We may now define the classical groups. The *symplectic group* $Sp(V, \beta)$ is the subgroup of $GL(V)$ whose elements preserve a non-degenerate, reflexive, alternating form β on V, that is

$$Sp(V, \beta) = \{g \in GL(V) : \beta(u^g, v^g) = \beta(u, v) \text{ for all } u, v \in V\}.$$

It is only possible to define such a form on V if the dimension of V is even. Also, it can be shown that, up to change of basis, there is only one non-degenerate, reflexive, alternating form on a vector space of dimension $2n$, so we shall often just write $Sp(V)$. If the field k is finite of order q, we may also write $Sp_{2n}(q)$. It is straightfoward to show that all elements of $Sp_{2n}(q)$ have determinant 1, so in fact $Sp_{2n}(q) \leq SL_{2n}(q)$.

The *general unitary group* $GU(V, \beta)$ is defined in the same way as the symplectic group above, but here β is a non-degenerate, reflexive, hermitian form. Again, up to change of basis there is only one such form on a vector space of dimension n, so we usually just write $GU(V)$. If k is finite, then since we require k to possess an involutary automorphism, it must be the case that k has order q^2 for some q, a power of a prime p. Then τ acts by raising the elements of k to the power q. As in the symplectic case, we may also write $GU_n(q)$, but by convention this means our matrix entries are taken from the field $\mathbb{F}_{q^2}$. The subgroup of $GU_n(q)$ consisting of matrices with determinant 1 is the *special unitary group*, denoted $SU_n(q)$.

Before defining the orthogonal groups, we require some more terminology concerning vector spaces equipped with forms. Recall that if V is a vector space equipped with a form β of a type listed in Theorem 6.5, and if U is a subset of V, then

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

Definition 6.6. Let V be a vector space equipped with one of the forms in Theorem 6.5.

(i) We say a non-zero vector $u \in V$ is *isotropic* if $\beta(u, u) = 0$.

(ii) A subspace $W \subseteq V$ is called *totally isotropic* if $W \subseteq W^{\perp}$.

(iii) A pair of vectors (u, v) such that u and v are isotropic and $\beta(u, v) = 1$ is called a *hyperbolic pair*. The line $\langle u, v\rangle$ in $\mathcal{P}(V)$ is called a *hyperbolic line*.

(iv) A subspace $W \subseteq V$ is *non-degenerate* if $W \cap W^{\perp} = 0$.

(v) If $V = U \oplus W$ and $\beta(u, w) = 0$ for all $u \in U$ and $w \in W$, we say that V is the *orthogonal* direct sum of U and W, and write $V = U \perp W$.

Now suppose that V is equipped with a quadratic form Q.

(i) A non-zero vector $v \in V$ is called *singular* if $Q(u) = 0$.

(ii) A subspace $W \subseteq V$ is called *totally singular* if $Q(w) = 0$ for all $w \in W$.

Now let V be a vector space equipped with a non-singular quadratic form Q. The subgroup of $GL(V)$ consisting of elements which preserve Q is called the *orthogonal group* $O(V, Q)$. The derived subgroup $O(V, Q)'$ is denoted $\Omega(V, Q)$. Additionally, when the characteristic of k is odd, we define the *special orthogonal group* $SO(V, Q)$ to be the subgroup of $O(V, Q)$ consisting of matrices with determinant 1. Notice that if the characteristic of the field k is odd, then given a non-degenerate, relexive, symmetric bilinear form β on V, it is possible to define a quadratic form Q using the identity

$$\beta(u, v) := Q(u + v) - Q(u) - Q(v).$$

Indeed, we can let

$$2Q(u) = Q(u + u) - Q(u) - Q(u) = \beta(u, u),$$

for all $u \in V$, and so $Q(u) = \beta(u, u)/2$. However, this is not possible when the characteristic of k is even. Thus the introduction of quadratic forms is necessary to define orthogonal groups in even characteristic.

It can be shown that any two maximally totally isotropic (respectively totally singular) subspaces of a vector space V have the same dimension (see [62], for example). This common dimension is called the *Witt index* of the form β (respectively Q). If the form on a vector space V is understood we may instead refer to the Witt index of V. Now suppose that $k = \mathbb{F}_q$, and that V is equipped with a nonsingular quadratic form Q. If the dimension of V is $2m$, it can be shown that the Witt index of Q is either m or $m - 1$, while if the dimension of V is $2m + 1$, then the Witt index of Q must be m. Moreover, V is determined up to isomorphism by its dimension and the Witt index of Q. In the even dimension case, if the Witt index of Q is m then V is said to be of *plus-type*, and we write $O^+_{2m}(q)$ and $\Omega^+_{2m}(q)$ for the groups $O(V, Q)$ and $\Omega(V, Q)$, while if Q has Witt index $m - 1$ then V is of *minus-type*, and we write

$O^-_{2m}(q)$ and $\Omega^-_{2m}(q)$ respectively. For odd dimension we may unambiguously write $O_{2m+1}(q)$ and $\Omega_{2m+1}(q)$.

The following lemma allows us in many situations to choose a 'nice' basis for our vector space V.

Lemma 6.7. *If U and W are totally isotropic (respectively totally singular) subspaces of V such that $U^\perp \cap W = \{0\}$, then there is a totally isotropic (respectively totally singular) subspace U' containing W such that $V = U^\perp \oplus U'$. Moreover, for each basis $u_1, u_2, \ldots, u_k$ of U, there is a unique basis $u'_1, u'_2, \ldots, u'_k$ of U' such that $\langle u_1, u'_1\rangle, \langle u_2, u'_2\rangle, \ldots, \langle u_k, u'_k\rangle$ are mutually orthogonal hyperbolic pairs.*

Proof. This may be found in [62], Lemma 7.5. □

A *flag* of a projective geometry $\mathcal{P}(V)$ is a chain of distinct subspaces

$$V_1 \subset V_2 \subset \cdots \subset V_K,$$

and a flag is called *proper* if neither 0 nor V occurs in the chain. The *type* of such a flag is the set $\{d_1, \ldots, d_k\}$, where $d_i = \dim(V_i)$ for $i = 1, \ldots, k$. If $\dim(V) = m$, a *maximal* flag is one of type $\{1, 2, \ldots, m-1\}$. In a polar geometry $(\mathcal{P}, \pi)$, the flags are defined to be those flags of $\mathcal{P}(V)$ which are fixed by π. These can be identified with the flags of totally isotropic subspaces.

We can now state the following important result, which gives a geometric characterisation of the Borel subgroups of the majority of finite classical groups.

Theorem 6.8. *Suppose G is a classical group which acts on an $\mathbb{F}_q$-vector space V. If G is an orthogonal group assume that q is odd and G is not of plus-type. Then the Borel subgroups of G are precisely the stabilisers of maximal flags in a suitable polar geometry $(\mathcal{P}(V), \pi)$.*

The Borel subgroups of some of the orthogonal groups not included in Theorem 6.8 will be described when required in Chapter 7.

6.7 Maximal Subgroups

When investigating the local fusion graphs of finite groups of Lie-type, we shall require some knowledge of the maximal subgroup structure of such groups. We first have the following result concerning the centralisers of field automorphisms.

Theorem 6.9. *Let $G = G(q)$ be a finite, simple group of Lie-type, defined over the field $\mathbb{F}_q$. Suppose we may write $q = q_0^r$ where r is prime. Then $G(q_0)$ is a maximal subgroup of G, where $G(q_0)$ denotes the finite group of the same type defined over the field $\mathbb{F}_{q_0}$.*

Proof. This is an immediate consequence of Theorem 1 in [21]. □

When dealing with classical groups, more detailed information regarding maximal subgroups will be required. In [50], Kleidman and Liebeck determine much of the maximal subgroup structure of the finite classical groups with dimension at least 13, while the lower dimensional cases are covered in [48]. We shall need but a fraction of the information contained in these sources, and include only the relevant results here.

Theorem 6.10. *Let $H = Sp_n(q)$ where $n \geq 6$. Suppose $M = \mathrm{Stab}_H(W)$, where $W \subseteq V$ is a non-degenerate subspace of even dimension m, with $2 \leq m < n/2$. Then M and $\overline{M}$ are maximal subgroups of H and $\overline{H}$ respectively. Moreover,*

$$M \cong Sp_m(q) \times Sp_{n-m}(q)$$

and

$$\overline{M} \cong Sp_m(q) \circ Sp_{n-m}(q).$$

Proof. See Proposition 4.1.3 of [50]. □

Theorem 6.11. *Let $H = SU_n(q)$, where $n \geq 3$. Suppose $M = \mathrm{Stab}_H(W)$, where $W \subseteq V$ is a non-degenerate subspace of dimension $0 < m < n/2$. Then M and $\overline{M}$ are maximal subgroups of H and $\overline{H}$ respectively. Moreover,*

$$SU_m \times SU_{n-m}(q) \leq M \leq GU_m \times GU_{n-m}(q).$$

Proof. See Proposition 4.1.4 of [50]. □

Theorem 6.12. *Let $H = SU_n(q)$, where $n \geq 3$ and q is odd. Suppose that M is the stabiliser of a decomposition*

$$V = W_1 \perp W_2 \perp \ldots \perp W_k$$

where $\dim W_i = m < n$, *for* $1 \leq i \leq k$. *Then M and $\overline{M}$ are maximal subgroups of H and $\overline{H}$ respectively, and*

$$SU_m(q) \wr \mathrm{Sym}(k) \leq M \leq GU_m(q) \wr \mathrm{Sym}(k).$$

Proof. See Proposition 4.2.9 of [50]. □

Theorem 6.13. *Let $H = SO_n^{\epsilon}(q)$, where q is odd, $n \geq 6$ and $\epsilon = \pm$. Suppose* $M = \mathrm{Stab}_H(W)$, *where $W \subseteq V$ is a totally singular subspace of dimension* $0 < m < n/2 - 1$. *Then M and $\overline{M}$ are maximal subgroups of H and $\overline{H}$ respectively. Moreover,*

$$M \cong [q^a] : (GL_m(q) \times SO_{n-2m}^{\epsilon}(q))$$

and

$$\overline{M} \cong [q^a] : (GL_m(q) \circ SO_{n-2m}^{\epsilon}(q)),$$

where $a = mn - \frac{m}{2}(3m+1)$.

Proof. See Proposition 4.1.20 of [50]. □

Theorem 6.14. *Let $H = \Omega_n^{+}(q)$, where q is even and $n \equiv 0 \bmod 4$. Suppose* $M = \mathrm{Stab}_H(W \oplus W')$, *where $V = W \oplus W'$ is a decomposition of V into totally singular subspaces of dimension $n/2$. Then M is a maximal subgroup of H. Moreover,*

$$M \cong GL_{n/2}(q).2,$$

where the outer automorphism of $GL_{n/2}(q)$ is an involution which has the effect of swapping W with W'.

Proof. See Proposition 4.1.20 of [50]. □

Theorem 6.15. *Let $H = SO_n^{\epsilon}(q)$, where $n \geq 6$ and $\epsilon = \pm$. Suppose $M = \mathrm{Stab}_H(W)$, where $W \subseteq V$ is a non-degenerate subspace of dimension m and type $\eta = \pm$. In addition, assume that $0 < m < n/2$ and that when $q \leq 3$ we have $(\eta, m) \neq (+, 2)$. Then M and $\overline{M}$ are maximal subgroups of H and $\overline{H}$ respectively. Moreover,*

- *when $\epsilon = +$ we have*

$$SO_m^{\eta}(q) \times SO_{n-m}^{\eta}(q) \leq M \leq O_m^{\eta}(q) \times O_{n-m}^{\eta}(q);$$

- *when $\epsilon = -$ we have*

$$SO_m^{\eta}(q) \times SO_{n-m}^{-\eta}(q) \leq M \leq O_m^{\eta}(q) \times O_{n-m}^{-\eta}(q).$$

Proof. See Proposition 4.1.6 of [50]. □

6.8 Generation of Classical Groups

We conclude this chapter by collecting together some results regarding generating sets for classical groups with respect to certain bases. These will be of use to us in Chapters 7 and 8.

Proposition 6.16. *If $G = SL_n(q) \cong SL(V)$ and $n \geq 4$, then G is generated by the set*

$$\mathcal{A} = \{I + \lambda e_{ij} : i \neq j\},$$

where the $\{e_{ij}\}$ are elementary matrices. Moreover, when i is odd and $j = i+1$, and when i is even and $j = i-1$, we may exclude the corresponding matrices from $\mathcal{A}$ and the resulting set $\mathcal{A}'$ still generates G.

Proof. It is well known that the set $\mathcal{A}$ generates G (see [61], for example). Now let $I + \lambda e_{ij} \in \mathcal{A}$ be such that i is odd and $j = i + 1$. Then a matrix calculation shows that

$$I + \lambda e_{ij} = (I + e_{ik})(I + \lambda e_{kj})(I - e_{ik})(I - \lambda e_{kj}),$$

and due to the restrictions on i, j, and our assumption that $n \geq 4$, it is possible to choose k such that all the matrices on the right hand side of this equation lie in $\mathcal{A}'$. A similar equality holds when i is even and $j = i - 1$. □

Proposition 6.17. *Let $G = Sp_{2n}(q) \cong Sp(V)$, where the symplectic form β on V has Gram matrix*

$$J = \left(\begin{array}{c|c} & I_n \\ \hline -I_n & \end{array}\right).$$

Then G is generated by the matrices

$$\left(\begin{array}{c|c} I_n & \lambda e_{ii} \\ \hline & I_n \end{array}\right), \left(\begin{array}{c|c} I_n & \\ \hline \lambda e_{ii} & I_n \end{array}\right),$$

$$\left(\begin{array}{c|c} I_n & \lambda(e_{ij}+e_{ji}) \\ \hline & I_n \end{array}\right), \left(\begin{array}{c|c} I_n & \\ \hline \lambda(e_{ij}+e_{ji}) & I_n \end{array}\right).$$

Proof. Looking in Section 2.2 of [53], we see that G is certainly generated by the matrices given above along with those of the form

$$\left(\begin{array}{c|c} I_n + \lambda e_{ij} & \\ \hline & I_n - \lambda e_{ji} \end{array}\right).$$

However, a straightforward matrix calculation shows that

$$\left(\begin{array}{c|c} I_n + \lambda e_{ij} & \\ \hline & I_n - \lambda e_{ji} \end{array}\right) = \left(\begin{array}{c|c} I_n & \\ \hline e_{ij}+e_{ji} & I_n \end{array}\right)^{gh}$$

where

$$g = \left(\begin{array}{c|c} I_n & -\lambda e_{ii} \\ \hline & I_n \end{array}\right)$$

and

$$h = \left(\begin{array}{c|c} I_n & \\ \hline \lambda^{-1} e_{ii} & I_n \end{array}\right),$$

where $i < j$. A similar relation holds when $i > j$. □

Proposition 6.18. *Let $G = SU_{2n}(q) \cong SU(V)$ where q is even, and the unitary form β on V has Gram matrix*

$$J = \left(\begin{array}{c|c} & I_n \\ \hline I_n & \end{array}\right).$$

Denote by τ the involutary automorphism of $\mathbb{F}_{q^2}$ associated to β. Then G is generated by the matrices

$$\left(\begin{array}{c|c} I_n & \mu e_{ii} \\ \hline & I_n \end{array}\right), \left(\begin{array}{c|c} I_n & \\ \hline \mu e_{ii} & I_n \end{array}\right),$$

$$\left(\begin{array}{c|c} I_n & \lambda e_{ij} + \lambda^\tau e_{ji} \\ \hline & I_n \end{array}\right), \left(\begin{array}{c|c} I_n & \\ \hline \lambda e_{ij} + \lambda^\tau e_{ji} & I_n \end{array}\right),$$

where $\mu, \lambda \in \mathbb{F}_{q^2}$, and $\mu + \mu^\tau = 0$.

Proof. Write G_0 for the subgroup of G which is generated by the matrices in the statement of the result, along with those of the form

$$\left(\begin{array}{c|c} I_n + \lambda e_{ij} & \\ \hline & I_n + \lambda^\tau e_{ji} \end{array}\right).$$

We first show that $G = G_0$. Let $\mathcal{B} = \{e_1, e_2, \ldots, e_n, f_1, f_2, \ldots, f_n\}$ be the unitary basis for V. From 10.10 of [62], G is generated by *unitary transvections.* These unitary transvections correspond to the isotropic vectors in V. Given an isotropic vector $u \in V$, the unitary transvection t_u is the linear transformation given by

$$t_u(v) = v + a\beta(v, u)u$$

for all $v \in V$, where $a \in \mathbb{F}_{q^2}$ satisfies $a + a^\tau = 0$. If we can show that G_0 contains all unitary transvections, the result will follow. In turn, this will follow if we can show G_0 acts transitively on the isotropic vectors in V.

Certainly G_0 contains the transvection which corresponds to the isotropic vector e_1. Let

$$v = a_1 e_1 + \cdots + a_n e_n + b_1 f_n + \cdots + b_n f_n$$

be isotropic, where $a_i, b_i \in \mathbb{F}_{q^2}$ are not all zero. We need to find a matrix in G_0 which sends e_1 to v. Certainly a matrix with first column equal to

$$(a_1, \ldots, a_n, b_1, \ldots, b_n)$$

will suffice. Firstly, note that G_0 contains elements

$$\left(\begin{array}{c|c} A & \\ \hline & A^* \end{array}\right),$$

where A runs over all elements of $SL_n(q^2)$, and A^* depends on our choice of A. Suppose all the $a_i = 0$ in our expression for v. Then pick A with first column equal to

$$(b_1, \ldots, b_n),$$

and note that

$$\left(\begin{array}{c|c} 0 & A^* \\ \hline A & 0 \end{array}\right) = \left(\begin{array}{c|c} 0 & I_n \\ \hline I_n & 0 \end{array}\right) \left(\begin{array}{c|c} A & 0 \\ \hline 0 & A^* \end{array}\right).$$

Since

$$\left(\begin{array}{c|c} 0 & I_n \\ \hline I_n & 0 \end{array}\right) = \left(\begin{array}{c|c} I_n & I_n \\ \hline 0 & I_n \end{array}\right) \left(\begin{array}{c|c} I_n & 0 \\ \hline I_n & I_n \end{array}\right) \left(\begin{array}{c|c} I_n & I_n \\ \hline 0 & I_n \end{array}\right)$$

it now follows that

$$\left(\begin{array}{c|c} 0 & A^* \\ \hline A & 0 \end{array}\right) \in G_0.$$

Now suppose we have $a_i \neq 0$ for some i. Let A be chosen with first column equal to

$$(a_1, \ldots, a_n).$$

Let B be the $n \times n$ matrix with i-th row and column as follows:

$$\begin{pmatrix} & & b_1 a_i^{-1} & & \\ & & \vdots & & \\ (b_1 a_i^{-1})^\tau & \cdots & x & \cdots & (b_n a_i^{-1})^\tau \\ & & \vdots & & \\ & & b_n a_i^{-1} & & \end{pmatrix},$$

where x is given by

$$(b_1 a_i^{-1})^\tau a_1 + \cdots + x a_i + \cdots + (b_n a_i^{-1})^\tau a_n = b_i.$$

We require that $x + x^\tau = 0$, to yield

$$\left(\begin{array}{c|c} I_n & 0 \\ \hline B & I_n \end{array}\right) \in G_0.$$

But a straightforward check shows that

$$x = a_i^{-1}(a_i^{-1})^\tau \left[a_i b_i^\tau + a_1^\tau b_1 + \cdots + a_{i-1}^\tau b_{i-1} + a_{i+1}^\tau b_{i+1} + \cdots + a_n^\tau b_n\right],$$

and since v is isotropic, we have

$$a_1b_1^\tau + \cdots a_nb_n^\tau + a_1^\tau b_1 + \cdots + a_n^\tau b_n = 0,$$

from whence a rearrangement of terms demonstrates $x + x^\tau = 0$ as desired. Now the first column of

$$\left(\begin{array}{c|c} I_n & 0 \\ \hline B & I_n \end{array}\right)\left(\begin{array}{c|c} A & \\ \hline & A^* \end{array}\right) \in G_0$$

is equal to

$$(a_1, \ldots, a_n, b_1, \ldots, b_n).$$

This proves that $G_0 = G$. To complete the proof, we note that a matrix calculation shows that

$$\left(\begin{array}{c|c} I_n + \lambda e_{ij} & \\ \hline & I_n + \lambda^\tau e_{ji} \end{array}\right) = \left(\begin{array}{c|c} I_n & \\ \hline \lambda e_{ij} + \lambda^\tau e_{ji} & I_n \end{array}\right)^{gh},$$

where

$$g = \left(\begin{array}{c|c} I_n & e_{ii} \\ \hline & I_n \end{array}\right)$$

and

$$h = \left(\begin{array}{c|c} I_n & \\ \hline e_{ii} & I_n \end{array}\right),$$

so matrices of this form are not required for our generating set. □

Chapter 7

Groups of Lie-Type over Fields of Odd Characteristic

We are now ready to tackle the local fusion graphs of finite groups of Lie-type when the defining characteristic is odd. Here is the main result we shall prove in this chapter.

Theorem 7.1. *Let G be a finite, simple group of Lie-type defined over a field of odd characteristic. If X is a G-conjugacy class of involution, then $\mathcal{F}(G, X)$ is connected.*

7.1 Strategy

To begin, we state a result which will be a major tool in dealing with the odd characteristic case.

Theorem 7.2 (Rowley)**.** *Suppose G is a group with a split BN-pair and G-conjugacy class of involutions X, and suppose $B = UT$ where U is the unipotent radical of B and T is a maximal split torus. If $X \cap T \neq \emptyset$, then the definining characteristic p must be odd, and $\mathcal{F}_{\{p\}}(G, X)$ is connected. Consequently $\mathcal{F}(G, X)$ is connected.*

In view of this result, our motivation for treating the odd and even characteristic cases separately becomes clear. For suppose G is a finite group of Lie-type defined over a field of even characteristic. Then the involutions of G are not semisimple elements.

However, the torus T consists only of semisimple elements, so the requirement that $X \cap T \neq \emptyset$ is never satisfied. Thus the theorem is of no use to us in even characteristic.

In odd characteristic, the immediate question is: when does $X \cap T \neq \emptyset$? By Theorem 6.4, the maximal split tori of a finite group of Lie-type are G-conjugate. Moreover, for a classical subgroup of $GL(V)$, the subgroup of diagonal matrices forms a maximal split torus T. Thus for finite classical groups the question reduces to determining when an involution can be diagonalised (within G) with respect to a certain basis. This also enables us to infer information about the corresponding projective groups, by observing that if T is maximal split torus of a classical group, then $\overline{T}$ (the image of T upon factoring out the centre of the matrix group) will be a maximal split torus of the projective group.

First, however, let us prove Theorem 7.2.

Proof of Theorem 7.2. By [24], for example, we may consider the Borel subgroup *opposite* to B, which can be written $B^- = HU^-$. Since $X \cap H \neq \emptyset$, the defining characteristic p must be odd, and hence U and U^- are p-groups of odd order. Without loss of generality, as $X \cap H \neq \emptyset$, we may suppose $t \in H$. Thus t normalises both U and U^-, so $\langle U, U^- \rangle \leq M$ by Lemma 1.22(iii). But $\langle U, U^- \rangle = G$ (see, for example, [24] once again), so $M = G$ and hence $\mathcal{F}_{\{p\}}(G, X)$ and $\mathcal{F}(G, X)$ are connected. $\square$

We now move on to study the various families of groups of Lie-type in detail.

7.2 Linear Groups

For this section we suppose $H = SL_n(q)$, where q is odd, and let H act on V in the natural way. We may take for a Borel subgroup B the group of upper unitriangular matrices. Then U is the group of upper uni-triangular matrices, while T is the diagonal subgroup. If $t \in H$ is an involution, then its only eigenvalues must be ± 1. Since q is odd, $-1 \in \mathbb{F}_q$, and so all eigenvalues of t are contained in $\mathbb{F}_q$. Therefore t can be diagonalised in H, and so $X \cap T \neq \emptyset$ holds for all H-conjugacy classes X of involutions. This argument also holds for the involution classes of $GL_n(q)$. Thus we may immediately apply Theorem 7.2 to deduce the following:

Proposition 7.3. *If $H = SL_n(q)$ or $GL_n(q)$, where q is odd, and X is an H-conjugacy class of involutions, then $\mathcal{F}(H, X)$ is connected.*

Since Theorem 7.1 concerns simple groups, we must consider the projective groups $PSL_n(q)$. We first consider the case were n is odd.

Proposition 7.4. *If $G = PSL_{2m+1}(q)$, where q is odd, and X is a G-conjugacy class of involutions, then $\mathcal{F}(G, X)$ is connected.*

Proof. Since the centre of $SL_{2m+1}(q)$ has odd order, the local fusion graphs of G are in one-to-one correspondence with those of $SL_{2m+1}(q)$, and the result follows immediately from Proposition 7.3. $\square$

We now deal with the groups $PSL_n(q)$ where n is even.

Proposition 7.5. *If $G \cong PSL_{2m}(q)$, and X is a G-conjugacy class of involutions. Then $\mathcal{F}(G, X)$ is connected, unless $m = 1$ and $q = 3$, in which case $\mathcal{F}(G, X)$ is totally disconnected.*

Proof. When $m = 1$ and $q = 3$ we have $PSL_2(3) \cong \mathrm{Alt}(4)$, which has a totally disconnected local fusion graph. When $m = 1$ and $q \geq 5$, then the result follows from Lemma 3.1. So let us proceed under the assumption that $m \geq 2$. We use the notation from the proof of Proposition 7.4. If t has any eigenvalues, then we may argue as in the proof of Proposition 7.4 to see that t may be diagonalised in H. Therefore we may assume that

$$t = \begin{pmatrix} 0 & \alpha_1 & & & & & \\ \alpha_2 & 0 & & & & & \\ & & 0 & \alpha_3 & & & \\ & & \alpha_4 & 0 & & & \\ & & & & \ddots & & \\ & & & & & 0 & \alpha_{2m-1} \\ & & & & & \alpha_{2m} & 0 \end{pmatrix},$$

where for each $1 \leq i \leq k$ we have $\alpha_{2i-1}\alpha_{2i} = \omega \neq 1$. Denote by L the inverse image of $\mathrm{Stab}_G(Y)$. Our aim is to show that $a \in L$ for all $a \in \mathcal{A}'$, where $\mathcal{A}'$ is the generating set for H given in Proposition 6.16.

Notice that for any $a = I + \lambda e_{ij} \in \mathcal{A}'$, the entry (i, j) does not coincide with the position of any of the α_i in t. We can easily check that $t^a = t + s$, where s is an upper triangular nilpotent matrix with nonzero entries which do not coincide with the positions of any α_i in t. As a consequence, $t^a t = \omega I_{2m} r$, where r is unipotent, and hence has odd order. Thus $\overline{t^a t}$ has odd order, from which we deduce that $a \in L$. Since the image of $\mathcal{A}'$ generates G, the result follows. □

We conclude this section with a result regarding 2-dimensional linear groups, which will be used in subsequent sections of this chapter. The following well-known result is required for its proof.

Theorem 7.6. *Let $G = PSL_2(q)$ where $q \geq 11$ is odd. If M is a maximal subgroup of G, then M is isomorphic to one of the following groups:*

(i) the dihedral group $\mathrm{Dih}(q + 1)$*, which is the centraliser of an involution of G;*

(ii) the dihedral group $\mathrm{Dih}(q - 1)$*;*

(iii) a group of order $q(q - 1)$;

(iv) $\mathrm{Alt}(4)$*,* $\mathrm{Sym}(4)$ *or* $\mathrm{Alt}(5)$*;*

(v) $PSL_2(r)$ or $PGL_2(r)$, where $r^m = q$.

Proof. See Theorem 6.25 of [61]. □

Now we make a definition. Let H be a finite group, and suppose X is an H-conjugacy class of elements which square to $z \in Z(H)$, where $z \neq 1$. We define the graph $\mathcal{D}(H, X)$ to have X as its vertex set, with $x, y \in X$ adjacent in $\mathcal{D}(H, X)$ if, and only if, $x \neq y$ and $xy = zw$, where w is some element of odd order.

Lemma 7.7. *Suppose $H = GL_2(q)$ where $q \neq 3$, and that X is an H-conjugacy class of elements which square to λI_2.*

(i) If $\lambda = -1$, then $\mathcal{D}(H,X)$ is connected.

(ii) If $q \equiv 3 \bmod 4$, then $\mathcal{D}(H,X)$ is connected.

Proof. When $q \leq 11$ we may verify the result using MAGMA, so assume $q > 11$. Let $t \in H$ be such that $t^2 = \lambda I_2$, and without loss of generality take

$$t = \begin{pmatrix} 0 & 1 \\ \lambda & 0 \end{pmatrix}.$$

We write $Z = Z(H)$, $C = C_H(t)$, $N = N_H(\langle t \rangle)$, and L for the subgroup of H which is naturally isomorphic to $SL_2(q)$. Notice that

$$C = \left\{ \begin{pmatrix} a & b \\ \lambda b & a \end{pmatrix} : a, b \in \mathbb{F}_q \right\}.$$

Our first claim is that N is a maximal subgroup of H. Indeed, it is certainly the case that $\overline{N} \cap \overline{L} = C_{\overline{L}}(\bar{t})$, which is a maximal subgroup of $\overline{L}$ isomorphic to $\mathrm{Dih}(q+1)$, by Theorem 7.6. Since $[\overline{H} : \overline{L}] = 2$, any maximal subgroup of $\overline{H}$ must be one of the subgroups listed in Theorem 7.6, an extension of one of these subgroups by a group of order 2, or $\overline{L}$ itself. Using the description of C given above, we see there exist elements of C (and so N) which lie outside $N_L(\langle t \rangle)Z$, and so $C_{\overline{L}}(\bar{t})$ is a proper subgroup of $C_{\overline{H}}(\bar{t})$. Therefore we must have $\overline{N} = C_{\overline{L}}(\bar{t}).2$ and $\overline{N}$ is a maximal subgroup of $\overline{H}$. Since $Z \leq N$, this implies that N is a maximal subgroup of H.

Next, we show that N is the unique maximal subgroup of H which contains C. Since $t^2 \in Z$, we have $[N : C] = 2$, and consequently $|\overline{C}| = q+1$. Suppose M is such that $C < M < H$. Then $\overline{M}$ is a maximal subgroup of $\overline{H}$ with order divisible by $q+1$. We have already noted the impossibility of $M \cong SL_2(q)$, and now an examination of the orders of the groups in Theorem 7.6 shows that the only possibility is $\overline{M} = \overline{N}$, whence $M = N$.

Now suppose that $\lambda = -1$, and notice that in this case $t \in SL_2(q)$, so $X \subseteq SL_2(q)$. If there exists $h \in H$ such that t and t^h are adjacent in $\mathcal{D}(H,X)$, then $h \in \mathrm{Stab}_H(Y)$, where Y is the connected component of $\mathcal{D}(H,X)$ which contains t. Moreover, since $h \notin N$, $\langle C, h \rangle = H$. Hence it suffices to show the existence of such an h. For contradiction, suppose $\mathcal{D}(H,X)$ is totally disconnected. If for all $x, y \in X$ it is the case that $\langle x, y\rangle$ is a 2-group, then Theorem 1.4 implies that $X \subseteq O_2(H)$, a contradiction. So there must exist $x \in X$ such that tx has order $2^k m$, where $m > 1$ has odd order. If $k = 1$, then $(tx)^m$ has order 2, which is sufficient since the only involution in $SL_2(q)$ is $-I_2$. If $k = 0$, then $t(-x)$ has order $2m$, and since x and $-x$ are conjugate in $SL_2(q)$ we see that $-x$ is adjacent to t in $\mathcal{D}(H,X)$. Finally, suppose that $k \geq 2$. Then $(tx)^{2^{k-1}m}$ has order 2. However,

$$(tx)^{2^{k-1}m} = txtx\cdots tx = (-t)(-x)(-t)\cdots(-x)txt\cdots tx = (-t)t^{xt\cdots x}$$

since $-t = t^{-1}$, and similarly for x. Thus we again have an edge in $\mathcal{D}(H,X)$, as required, completing the proof of (i).

To prove (ii), suppose that $q \equiv 3 \bmod 4$, and let $\omega \in \mathbb{F}_q$ be an element of maximal (multiplicative) odd order. Since $q \equiv 3 \bmod 4$, this order must be greater than 1. Now define

$$y = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}.$$

Then we may easily check that t^y is adjacent to t in $\mathcal{D}(H,X)$, and so $y \in \mathrm{Stab}_H(Y)$, where Y is the connected component of $\mathcal{D}(H,X)$ which contains t. But clearly we also have $C \leq \mathrm{Stab}_H(Y)$. Furthermore, $y \notin N$, and since N is the unique maximal subgroup of H which contains C, it must be that $\langle C, y\rangle = H$. Thus $H = \mathrm{Stab}_H(Y)$, and the proof is complete. □

7.3 Symplectic Groups

Let $H = Sp_{2m}(q)$ act on V. Recall that H preserves a non-degenerate, alternating bilinear form β on V, as defined in Theorem 6.5.

Lemma 7.8. *Let $H = Sp_{2m}(q)$, where q is odd, and let X be a H-conjugacy class of involutions. If T is a maximal split torus of H, then $X \cap T \neq \emptyset$.*

Proof. In view of Theorem 6.4 it suffices to prove that an involution x of any H-conjugacy class X lies in a Borel subgroup B. Theorem 6.8 tells us that the Borel subgroups of G are precisely the stabilisers of maximal isotropic flags of V. Thus we must show that x stabilises such a flag. Let $v \in V$ be an arbitrary vector. Then we may write

$$v = \frac{1}{2}(v + v^x) + \frac{1}{2}(v - v^x),$$

which implies that $V = V_{+1} \oplus V_{-1}$, where x acts trivially on V_{+1} and as -1 on V_{-1}. Suppose that $u \in V_{+1}$ and $v \in V_{-1}$ are nonzero vectors. Then

$$\beta(u, v) = \beta(u^x, v^x) = \beta(u, -v) = -\beta(u, v).$$

Thus $\beta(u, v) = 0$ and we have $V = V_{+1} \perp V_{-1}$. Note that this implies both V_{+1} and V_{-1} are non-degenerate. Also, as $\det(x) = 1$ and x acts as -1 on V_{-1}, we must have that the dimension of V_{-1} is even, say $\dim V_{-1} = 2k$.

By considering maximal totally isotropic subspaces of V_{+1} and V_{-1}, and using Lemma 6.7, we may write

$$V_{+1} = L_1 \perp L_2 \perp \cdots \perp L_k$$

and

$$V_{-1} = L_{k+1} \perp L_{k+2} \perp \cdots \perp L_m,$$

where the L_i are hyperbolic lines. For $i = 1, \ldots, m$ let e_i be an isotropic vector in L_i. Then the following is an isotropic flag in V:

$$\mathcal{F} = \langle e_1 \rangle \subset \langle e_1, e_2 \rangle \subset \cdots \subset \langle e_1, e_2, \ldots, e_m \rangle.$$

Moreover, since $\mathcal{F}$ has type $\{1, \ldots, m\}$ this is a maximal isotropic flag. Since x acts trivially on V_{+1} and as -1 on V_{-1}, x stabilises $\mathcal{F}$, as required. □

Corollary 7.9. *If $H = Sp_{2n}(q)$, where q is odd, and X is an H-conjugacy class of involutions, then $\mathcal{F}(H, X)$ is connected.*

Proof. Apply Lemma 7.8 along with Theorem 7.2. □

We now consider the local fusion graphs of the (usually) simple groups $PSp_{2m}(q)$. In view of Corollary 7.9, when proving Theorem 7.12 we need only be concerned with involution classes of $PSp_{2m}(q)$ which arise from elements of $Sp_{2m}(q)$ which square to -1. Fortunately, there is only ever one such class.

Lemma 7.10. *Let $H = Sp_{2m}(q)$, where q is odd. Then there is a unique H-conjugacy class of elements which square to $-1 \in Z(H)$.*

Proof. This is contained in the proof of Lemma 11.52 in [62]. $\square$

Lemma 7.11. *Suppose $H = Sp_{2m}(q)$, where q is odd, and that $x \in H$ is an element which squares to -1. Then $x \in L$, where $L \leq H$ and $L \cong Sp_2(q^m)$.*

Proof. Without loss of generality suppose that V has symplectic basis

$$\{e_1, \ldots, e_m, f_1, \ldots, f_m\}$$

so that the sympletic form β on V has Gram matrix

$$J = \left(\begin{array}{c|c} & I_n \\ \hline -I_n & \end{array}\right),$$

and suppose that

$$x = \left(\begin{array}{c|c} & A_m \\ \hline -A_m & \end{array}\right)$$

where A_m is the $m \times m$ matrix with 1 in positions $(1, m), (2, m-1), \ldots, (m, 1)$ and zeroes elsewhere. Notice that there exists an $\mathbb{F}_q$-vector space isomorphism ϕ between V and V', where V' is a 2-dimensional $\mathbb{F}_{q^m}$-vector space. For example, if V' has basis $\{e'_1, \ldots, e'_m, f'_1, \ldots, f'_m\}$ as an $\mathbb{F}_q$-vector space, we can set $e_i\phi = e'_i$ and $f_i\phi = f'_i$ for $1 \leq i \leq m$, and extend $\mathbb{F}_q$-linearly. We can also endow V' with a symplectic form β', where β' has Gram matrix

$$J' = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Clearly H acts on V' via the isomorphism ϕ, and one can show (see page 111 of [50], for example) that the subgroup of H consisting of elements which preserve β' is in fact isomorphic to $Sp_2(q^m)$. Moreover, it is straightforward to check by explicit calculation that x also preserves β', so lies in this subgroup. $\square$

Proposition 7.12. *Let $G = PSp_{2m}(q)$, where q is odd, and let X be a G-conjugacy class of involutions. Then $\mathcal{F}(G, X)$ is connected, unless $m = 1$ and $q = 3$, where $\mathcal{F}(G, X)$ is totally disconnected.*

Proof. We prove the result by induction on m. First note that if $q \geq 5$ then $PSp_2(q) \cong PSL_2(q)$, and the result holds by Theorem 3.1. If $q = 3$, then $PSp_2(q) \cong \mathrm{Alt}(4)$, which has a totally disconnected local fusion graph. However, we may easily check using MAGMA that $PSp_4(3)$ and $PSp_6(3)$ have connected local fusion graphs.

Let $G = \overline{H}$, and suppose V has basis $\{e_1, \ldots, e_m, f_1, \ldots, f_m\}$ so that the sympletic form β on V has Gram matrix

$$J = \left(\begin{array}{c|c} & I_n \\ \hline -I_n & \end{array}\right).$$

Set

$$t = \left(\begin{array}{c|c} & A_m \\ \hline -A_m & \end{array}\right)$$

where A_m is the $m \times m$ matrix with 1 in positions $(1, m), (2, m-1), \ldots, (m, 1)$ and zeroes elsewhere. Then $t \in H$, and $t^2 = -1 \in Z(H)$, so using Lemma 7.10 we may take $\bar{t}$ as our representative for the relevant involution class of G. We may write $t = t_1 t_2$, where

$$t_1 = \left(\begin{array}{c|cc|c} I_{m-k} & & & \\ \hline & & A_k & \\ & -A_k & & \\ \hline & & & I_{m-k} \end{array}\right)$$

and

$$t_2 = \left(\begin{array}{c|cc|c} & & & A_{m-k} \\ \hline & I_k & & \\ & & I_k & \\ \hline -A_{m-k} & & & \end{array}\right),$$

where $1 \leq k \leq m-1$. It is clear that t_1 and t_2 commute. Notice that t stabilises a non-degenerate subspace of V of dimension $2k$, namely

$$W = \langle e_{2m-k+1}, \ldots, e_{2m}, f_{2m}, \ldots, f_{2m-k+1} \rangle,$$

and so by Theorem 6.10 lies in a subgroup $M \leq H$, where

$$M = M_1 \times M_2 \cong Sp_{2k}(q) \times Sp_{2m-2k}(q).$$

Furthermore, if $k \neq m$, then M is a maximal subgroup of H and $\overline{M}$ is a maximal subgroup of G. Our aim is to show that $\overline{M} \leq \mathrm{Stab}_G(Y)$, where Y is the connected component of $\mathcal{F}(G,X)$ which contains $\bar{t}$.

Denote by X_i the $\overline{M_i}$-conjugacy class of involutions which contains $\overline{t_i}$, for $i = 1, 2$. If $q \geq 5$, then by induction $\mathcal{F}(\overline{M_1}, X_1)$ and $\mathcal{F}(\overline{M_2}, X_2)$ are connected. If $q = 3$ then since we have checked cases when $m = 2$ and $m = 3$, we may assume that $m \geq 4$. We can now choose $k \notin \{2, 2m-2\}$ so that neither $\overline{M_1}$ nor $\overline{M_2}$ is isomorphic to $PSp_2(3)$. This allows us to use induction in this case also.

Let $\overline{x} \in X'$ have preimage $x \in M$, where X' denotes the $\overline{M}$-conjugacy class of $\bar{t}$, and write $x = x_1 x_2$, where $x_1 \in M_1$ and $x_2 \in M_2$. By induction there exists a path

$$t_1 = x_1^{(0)} \to x_1^{(1)} \to x_1^{(2)} \to \cdots \to x_1^{(m)} = x_1$$

of elements in $x_1^{M_1}$ such that $x_1^{(i)} x_1^{(i+1)} = y_1^{(i)} z_1^{(i)}$, where $y_1^{(i)}$ has odd order and $z_1^{(i)} \in Z(M_1)$, for $0 \leq i \leq m-1$. This path induces in a natural way a path in $\mathcal{F}(G,X)$ from $t_1 t_2$ to either $x_1 t_2$ or $x_1(-1_{M_2} t_2)$. For suppose first that $z_1^{(i)} = -1_{M_1} \in Z(M_1)$ for some i. Then

$$(x_1^{(i)} t_2)(x_1^{(i+1)} t_2) = (x_1^{(i)} x_1^{(i+1)}) t_2^2 = y_1^{(i)} (-1_{M_1})(-1_{M_2}).$$

Since $(-1_{M_1})(-1_{M_2}) = -1 \in Z(H)$, we have that $\overline{x_1^{(i)} t_2}$ and $\overline{x_1^{(i+1)} t_2}$ are adjacent in $\mathcal{F}(G,X)$. Now suppose that $z_1^{(j)} = 1$ for some j. Then

$$(x_1^{(j)} t_2)(x^{(j+1)} t_2(-1_{M_2})) = x_1^{(j)} x_1^{(j+1)} t_2^2 (-1_{M_2}) = y_1^{(j)}$$

has odd order. Moreoever, $(-1_{M_2} t_2)^2 = -1_{M_2}$, so by Lemma 7.10 we deduce that t_2 and $-1_{M_2} t_2$ are M_2-conjugate. Hence we have a path from $t_1 t_2$ to either $x_1 t_2$ or $x_1(-1_{M_2} t_2)$ in $\mathcal{F}(G,X)$. A similar argument now allows us to find a path in $\mathcal{F}(G,X)$ from this element to one of $x_1 x_2$, $-(x_1 x_2)$, $(-1_{M_1} x_1) x_2$ or $x_1(-1_{M_2} x_2)$. In the former two cases we are done, since both $x_1 x_2$ and $-(x_1 x_2)$ have image $\overline{x}$ in G. So without loss of generality suppose we are in one of the latter two cases, say with a path from $t_1 t_2$ to $(-1_{M_1} x_1) x_2$. Then the isomorphism $Sp_2(q) \cong SL_2(q)$ allows us to use Lemma 7.7(i) to see that there exists a path in the graph $\mathcal{D}(M_1, x_1^{M_1})$ from x_1 to $-1_{M_1} x_1$, which in turn induces a path from $(-1_{M_1} x_1) x_2$ to $x_1 x_2$ in $\mathcal{F}(G,X)$.

As this method allows us to construct a path between $\bar{t}$ and an arbitrary $\overline{x}$ in $\mathcal{F}(\overline{M}, X')$, we deduce that $\overline{M} \leq \mathrm{Stab}_G(Y)$.

Denote by M^* the stabiliser of the decomposition $V = W \oplus W^{\perp}$. If $k \neq m$, then $M = M^*$, while if $k = m$ then M is a subgroup of index 2 in M^*. In the former case, by Theorem 6.10, $\overline{M^*}$ is a maximal subgroup of G, while in the latter case reference to Table 3.5C of [50] tells us that $\overline{M^*}$ is again a maximal subgroup of G, and is the unique maximal subgroup of G which contains $\overline{M}$. However, by Lemma 7.11 we have that $\bar{t} \in \overline{L}$, where $\overline{L} \cong PSp_2(q^m)$. As $PSp_2(q^m) \cong PSL_2(q^m)$, and $m \geq 2$, Theorem 3.1 tells us that $\overline{L} \leq \mathrm{Stab}_G(Y)$. Since $\overline{L} \not\leq \overline{M^*}$ (by comparing group orders from the formulae given in [50], for example), it must be that $\langle \overline{M}, \overline{L} \rangle = G$, and so $\mathcal{F}(G, X)$ is connected. □

7.4 Unitary Groups

The unitary groups are next on our agenda. Let $H = GU_n(q) \cong GU(V)$, where q is odd. Recall that this means the entries of matrices in H are taken from $\mathbb{F}_{q^2}$. To help determine H-conjugacy there is the following result:

Theorem 7.13. *Elements of $GU_n(q)$ are conjugate in $GU_n(q)$ if, and only if, they are conjugate in $GL_n(q^2)$.*

Proof. This is proved by G. E. Wall in [64]. □

Theorem 7.14. *If $H = SU_n(q)$ or $GU_n(q)$, and X is an H-conjugacy class of involutions, then $\mathcal{F}(G, X)$ is connected.*

Proof. By Proposition 2.3.1 of [50] we may suppose that the unitary form β on V has Gram matrix $J = I_n$. Theorem 7.13 implies that H has at most the number of involution classes as $GL_n(q^2)$. But we make take diagonal representatives for each involution class of $GL_n(q^2)$, with nonzero entries 1 and -1, both of which are fixed by the involutary automorphism τ of $\mathbb{F}_{q^2}$ associated to β. Hence these representatives lie in H, and the result follows using Theorem 7.2. □

When dealing with the projective unitary groups, we must consider elements of $GU_n(q)$ which square to non-trivial central elements. We first consider how the vector space V can decompose under the action of such an element. So for $H = GU_n(q)$, let $t \in H$ be such that $t^2 \in Z(H)$, say $t^2 = \lambda I_n$. For $v \in V$ the subspace $\langle v, v^t \rangle$ must be either 1 or 2-dimensional. Thus, first taking v to be a non-isotropic vector, then taking a non-isotropic vector in $\langle v, v^t \rangle^\perp$, and so on, we see that t must stabilise a decomposition

$$V = W_1 \perp \ldots \perp W_k \perp U_{k+1} \perp U_{2m+1},$$

where the W_i are non-degenerate 2-spaces and the U_i are non-degenerate 1-spaces. For each 2-space we may choose a basis so that the restriction of β to W_i has Gram matrix $J_i = I_2$, and then by taking a suitable basis vector for each U_i we may ensure that β has Gram matrix $J = I_n$. With respect to this basis for V we have

$$t = \left(\begin{array}{c|c|c|c} t_1 & & & \\ \hline & \ddots & & \\ \hline & & t_k & \\ \hline & & & \mu I_{n-2k} \end{array} \right),$$

where $t_i \in GU_2(q)$ and $t_i^2 = \lambda I_2$ for each i, and $\mu^2 = \lambda$.

Proposition 7.15. *Let $H = GU_n(q)$ where q is odd, and suppose that $t \in H$ is such that $t^2 \in Z(H)$. If t has a non-zero eigenvalue, then t lies in a maximal split torus of H.*

Proof. Suppose $t^2 = \lambda I_n$, and choose the basis for V and representative for t in the form described above. By assumption t has at least one non-zero eigenvalue μ, and since t must preserve the unitary form β we deduce that $\mu\mu^\tau = 1$. Since $t^2 = \lambda I_n$, t has characteristic polynomial

$$(\chi - \mu)^{n-2k}(\chi^2 - \lambda)^k,$$

and since $\mu^2 = \lambda$ this splits into linear factors

$$(\chi - \mu)^{n-k}(\chi + \mu)^k.$$

Hence t is conjugate in $GL_n(q^2)$ to a diagonal element. But since $\mu\mu^\tau = 1$, such a diagonal element will also preserve β, so will lie in H, and by Theorem 7.13 will be H-conjugate to t. Thus without loss of generality we may choose t to be diagonal, and so t lies in a maximal split torus of H. $\square$

Lemma 7.16. *If $G = PSU_{2m+1}(q)$ and X is a G-conjugacy class of involutions, then $\mathcal{F}(G, X)$ is connected.*

Proof. Since the centre of $SU_{2m+1}(q)$ has odd order, this follows immediately from Theorem 7.14. $\square$

We deal with the groups $PSU_{2m}(q)$ in two stages. First, we consider the cases where $q \equiv 1$ mod 4.

Theorem 7.17. *Let $G = PSU_{2m}(q)$, where $m \geq 2$ and $q \equiv 1$ mod 4. If X is a G-conjugacy class of involutions, then $\mathcal{F}(G, X)$ is connected.*

Proof. Let V have Gram matrix

$$J = \left(\begin{array}{c|c} & I_m \\ \hline I_m & \end{array}\right).$$

By consulting Table 4.5.1 of [39], we see that G has $\lfloor m/2 + 1 \rfloor$ conjugacy classes of involutions. For elements of H which map canonically into $\lfloor m/2 \rfloor$ of these classes, we may simply take diagonal elements t_i, for $1 \leq i \leq \lfloor m/2 \rfloor$, with eigenvalues ± 1. The final G-conjugacy class of involutions comes from elements which square to a non-trivial central element in H. Since $q \equiv 1$ mod 4, there exists $\omega \in \mathbb{F}_{q^2}$ which squares to -1. Define

$$t = \begin{pmatrix} \omega & & & & & \\ & \ddots & & & & \\ & & \omega & & & \\ & & & \omega^{-1} & & \\ & & & & \ddots & \\ & & & & & \omega^{-1} \end{pmatrix}.$$

Notice that $\det(t_2) = 1$. Furthermore, t will preserve the unitary form β if $\omega^{q-1} = 1$. But 4 divides $q-1$, so this is certainly the case. Hence $t \in H$. Moreover, since ωI_{2m} does not preserve β (as $\omega^{q+1} \neq 1$), so does not lie in H, we see that $\bar{t}$ must lie in a different G-conjugacy class of involutions to $\overline{t_i}$ for $1 \leq i \leq \lfloor m/2 \rfloor$. Nevertheless, $\bar{t}$ lies in a maximal split torus of G, so once again the result follows by Theorem 7.2.

□

To proceed with the case where $q \equiv 3 \bmod 4$, we require a corollary to Lemma 7.7.

Corollary 7.18. *If $H = GU_2(q)$ where $q \equiv 3$ mod 4 but $q \neq 3$, and X is an H-conjugacy class of elements which square to λI_2, then $\mathcal{D}(H, X)$ is connected.*

Proof. Here we make use of the isomorphisms $PGU_2(q) \cong PGL_2(q)$ and $SU_2(q) \cong SL_2(q)$. As a result, the proof is almost identical to that of Lemma 7.7. □

Lemma 7.19. *If $H = SU_4(3)$, and X is a conjugacy class of elements which square to -1, then $\mathcal{D}(H, X)$ is connected.*

Proof. This can be easily verified using Magma. □

We shall see in a moment that our general method for dealing with the groups $PSU_{2m}(q)$ when $q \equiv 3 \bmod 4$ does not cover the case when $q = 3$. This is due to the fact that $PSU_2(3) \cong PSL_2(3)$, which has a disconnected local fusion graph. Therefore we deal with this case separately.

Lemma 7.20. *If $G = PSU_{2m}(3)$, where $m \geq 2$ and X is a G-conjugacy class of involutions, then $\mathcal{F}(G, X)$ is connected.*

Proof. We can check using Magma the cases $PSU_4(3)$, $PSU_6(3)$ and $PSU_8(3)$, so assume that $m \geq 5$. Note that $|Z(H)| = 2$ or 4, depending on whether m is odd or even, respectively.

If $|Z(H)| = 2$, then any G-conjugacy class of involutions must either be the image of an H-conjugacy class of involutions, or the image of an H-conjugacy class of elements which square to -1. In the former case we may apply Theorem 7.2. In the latter case, suppose β is such that $J = I_{2m}$, and let t be the diagonal element given in the proof of Theorem 7.17, and set $X = \bar{t}^G$. Note that such an element ω exists in $\mathbb{F}_9$, and t preserves β since $\omega^{q+1} = \omega^4 = 1$. Thus $t \in H$, and $t^2 = -1$. Moreover, since m is odd, ωI_{2m} has determinant -1, so $\omega I_{2m} \notin H$. Hence $\bar{t}$ does not represent the same G-conjugacy as the image of any involution in H, and we may apply Theorem 7.2 once again to see that $\mathcal{F}(G, X)$ is connected.

Now suppose that $|Z(H)| = 4$, so m is even. Reference to Table 4.5.1 of [39] tells us that G has either $m/2$ or $m/2+1$ conjugacy classes of involutions, and by considering the representatives t and t_i for $1 \leq i \leq m/2$, as given in the proof of Theorem 7.17, we see that at most one G-conjugacy class of involutions is not the image of an H-conjugacy class of involutions. Moreover, we can take as our representative for the possible remaining class the involution $\bar{t}$, where

$$t = \left(\begin{array}{c|c} & A_m \\ \hline -A_m & \end{array}\right)$$

and A_m is the $m \times m$ matrix with 1 in positions $(1, m), (2, m-1), \ldots, (m, 1)$ and zeroes elsewhere. Since $m \geq 5$ and m is even, we see that t stabilises a non-degenerate subspace of V of dimension 6, for example

$$W = \langle e_{2m-5}, \ldots, e_{2m}, f_{2m}, \ldots, f_{2m-5} \rangle,$$

and so lies in a subgroup $M \leq H$, where

$$M = M_1 \times M_2 \cong SU_6(q) \times SU_{2m-6}(q).$$

Since 4 does not divide 6 or $2m-6$, $|Z(M_1)| = |Z(M_2)| = 2$, and so we may argue as above to see that $\overline{M} \leq \mathrm{Stab}_G(Y)$. If $6 \neq m$, then by Theorem 6.11 $M \lhd K$ where K is a maximal subgroup of H and

$$K \leq GU_6(q) \times GU_{2m-6}(q).$$

By Theorem 7.13, no M-conjugacy classes fuse in K, so $\overline{K} \leq \mathrm{Stab}_G(Y)$. But t stabilises a further non-degenerate 6-space of V, say

$$U = \langle e_1, \ldots, e_6, f_6, \ldots, f_1 \rangle,$$

so by the same argument we get $\overline{K'} \leq \mathrm{Stab}_G(Y)$, where K' is another maximal subgroup of H. The result now follows by the maximality of $\overline{K}$ or $\overline{K'}$.

Suppose then that $m = 6$, so $H = SU_{12}(3)$. Here M lies in a unique maximal subgroup K^* of H, the stabiliser of the decomposition

$$V = W \perp W'$$

into two non-degenerate 6-spaces. Notice that t also stabilises the decomposition

$$V = W_1 \perp W_2 \perp W_3,$$

where

$$W_1 = \langle e_1, e_2, f_1, f_2 \rangle,$$

$$W_2 = \langle e_3, e_4, f_3, f_4 \rangle$$

and

$$W_3 = \langle e_5, e_6, f_5, f_6 \rangle.$$

Using Lemma 7.19, we have that $\overline{L} \leq \mathrm{Stab}_G(Y)$, where

$$L \cong SU_4(3) \times SU_4(3) \times SU_4(3).$$

Since L does not lie in K^*, we have that $G = \mathrm{Stab}_G(Y)$ by the maximality of K^*. Hence $\mathcal{F}(G, X)$ is connected. □

We now tackle the cases where $q \neq 3$.

Theorem 7.21. *Let $G = PGU_{2m}(q)$, where $m \geq 2$ and $q \equiv 3 \bmod 4$. If X is a G-conjugacy class of involutions, then $\mathcal{F}(G, X)$ is connected.*

Proof. If $\bar{t} \in X$ has preimage $t \in H$ which is an involution, then we may apply Theorem 7.14, and indeed if t has any non-zero eigenvalues we may argue as in the proof of Proposition 7.15 to show that $\bar{t}$ lies in a maximal split torus of G, and so the result follows by Theorem 7.2. Assume therefore that $t^2 = \lambda I_{2m}$, t has no eigenvectors, and that t preserves a decomposition

$$V = W_1 \perp W_2 \perp \ldots \perp W_m$$

of V into non-degenerate 2-spaces. For each W_i we may choose a basis $\mathcal{B}_i$ so that the restriction of β to W_i has Gram matrix $J_i = I_2$, so $J = I_{2m}$. As $t^2 = \lambda I_{2m}$, t is conjugate in $GL_{2m}(q)$ to an element

$$t' = \begin{pmatrix} 0 & 1 & & & & & \\ \lambda & 0 & & & & & \\ & & 0 & 1 & & & \\ & & \lambda & 0 & & & \\ & & & & \ddots & & \\ & & & & & 0 & 1 \\ & & & & & \lambda & 0 \end{pmatrix}.$$

Since $\lambda I_{2m} \in Z(H)$, we must have $\lambda\lambda^\tau = 1$, and using this fact we see that t' also preserves J, so lies in H. Now Theorem 7.13 implies that t and t' are H-conjugate, so without loss of generality let $t = t'$. We now rearrange our basis vectors for V, and write $\mathcal{B}'$ for this new basis. If m is even, we do this so that β has Gram matrix

$$J_{\text{even}} = \left(\begin{array}{c|c} & I_m \\ \hline I_m & \end{array}\right),$$

while if m is odd we rearrange so that

$$J_{\text{odd}} = \left(\begin{array}{c|c|c} & I_{m-1} & \\ \hline I_{m-1} & & \\ \hline & & I_2 \end{array}\right).$$

Write V' for V with respect $\mathcal{B}'$. This change of basis will of course give a new representation $t_{\mathcal{B}'}$, but notice that $t_{\mathcal{B}}$ given above also preserves both J_{even} and J_{odd}, so lies in $SU(V')$. Since $t_{\mathcal{B}'}$ is conjugate in $GL_{2m}(q)$ to $t_{\mathcal{B}}$, Theorem 7.13 tells us that these elements are conjugate in $SU(V')$. Writing $H = SU(V')$, we may therefore take $t = t_{\mathcal{B}} \in H$ as our conjugacy class representative.

Since t preserves the decomposition

$$V = W_1 \perp W_2 \perp \ldots \perp W_m,$$

by Theorem 6.12 t lies in a maximal subgroup $M \leq H$, where

$$M = L \wr K \leq GU_2(q) \wr \mathrm{Sym}(m).$$

Our aim is to show that $\overline{M} \leq \mathrm{Stab}_G(Y)$. First consider an element of M which lies in the subgroup K. Such an element permutes the subspaces $W_1, \dots, W_m$, but within each W_i acts trivially. Thus, these elements lie in $C_H(t)$, and so $\overline{K} \leq \mathrm{Stab}_G(Y)$. Next, consider

$$L = L_1 \times L_2 \times \cdots \times L_m,$$

and write $t = t_1 \cdots t_m$ where $t_i \in L_i$ for each i. Suppose that $h \in L_i$ for some i, and without loss of generality let $h \in L_1$. Then h commutes with $t_2, \dots, t_m$. Moreover, by Lemma 7.18, t_1^h is connected to t_1 in the graph $\mathcal{D}(L_1, t_1^{L_1})$. Using any suitable path in this graph, we may construct a chain of elements

$$t = x^{(0)} \to x^{(1)} \to x^{(2)} \to \cdots \to x^{(l)} = t^h$$

in X such that $x^{(j)}x^{(j+1)} = \lambda y^{(j+1)}$, where $y^{(j+1)}$ is an element of odd order, for $1 \leq j \leq l-1$. Thus $\overline{x^{(j)}}$ and $\overline{x^{(j+1)}}$ are adjacent in $\mathcal{F}(G, X)$ for each j, and so $\bar{t}$ is connected to $\overline{t^h}$ in $\mathcal{F}(G, X)$. Thus $\overline{h} \in \mathrm{Stab}_G(Y)$. As h was chosen arbitrarily, we get that $\overline{L} \leq \mathrm{Stab}_G(Y)$, and consequently $\overline{M} = \langle \overline{L}, \overline{K} \rangle \leq \mathrm{Stab}_G(Y)$.

Since $\overline{M}$ is a maximal subgroup of G, it now suffices to show the existence of an element $\overline{y} \in \mathrm{Stab}_G(Y) \setminus \overline{M}$. If β has Gram matrix J_{even}, then define

$$y = \left(\begin{array}{c|c} I_m & \mu e_{1,1} \\ \hline & I_m \end{array}\right),$$

while if β has Gram matrix J_{odd} let

$$y = \left(\begin{array}{c|c|c} I_{m-1} & \mu e_{1,1} & \\ \hline & I_{m-1} & \\ \hline & & I_2 \end{array}\right),$$

where $\mu \in \mathbb{F}_{q^2}$ is such that $\mu + \mu^\tau = 0$. Then $y \in H$, and since y does not preserve the decomposition of V which t preserves, $y \notin M$. But as in the proof of Theorem 7.5 we may check that

$$tt^y = \lambda I_{2m} r,$$

where r is an upper-triangular unipotent matrix, which consequently must have odd order. Therefore $\overline{y} \in \mathrm{Stab}_G(Y)$, and the proof is complete. □

Corollary 7.22. *If $G = PSU_{2m}(q)$, where $m \geq 2$ and $q \equiv 3$ mod 4, and X is a G-conjugacy class of involutions, then $\mathcal{F}(G, X)$ is connected.*

Proof. When $q = 3$ the result follows by Lemma 7.20, while if $q \neq 3$ we use Theorem 7.21 along with Lemma 1.19. □

7.5 Orthogonal Groups

In this section we investigate the local fusion graphs of orthogonal groups. The first step is to consider the matrix groups. We deal separately with cases of minus-type, plus-type, and odd dimension. As usual we denote the matrix group by H, which acts on a vector space V equipped with a symmetric bilinear form β.

Proposition 7.23. *Let $H = \Omega^{-}_{2m}(q)$ or $SO^{-}_{2m}(q)$, where q is odd and $m \geq 2$, and let $x \in H$ be an involution. Then x lies in a maximal split torus of H.*

Proof. Let $v \in V$ be an arbitrary vector. Then we may write

$$v = \frac{1}{2}(v + v^x) + \frac{1}{2}(v - v^x),$$

which implies that $V = V_{+1} \oplus V_{-1}$, where x acts trivially on V_{+1} and as -1 on V_{-1}. Suppose that $u \in V_{+1}$ and $v \in V_{-1}$. Then

$$\beta(u, v) = \beta(u^x, v^x) = \beta(u, -v) = -\beta(u, v).$$

Thus $\beta(u, v) = 0$ and we have $V = V_{+1} \perp V_{-1}$. Note that this implies both V_{+1} and V_{-1} are non-degenerate. Also, as $\det(x) = 1$ and x acts as -1 on V_{-1}, we must have that the dimension of V_{-1} is even, say $\dim V_{-1} = 2k$.

Since V has minus-type, from [62] we have that V_{+1} and V_{-1} have different types. Suppose first that V_{-1} has minus-type, so V_{+1} has plus-type. Then V_{+1} and V_{-1} contain maximal isotropic subspaces of dimensions $m - k$ and $k - 2$ respectively. By considering these and using Lemma 6.7 we may write

$$V_{+1} = L_1 \perp L_2 \perp \cdots \perp L_k$$

and

$$V_{-1} = L_{k+1} \perp L_{k+2} \perp \cdots \perp L_{m-1} \perp W,$$

where the L_i are hyperbolic lines, and W is a 2-space which contains no singular vectors.

For $i = 1, \ldots, m-1$ let e_i be a singular vector in L_i. Then the following is an isotropic flag in V:

$$\mathcal{F} = \langle e_1 \rangle \subset \langle e_1, e_2 \rangle \subset \cdots \subset \langle e_1, e_2, \ldots, e_{m-1} \rangle.$$

Moreover, since the Witt index of V is $m-1$, this is a maximal isotropic flag. Since x acts trivially on V_{+1} and as -1 on V_{-1}, x stabilises $\mathcal{F}$. Now Theorem 6.8 implies that x lies in Borel subgroup B of H. Thus by Theorem 6.4, x must lie in a maximal split torus of H. □

Corollary 7.24. *Let $H = \Omega^-_{2m}(q)$ or $SO^-_{2m}(q)$, where q is odd, and let $t \in H$ be an involution, with $X = t^H$. Then $\mathcal{F}(H, X)$ is connected.*

Proof. Both $\Omega^-_2(q)$ and $SO^-_2(q)$ are cyclic groups (see Proposition 2.9.1 of [50]), so the result trivially holds here. When $m \geq 2$, then by Proposition 7.23, t lies in a maximal split torus of H. We now apply Theorem 7.2. □

We now come to the orthogonal groups of plus-type. Recall that Theorem 6.8, which characterised Borel subgroups in terms of maximal isotropic flags, excluded such orthogonal groups. In fact, the Borel subgroups of orthogonal groups of plus-type arise as stabilisers of maximal flags in the *oriflamme geometry.* Full details may be found in [62], but for our purposes, a maximal flag in the oriflamme geometry consists of a pair $(\mathcal{F}_1, \mathcal{F}_2)$ of distinct maximal isotropic flags, where the first $m-1$ subspaces of $\mathcal{F}_1$ coincide with those of $\mathcal{F}_2$.

Proposition 7.25. *Let $H = \Omega^+_{2m}(q)$ or $SO^+_{2m}(q)$, where q is odd and $m \geq 3$. If X is an H-conjugacy class of involutions, then $\mathcal{F}(G, X)$ is connected.*

Proof. Let $t \in X$. As in the proof of Proposition 7.23 we may write $V = V_{+1} \perp V_{-1}$, where t acts trivially on V_{+1} and as -1 on V_{-1}. If $\dim V_{+1} = 0$, then t acts as -1 on the whole space V, implying $t \in Z(H)$, whence the result clearly holds. So assume $\dim V_{-1} = 2k$ where $k < m$. Since V has plus-type, using [62] we see that the spaces V_{+1} and V_{-1} have the same type. We first consider the case when both V_{+1} and V_{-1} are of plus-type. By Lemma 6.7 we may write

$$V_{+1} = L_1 \perp L_2 \perp \cdots \perp L_k$$

and

$$V_{-1} = L_{k+1} \perp L_{k+2} \perp \cdots \perp L_m.$$

If we write $L_i = \langle e_i, f_i \rangle$ for $1 \leq i \leq m$, then t stabilises the isotropic flag

$$\mathcal{F} = \langle e_1 \rangle \subset \langle e_1, e_2 \rangle \subset \cdots \subset \langle e_1, e_2, \ldots, e_{m-1}, e_m \rangle,$$

and also stabilises the isotropic flag

$$\mathcal{F}' = \langle e_1 \rangle \subset \langle e_1, e_2 \rangle \subset \cdots \subset \langle e_1, e_2, \ldots, e_{m-1}, f_m \rangle.$$

Since the first $m-1$ subspace of $\mathcal{F}$ and $\mathcal{F}'$ coincide, t stabilises a maximal flag in the oriflamme geometry, and so lies in a Borel subgroup B of H. Since t is semisimple, it must therefore lie in a maximal split torus T of H, and the result follows by Theorem 7.2.

Now suppose that both V_{+1} and V_{-1} are of minus-type. Then by Lemma 6.7 we may write

$$V_{+1} = L_1 \perp L_2 \perp \cdots \perp L_{k-1} \perp W_1$$

and

$$V_{-1} = L_{k+1} \perp L_{k+2} \perp \cdots \perp L_{m-1} \perp W_2,$$

where the L_i are hyperbolic lines and W_1 and W_2 are 2-spaces which contain no singular vectors. Since t stabilises the decomposition $V_{+1} \perp V_{-1}$, by Theorem 6.15 we have that t lies in a subgroup $M \leq H$, where

$$M \leq O^-_{2k}(q) \times O^-_{2(m-k)}(q).$$

If $k \neq m-k$, then M is a maximal subgroup of H. Otherwise, note that t also preserves the decomposition $V'_{+1} \perp V'_{-1}$, where

$$V'_{+1} = L_1 \perp L_2 \perp \cdots \perp L_{k-2} \perp W_1$$

and

$$V'_{-1} = L_k \perp L_{k+2} \perp \cdots \perp L_{m-1} \perp W_2,$$

so t lies in a maximal subgroup M' of H, where $M' \leq O^-_{2(k-1)}(q) \times O^-_{2(m-k+1)}(q)$.

Since t acts trivially on V_{+1}, and as -1 on V_{-1} which has even dimension, we have that t lies in a normal subgroup $N \lhd M$, where

$$N \leq SO^-_{2k}(q) \times SO^-_{2(m-k)}(q).$$

Now using Corollary 7.24 and Lemma 1.18, we see that $N \leq \mathrm{Stab}_H(Y)$, where Y is the connected component of $\mathcal{F}(H,X)$ which contains x. Since $N \lhd M$, we have that $M \leq \mathrm{Stab}_H(Y)$. But it is straightforward to show that t also lies in a distinct maximal subgroup M' of H, which has the same type as M. Now using similar arguments we have that $M' \leq \mathrm{Stab}_H(Y)$. By the maximality of M (or M') it follows that $H = \mathrm{Stab}_H(Y)$, whence $\mathcal{F}(H,X)$ is connected. □

Proposition 7.26. *Let $H = \Omega_{2m+1}(q)$ or $SO_{2m+1}(q)$, where q is odd and $m \geq 2$. If X is an H-conjugacy class of involutions, then $\mathcal{F}(H,X)$ is connected.*

Proof. Once again we write $V = V_{+1} \perp V_{-1}$. Since x must have determinant 1, it must be that V_{-1} has even dimension. Suppose that V_{-1} has plus-type. Then using Lemma 6.7 we have

$$V_{+1} = L_1 \perp L_2 \perp \cdots \perp L_k \perp W,$$

where W is a nonsingular 1-space, and

$$V_{-1} = L_{k+1} \perp L_{k+2} \perp \cdots \perp L_m.$$

Notice that t stabilises the maximal totally isotropic space

$$\langle e_1, e_2, \ldots, e_m \rangle,$$

and so lies in a Borel subgroup, and hence maximal torus of H. We may now apply Theorem 7.2 to show that $\mathcal{F}(H,X)$ is connected.

Now suppose that V_{-1} has minus-type, so we may write

$$V_{-1} = L_{k+1} \perp L_{k+2} \perp \cdots \perp L_{k-1} \perp W'$$

where W' is a 2-space which contains no singular points. By pairing W with any hyperbolic line L_i, or with W', we see that t stabilises a non-degenerate 3-space, and acts with determinant 1 on this space. Hence, using Theorem 6.15, t lies in a maximal subgroup $M \leq G$ such that $L \leq M \leq K$, where

$$L = \Omega_3(q) \times \Omega^{-}_{2m-2}(q)$$

and

$$K = SO_3(q) \times SO^{-}_{2m-2}(q).$$

Assume that $q \neq 3$. We see from [50] for example that $SO_3(q) \cong PGL_2(q)$, which has connected local fusion graphs. Therefore, by Lemma 1.18 and Proposition 7.24, the local fusion graphs of K are connected. Moreover, since $L \lhd K$ it must be that $M \lhd K$, and so by Lemma 1.19 the local fusion graphs of M must be connected. We deduce that $M \leq \mathrm{Stab}_H(Y)$. However, since $m \geq 2$, it can be seen from the decomposition of V that we may choose another non-degenerate 3-space which is stabilised by t. An identical argument shows that $M' \leq \mathrm{Stab}_H(Y)$, where M' is a maximal subgroup of H, and $M' \neq M$. Thus by the maximality of M or M', $\mathcal{F}(H, X)$ is connected.

When $q = 3$, we cannot use the method above since $PGL_2(3)$ has a disconnected local fusion graph. But we can easily check using MAGMA that the local fusion graphs of $SO_5(3)$ are connected, and so we may assume that $m \geq 3$. We then observe that t stabilises a non-degenerate 5-space, and argue as above. □

Having dealt with the matrix groups, we now start to work towards proving that the local fusion graphs of the corresponding projective orthogonal groups are also connected. As was the case for symplectic groups, the involution classes we must deal with arise from elements of the matrix groups which square to -1. Also exerting influence here is the congruence of the field. First we have the case where $q \equiv 1$ mod 4.

Lemma 7.27. *Let $H = SO^{\epsilon}_{2m}(q)$, where $m \geq 3$, $\epsilon = \pm$ and $q \equiv 1$ mod 4. If $t \in H$ is such that $t^2 = -1$, then H must have plus-type, and t lies in a maximal split torus of H.*

Proof. Since 4 divides $q-1$, there exists $\omega \in \mathbb{F}_q$ such that $\omega^2 = -1$. For $v \in V$ we may write

$$v = \frac{1}{2}(v + \omega v^t) + \frac{1}{2}(v - \omega v^t).$$

As $t^2 = -1$, we have $(v + \omega v^t)^t = -\omega v + v^t$ and $(v - \omega v^t)^t = \omega v + v^t$, and so

$$V = V_\omega \oplus V_{-\omega},$$

where

$$V_\omega = \{v \in V : v^t = \omega v\}$$

and

$$V_{-\omega} = \{v \in V : v^t = -\omega v\}.$$

Suppose $u, v \in V_\omega$. Then

$$\beta(u,v) = \beta(u^t, v^t) = \beta(\omega u, \omega v) = -\beta(u,v),$$

and so V_ω (and $V_{-\omega}$) is a totally singular subspace of dimension m. If $H = SO^-_{2m}(q)$, then this contradicts the fact that V has Witt index $m-1$, so we deduce that $H = SO^+_{2m}(q)$.

Using Lemma 6.7, choose a basis $\{e_1, \ldots, e_m, f_1, \ldots, f_m\}$ for V so that

$$V_\omega = \langle e_1, \ldots, e_m \rangle,$$

$$V_{-\omega} = \langle f_1, \ldots, f_m \rangle$$

and $\beta(e_i, f_j) = \delta_{ij}$. Then t stabilises the maximal isotropic flag

$$\mathcal{F} = \langle e_1 \rangle \subset \langle e_1, e_2 \rangle \subset \cdots \subset \langle e_1, e_2, \ldots, e_m \rangle,$$

and t also stabilises the flag

$$\mathcal{F}' = \langle e_1 \rangle \subset \langle e_1, e_2 \rangle \subset \cdots \subset \langle e_1, \ldots, e_{m-1}, f_m \rangle.$$

Since these flags coincide in their first $m-1$ subspaces, we have that t stabilises a maximal flag in the oriflamme geometry, and hence lies in a Borel subgroup, and consequently maximal split torus, of H. $\square$

Proposition 7.28. *Let $G = PSO^{\epsilon}_{2m}(q)$ or $P\Omega_{2m}(q)$, where $m \geq 3$, $\epsilon = \pm$, and $q \equiv 1$ mod 4, and let X be a G-conjugacy class of involutions. Then $\mathcal{F}(G, X)$ is connected.*

Proof. This follows from Propositions 7.24, 7.25 and Lemma 7.27. □

When $q \equiv 3$ mod 4 the situtation is slightly more complicated. The next lemma establishes some details regarding the relevant involution classes.

Lemma 7.29. *Let $H = SO^{\epsilon}_{2m}(q)$, where $m \geq 3$ and $q \equiv 3$ mod 4. Suppose there exists $t \in H$ such that $t^2 = -1$. Then the following hold:*

(i) Either m is even and H has plus-type, or m is odd and H has minus-type;

(ii) If $t \in H' = \Omega^{\epsilon}_{2m}(q)$, then there exists exactly one further H'-conjugacy class of elements which square to -1. Moreover, these classes do not fuse in H.

Proof. Choose a singular vector $v \in V$, and consider $U = \langle v, v^t \rangle$. If $\dim(U) = 1$, then it must be that $v^t = \omega v$, where $\omega^2 = -1$. Thus ω has multiplicative order 4 in $\mathbb{F}_q$, a contradiction since $q \equiv 3$ mod 4. Therefore U must be a 2-dimensional subspace of V. Since v is singular, it is certainly the case that v^t is also singular. We claim that $\beta(v, v^t) = 0$. Indeed, suppose that $\beta(v, v^t) \neq 0$, so that W has plus-type. Then using Theorem 6.15, t lies in a subgroup $M \leq H$, where

$$M = M_1 \times M_2 \leq O^+_2(q) \times O^{\epsilon}_{2m-2}$$

Hence we may write $t = t_1 t_2$, where $t_1 \in M_1$ and $t_2 \in M_2$. Theorem 11.4 of [62] tells us that $O^+_2(q) \cong \mathrm{Dih}(2(q-1))$, and since $q \equiv 3$ mod 4 this group contains no elements of order 4. But $t_1^2 = -1_{M_1}$, so t_1 must have order 4. This is a contradiction. Hence $\beta(v, v^t) = 0$, and U is totally singular.

Now, if possible, choose a singular vector in $U^{\perp} \backslash U$, and proceed as above. Suppose that $\epsilon = +$ and m is even. Following this method to its conclusion shows that t stabilises a maximal totally singular subspace of V of dimension m. By Theorem 11.61 of [62], both H and H' have exactly two orbits on the set of maximal totally singular subspaces of V, and consequently have exactly two conjugacy classes of elements which square to -1. Now suppose that m is odd. If such a t were to exist in H, then by breaking off totally singular 2-spaces stabilised by t as above, t would stabilise a totally singular subspace of dimension $m+1$, contradicting the Witt index of V being m.

We now suppose that H has minus-type. If m is even, then the Witt index $m-1$ of V is odd, and if we have $t \in H$ such that $t^2 = -1$, then the preceding argument provides a contradiction. So assume m is odd, so that $m-1$ is even. Then t stabilises a maximal totally singular subspace $W \subseteq V$, and so by Theorem 6.13, t lies in a subgroup $K \leq H$, where

$$K \cong C : (K_1 \times K_2) = [q^a] : (GL_{m-1}(q) \times SO_2^-(q)).$$

Note that the elements of C are unipotent, so have determinant 1. Since the elements of K_2 have determinant 1, this implies that the elements of K_1 have determinant 1 also. We may write $t = t_1t_2$, where $t_1 \in K_1$ and $t_2 \in K_2$. By Proposition 2.9.1 of [50], $K_2 \cong C_{q+1}$, a cyclic group which contains two elements which square to -1, namely t_2 and $(-1_{M_2})t_2$. We claim that t and $t' = t_1(-1_{M_2})t_2$ are not H-conjugate.

By Lemma 6.7 we can find hyperbolic lines $\langle e_1, f_1\rangle, \ldots, \langle e_{m-1}, f_{m-1}\rangle$ so that

$$W = \langle e_1, \ldots, e_{m-1}\rangle,$$

and so K_1, and t, stabilise the non-degenerate space

$$W \oplus W' = \langle e_1, \ldots, e_{m-1}\rangle \oplus \langle f_1, \ldots, f_{m-1}\rangle,$$

which has plus-type. Consequently t must also stabilise the 2-dimensional space $(W \oplus W')^{\perp}$, and since V has minus-type this space must have minus-type. Hence, using Theorem 6.15, t lies in a subgroup $L \leq H$, where $L = L_1 \times L_2 \leq O^+_{2m-2}(q) \times O_2^-(q)$. Notice that t' also stabilises the subspaces W and W'. Therefore any element $h \in H$ such that $t^h = t'$ must stabilise the decomposition $W \oplus W'$, and so lie in L. If $W^h = W$, then $h \in K$, and since t_2 and $(-1_{M_2})t_2$ are not conjugate in $SO_2^-(q)$, it cannot be the case that $t^h = t'$. Therefore h must swap the spaces W and W'. Since $h \in L$, we may write $h = h_1h_2$, where $h_1 \in L_1$ and $h_2 \in L_2$. Denote by r the product of the reflections $r_1, \ldots, r_{m-1}$, where r_i swaps e_i and f_i. Then r stabilises $W \oplus W'$, so lies in L_1, and since r is a product of $m-1$ reflections, where $m-1$ is even, $\det(r) = 1$, and so r lies in the subgroup of L_1 which is isomorphic to $SO^+_{2m-2}(q)$. But $K_1 \cong GL_{m-1}(q)$, so acts transitively on the (singular) vectors of W, and so we may write $h_1 = rk_1$, where k_1 is an appropriate element of $K_1 \leq SO_{2m-2}(q)$, and hence we may consider $h_1 \in SO_{2m-2}(q)$. This now forces $h_2 \in SO^-_2(q)$, but as already noted, t_2 and $(-1_{M_2})t_2$ are not conjugate in $SO^-_2(q)$. This contradiction implies that t and t' cannot be H-conjugate. To complete the proof, we note that since H acts transitively on the set of maximal totally isotropic subspaces of V (see [62]), any element of H which squares to -1 must be H-conjugate to either t or t'. □

We are now in a position to deal with remaining projective orthogonal groups.

Proposition 7.30. *Let $G = PSO^\epsilon_{2m}(q)$, where $\epsilon = \pm$, $q \equiv 3$ mod 4, and $m \geq 3$, and let X be a G-conjugacy class of involutions. Then $\mathcal{F}(G, X)$ is connected.*

Proof. Let $H = SO^\epsilon_{2m}(q)$, so that $G = \overline{H}$, and let $\overline{t} \in G$ be an involution. By Propositions 7.24 and 7.25, we need only consider the cases where $t \in H$ squares to -1. We proceed by induction on m, and first verify the cases when m is small.

When q is odd, we have the following isomorphisms (see [62], for example):

$$\begin{aligned}
P\Omega^+_4(q) &\cong PSL_2(q) \times PSL_2(q),\\
P\Omega^-_4(q) &\cong PSL_2(q^2),\\
P\Omega^+_6(q) &\cong PSL_4(q),\\
P\Omega^-_6(q) &\cong PSU_4(q),
\end{aligned}$$

from which we deduce that

$$\begin{aligned}
PSO^+_4(q) &\lhd PGL_2(q) \times PGL_2(q),\\
PSO^-_4(q) &\lhd PGL_2(q^2),\\
PSO^+_6(q) &\lhd PGL_4(q),\\
PSO^-_6(q) &\lhd PGU_4(q).
\end{aligned}$$

The first four automorphisms, along with Lemma 1.18, Theorems 7.5, 7.17 and Corollary 7.22 show that, with the exception of $P\Omega^+_4(3)$ (since $PSL_2(3)$ has a disconnected local fusion graph), the groups $P\Omega_4^\epsilon(q)$ and $P\Omega_6^\epsilon(q)$ have connected local fusion graphs. Since Lemma 7.29 shows that conjugacy classes of elements which square to -1 in $\Omega_4^\epsilon(q)$ and $\Omega_6^\epsilon(q)$ do not fuse in $SO_4^\epsilon(q)$ and $SO_6^\epsilon(q)$ respectively, we infer that the latter four families also have connected local fusion graphs, with the exception of $PSO_4^+(3)$. To allow us to include the case where $q = 3$, we also check using MAGMA the case when $G = PSO_8^+(3)$. We assume therefore that $m \geq 4$, and when $q = 3$ additionally assume that $m \geq 5$. The proof of Lemma 7.29 shows that t stabilises a totally singular 2-space $W \subseteq V$, and so by Theorem 6.13 we have $t \in M$, where M is a maximal subgroup of H, and

$$\overline{M} = C : (M_1 \circ M_2) \cong [q^a] : (GL_2(q) \circ SO_{2m-4}^\epsilon(q)).$$

We may write $t = t_1 t_2$, where $t_1 \in M_1$ and $t_2 \in M_2$. Since the subgroup C has odd order and is normalised by t, Lemma 1.22(iii) implies that $\overline{C} \leq \mathrm{Stab}_G(Y)$. Let $\overline{x}$ be any element of the $\overline{M}$-conjugacy class which contains $\overline{t}$, and write $x = x_1 x_2$ where $x_1 \in M_1$ and $x_2 \in M_2$. By induction there exists a path

$$t_2 \to x_2^{(1)} \to x_2^{(2)} \to \cdots \to x_2^{(k)} = x_2$$

of elements of X such that $x_2^{(i)} x_2^{(i+1)} = \pm y^{(i)}$, where $y^{(i)}$ has odd order, for each i. Thus for each i we have that the images of either $t_1 x_2^{(i)} t_1 x_2^{(i+1)}$ or $t_1 x_2^{(i)} (-1_{M_1}) t_1 x_2^{(i+1)}$ have odd order in G. Hence there exists a path in $\mathcal{F}(G, X)$ from $t = t_1 t_2$ to either $t_1 x_2$ or $(-1_{M_1}) t_1 x_2$. Since the local fusion graphs of $PGL_2(q)$ are connected (for $q \neq 3$) we may extend this path to either $x_1 x_2$ or $(-1_{M_1}) x_1 x_2$. In the former case we are done, whereas in the latter we use Lemma 7.7 to get a path from $(-1_{M_1}) x_1 x_2$ to $x_1 x_2 = x$.

We have therefore shown that $\overline{M} \leq \mathrm{Stab}_G(Y)$. However, it is certainly the case that t stabilises a totally singular 2-space of V which is distinct from W, and an identical argument shows that the corresponding maximal subgroup $\overline{M'} \leq \mathrm{Stab}_G(Y)$. The maximality of either $\overline{M}$ or $\overline{M'}$ now yields the result. □

Corollary 7.31. *Let $G = P\Omega_{2m}^\epsilon(q)$, where $\epsilon = \pm$, $q \equiv 3 \bmod 4$, and $m \geq 3$, and let X be a G-conjugacy class of involutions. Then $\mathcal{F}(G, X)$ is connected.*

Proof. We have that $P\Omega^{\epsilon}_{2m}(q)$ is a subgroup of index at most 2 in $PSO^{\epsilon}_{2m}(q)$, so is a normal subgroup. If $t \in X$, then the cases when t lies in a maximal split torus of G are covered by Propositions 7.24 and 7.25. The remaining cases follows from Proposition 7.30. □

7.6 Exceptional and Twisted Groups

To conclude this chapter, we consider the local fusion graphs of the exceptional and twisted groups of Lie-type, when the defining characteristic is odd. We require information on the number of involution classes in each case. This is detailed in Table 7.1, the data for which has been taken from Table 4.5.1 of [39].

Table 7.1: Involutions in Exceptional and Twisted Groups - q odd

Group	Involution Classes
$G_2(q)$	1
$^2G_2(q)$	1
$^3D_4(q)$	1
$F_4(q)$	2
$E_6(q)$	2
$^2E_6(q)$	2
$E_7(q)$	3
$E_8(q)$	2

Proposition 7.32. *Let $G = G_2(q)$, $^2G_2(q)$, $^3D_4(q)$ or $F_4(q)$, where q is odd, and let $t \in G$ be an involution. Then $C_G(t)$ is a maximal subgroup of G.*

Proof. In [65], descriptions of the maximal subgroups of these group are given, and it is noted which such subgroups are involution centralisers. The relevant pages are 125, 137, 144 and 159, and we use Table 7.1 to verify this accounts for all involution classes. We may now apply Lemma 1.20 in each case to deduce the result. □

Proposition 7.33. *Let $G = E_6(q)$, $^2E_6(q)$, $E_7(q)$ or $E_8(q)$, where q is odd. If X is a G-conjugacy class of involutions, then $\mathcal{F}(G, X)$ is connected.*

Proof. In Chapter 4 of [65], explicit representations of these groups are given, along with descriptions of their maximal split tori. Using this information it is straightforward to construct involutions which lie in the maximal split tori, and to determine the dimension of their eigenspaces which correspond to the eigenvalue -1. Since this dimension must be the same for conjugate involutions, with the help of Table 7.1 we can verify that representatives for each G-conjugacy class of involutions lie in a maximal split torus. This allows us to apply Theorem 7.2 to complete the proof. $\square$

Chapter 8

Groups of Lie-Type over Fields of Even Characteristic

In this chapter, our goal is to show connectedness of the local fusion graphs of finite, simple groups of Lie-type, defined over fields of even characteristic. As mentioned in Chapter 7, Theorem 7.2 is of no use to us in even characteristic, since in this situation involutions are not semisimple elements. We must therefore adopt a different strategy. As a first step, we wish to gather together some information regarding the conjugacy classes of involutions in classical groups in even characteristic.

8.1 Involutions

The material in this section comes almost exclusively from the paper by Aschbacher and Seitz [5]. Let V be an n-dimensional vector space over $\mathbb{F}_q$, where q is even. Suppose we have an involution $t \in SL(V)$. The *rank* of t is defined to be the dimension of the commutator space $[V, t]$ of t. The following result is well known.

Lemma 8.1. *Let $x, y \in SL(V)$ be involutions. Then x and y are conjugate in $SL(V)$ if and only if they have the same rank.*

Now fix an ordered basis for V. Given an integer l such that $1 \leq l \leq n/2$, we define the involution j_l of $SL(V)$ to be

$$j_l = \left(\begin{array}{c|c|c} I_l & & \\ \hline & I_{n-2l} & \\ \hline I_l & & I_l \end{array}\right),$$

where I_m is the $m \times m$ identity matrix, and I_0 is defined to be the 'empty' matrix. Then j_l has rank l, and is referred to as the *Suzuki form* of its invoution class.

Lemma 8.2. *The involutions j_l, where $1 \leq l \leq n/2$, form a complete set of representatives for the conjugacy classes of involutions of $SL(V)$.*

Proof. This follows as there are exactly $\lfloor n/2 \rfloor$ possibilities for the rank of an involution in $SL(V)$. □

We shall also require a further set of representatives for involution classes.

Lemma 8.3. *Let $H = SL(V)$, and for $1 \leq i \leq \lfloor n/2 \rfloor$ define*

$$x_i = \left(\begin{array}{c|c} B_i & \\ \hline & I_{n-2i} \end{array}\right),$$

where B_i is the $2i \times 2i$ matrix with 2×2 blocks

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

along its main diagonal, and zeroes elsewhere. Then

$$\mathcal{I} = \{x_i : 1 \leq i \leq \lfloor n/2 \rfloor\}$$

is a complete set of representatives of the conjugacy classes of involutions in H.

Proof. Since the elements of $\mathcal{I}$ have distinct ranks, the result follows from Lemma 8.1. □

Now suppose that V is a symplectic space, with symplectic form β. If t is an involution in $Sp(V)$, we define

$$V(t) = \{v \in V : \beta(v, v^t) = 0\}.$$

Also define E_{2m} to the the $2m \times 2m$ matrix with 1 in the $(2i, 2i-1)$ and $(2i-1, 2i)$ positions, for $1 \leq i \leq m$, and zeroes elsewhere. We shall make extensive use of the next result later in this chapter.

Proposition 8.4. *Let t be an involution in $Sp(V)$ with rank l. Then there exists a basis of V so that β has Gram matrix*

$$J = \left(\begin{array}{c|c|c} & & F \\ \hline & E_{n-2l} & \\ \hline F & & \end{array}\right)$$

in which $t = j_l$ and exactly one of the following holds:

(i) l is even, $V = V(t)$ and $F = E_l$;

(ii) l is odd, $V(t) = \langle e_i : i \neq n-l+1 \rangle$, $V(t)^\perp = \langle e_1 \rangle$,

$$[V(t), t]^\perp = \langle e_i : 1 \leq i \leq n-l+1 \rangle,$$

$$[V(t), t] = \langle e_i : 1 \leq i \leq l \rangle,$$

$$F = \left(\begin{array}{c|c} 1 & \\ \hline & E_{l-1} \end{array}\right).$$

(iii) l is even, $V(t) = \langle e_i : 1 \leq i < n \rangle$, $V(t)^\perp = \langle e_1 \rangle$,

$$[V(t), t]^\perp = \langle e_i : 1 \leq i \leq n-l+1 \rangle,$$

$$[V(t), t] = \langle e_i : 1 \leq i < l \rangle,$$

$$F = \left(\begin{array}{c|c|c} & & 1 \\ \hline & E_{l-2} & \\ \hline 1 & & 1 \end{array}\right).$$

Proof. See 7.6 of [5]. □

An involution $t \in Sp(V)$ is said to be in *symplectic Suzuki form* if the basis for V is chosen as in Proposition 8.4. We also denote by a_l, b_l and c_l the Suzuki forms in parts (i), (ii) and (iii) of Proposition 8.4.

Proposition 8.5. *Let t and s be involutions in $Sp(V)$. Then the following are equivalent:*

(i) t is conjugate to s in $Sp(V)$;

(ii) t and s have the same symplectic Suzuki form;

(iii) t and s have the same rank l, and if l is even then $V(t)$ and $V(s)$ have the same dimension.

Proof. This follows from Proposition 8.4 and the fact that $Sp(V)$ is transitive on the set of ordered symplectic bases of V (see [62]). $\square$

8.2 Linear Groups

We are now in a position to examine the local fusion graphs of linear groups. Let $H = SL_n(q) \cong SL(V)$, where q is even. First we have a lemma concerning our set of involution representatives $\mathcal{I}$ from Lemma 8.3.

Lemma 8.6. *Let $x_i \in \mathcal{I}$ be a representative of an H-conjugacy class X, and let x_i' be equal to x_i but with at least one 2×2 block on the diagonal of B_i transposed. Then x_i and x_i' are adjacent in $\mathcal{F}(H, X)$.*

Proof. Since

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

it is easy to see that there exists an element of H, built up of suitable blocks, which conjugates x_i to x_i'. Furthermore, we have

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

which has order 3, and it follows that $x_i x_i'$ also has order 3. Hence x_i and x_i' are adjacent in $\mathcal{F}(H, X)$. $\square$

Theorem 8.7. *If $H = SL_n(q)$ or $GL_n(q)$, and X is an H-conjugacy class of involutions, then $\mathcal{F}(H, X)$ is connected.*

Proof. When q is even, any involution of $GL_n(q)$ has determinant 1, so lies in $SL_n(q)$. Moreover, it is clear that no involution classes of $SL_n(q)$ fuse in $GL_n(q)$. Hence it suffices to prove the result for $H = SL_n(q)$. By Lemma 8.3 we have $x_k \in X$ for some k. Denote by Y the connected component of $\mathcal{F}(H, X)$ which contains x_k. Note that for any $y \in Y$, $C_H(y) \leq \mathrm{Stab}_H(Y)$. By Proposition 6.16, the set

$$\mathcal{A} = \{I_n + \lambda e_{ij} : i \neq j, \lambda \in \mathbb{F}_q\}$$

generates H (where the e_{ij} are elementary $n \times n$ matrices). We claim that if $a \in \mathcal{A}$, then $a \in C_H(y)$ for some $y \in Y$. Indeed, let $a = I_n + \lambda e_{ij}$. We may check that a centralises x_k if and only if the i-th column and j-th row of x_k contain exactly one non-zero entry each. If this is not the case, by transposing a suitable 2×2 block of B_i, we obtain an element x'_k which is centralised by a. Moreover, by Lemma 8.6, x'_k is adjacent to x_k in $\mathcal{F}(H, X)$, so is certainly in Y. Hence

$$\mathcal{A} \subseteq \langle C_H(y) : y \in Y \rangle \leq \mathrm{Stab}_H(Y).$$

Since $\mathcal{A}$ generates H, we have that $H = \mathrm{Stab}_H(Y)$. But H acts transitively on X, implying that $Y = X$, so $\mathcal{F}(H, X)$ is connected. □

In preparation for dealing with the simple groups $PSL_n(q)$, we require a lemma regarding $GL_2(q)$.

Lemma 8.8. *Let $K = GL_2(q) \cong GL(V)$, and suppose $g \in K$ is an element of even order such that $g^2 \in Z(K)$. Then g is K-conjugate to an element y such that the product yy^T has odd order.*

Proof. Observe that

$$Z = Z(K) = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda \in \mathbb{F}_q^* \right\},$$

and hence $|Z| = q-1$, which is odd. Let $SL_2(q) \cong H \leq G$, and note that $Z \cap H = 1$. We therefore have $G = ZH$. Furthermore, we know that any element of even order in H must be an involution. Hence if $x \in K$ has even order, then $x = zy$ for some $z \in Z$ and $y \in H$ an involution. Thus $x^2 \in Z$, so

$$x^2 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$$

for some $\lambda \in \mathbb{F}_q^*$. Thus the minimal polynomial of x is $\chi^2 + \lambda$.

Now suppose $g \in K$ is such that $g^2 \in Z$. Then by the above argument g has minimal polynomial $\chi^2 + \alpha$ for some $\alpha \in \mathbb{F}_q^*$. Choose $v \in V$ such that $v^g = \mu w$, where $w \notin \langle v \rangle$ and $\mu^2 = \alpha$ (this is possible since otherwise g would be diagonalisable, contradicting our assumption that g has even order). Suppose the scalar μ has multiplicative order k in $\mathbb{F}_q$. Then by choosing basis $\mathcal{B} = \{v + w, \mu^{k-1} v\}$ for V, we see that g has representation

$$g_{\mathcal{B}} = \begin{pmatrix} \mu & 1 \\ 0 & \mu \end{pmatrix}.$$

But now

$$g_{\mathcal{B}} g_{\mathcal{B}}^T = \begin{pmatrix} \omega^2 + 1 & \omega \\ \omega & \omega^2 \end{pmatrix},$$

which has minimal polynomial $\chi^2 + \chi + \omega^4$. Hence $g_{\mathcal{B}} g_{\mathcal{B}}^T$ cannot have even order. Since H acts transitively on ordered bases of V, g and $y = g_{\mathcal{B}}$ must be H-conjugate. $\square$

Lemma 8.9. *Let $H = SL_n(q) \cong SL(V)$, suppose $g \in H$ is such that $g^2 \in Z(H)$. Then g is H-conjugate to an element*

$$y = \left(\begin{array}{c|c} A_{2k} & \\ \hline & \lambda I_{n-k} \end{array}\right),$$

where A is the $2k \times 2k$ matrix with 2×2 blocks

$$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$$

along its main diagonal and zeroes elsewhere, and $\lambda \in \mathbb{F}_q^*$.

Furthermore, if y^* is equal to y but with at least one 2×2 block on the diagonal of A transposed, then y and y^* are H-conjugate, and yy^* has odd order.

Proof. Write $Z = Z(G)$ and note that $|Z| = q - 1$, which is odd. As $g^2 \in Z$, g must have minimal polynomial $\chi^2 + \alpha$ for some $\alpha \in \mathbb{F}_q^*$. By choosing a basis for V in a similar manner to that in the proof of Lemma 8.8, we see that g is $GL_n(q)$-conjugate, and consequently H-conjugate, to an element y as in the statement of the lemma, where $\lambda^2 = \alpha$. Now let y^* equal y but with one or more blocks of A transposed. Since

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

it follows that y and y^* are H-conjugate. Furthermore, using Lemma 8.8 and the fact that $|Z|$ is odd, we see that yy^* is essentially a direct sum of 2×2 blocks, each of which has odd order. Hence yy^* also has odd order. □

Theorem 8.10. *If $G = PSL_n(q)$ and X is a G-conjugacy class of involutions, then $\mathcal{F}(G, X)$ is connected.*

Proof. Write $G = \overline{H}$. Let $\bar{t} \in X$ have preimage $t \in H$. As $\bar{t}$ is an involution, we must have $t^2 \in Z$. So by the first part of Lemma 8.9, t is H-conjugate to an element

$$y = \left(\begin{array}{c|c} A_k & \\ \hline & \lambda I_{n-k} \end{array}\right).$$

Therefore $\bar{t}$ and $\bar{y}$ are G-conjugate, so without loss of generality let $t = y$.

Let

$$\mathcal{A} = \{I_n + \lambda e_{ij} : i \neq j, \lambda \in \mathbb{F}_q\}$$

be the generating set for H as in Proposition 6.16. As in the proof of Theorem 8.7, if $a \in \mathcal{A}$ then a centralises either t or t^*, where t^* is equal to t but with a suitable block of A transposed. Hence for each $\bar{a} \in \overline{\mathcal{A}}$, $\bar{a}$ centralises either $\bar{t}$ or $\overline{t^*}$. But by Lemma 8.9, t and t^* are H-conjugate, so must be their images must be G-conjugate. Also tt^* has odd order, so $\overline{tt^*}$ must have odd order. Thus $\bar{t}$ and $\overline{t^*}$ are adjacent in $\mathcal{F}(G, X)$.

Therefore $\langle \overline{\mathcal{A}} \rangle = \mathrm{Stab}_G(Y)$, where Y is the connected component of $\mathcal{F}(G, X)$ which contains $\bar{t}$. It follows that $\mathcal{F}(G, X)$ is connected. □

8.3 Symplectic Groups

Next we address the case of symplectic groups. Let $H = Sp_{2m}(q) \cong Sp(V)$. We have seen previously that $Z(H) = \{\pm 1\}$, and so when q is even the centre of H is trivial. It follows that $PSp_{2m}(q) \cong Sp_{2m}(q)$ when q is even, and so we can write $G = Sp_{2m}(q)$, which is a simple group except for the case $Sp_4(2)$. This simplifies considerably our treatment of the local fusion graphs.

Theorem 8.11. *If $G = Sp_{2n}(q)$ where q is even, with X a G-conjugacy class of involutions, then $\mathcal{F}(G, X)$ is connected.*

Proof. Let V have basis so that β has Gram matrix

$$J = \left(\begin{array}{c|c} & I_n \\ \hline I_n & \end{array}\right).$$

By Proposition 6.17, G is generated by the set $\mathcal{E}$ consisting of matrices of the forms

$$\left(\begin{array}{c|c} I_n & \lambda e_{ii} \\ \hline & I_n \end{array}\right), \left(\begin{array}{c|c} I_n & \\ \hline \lambda e_{ii} & I_n \end{array}\right),$$

$$\left(\begin{array}{c|c} I_n & \lambda(e_{ij} + e_{ji}) \\ \hline & I_n \end{array}\right), \left(\begin{array}{c|c} I_n & \\ \hline \lambda(e_{ij} + e_{ji}) & I_n \end{array}\right).$$

Let $t \in X$, with Y the relevant connected component of $\mathcal{F}(G, X)$. By 2.1.16 of [62], t is G-conjugate to an element

$$x = \left(\begin{array}{c|c} I_n & A \\ \hline & I_n \end{array}\right),$$

where

$$A = \left(\begin{array}{c|c} A' & \\ \hline & 0 \end{array}\right)$$

and A' is either invertible and diagonal, or has blocks

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

along its main diagonal. In particular, note every row (and column) of A' contains one nonzero entry. Without loss of generality let $t = x$. Note that $t^T \in G$, and that $t^T \in X$ since t^T has the same symplectic Suzuki form as x, as in Proposition 8.5.

We claim that t and t^T are adjacent in $\mathcal{F}(G, X)$. Define elements $a_i \in \mathbb{F}_q$, $1 \leq i \leq n$, by setting a_i to be the nonzero entry in the i-th row of A' if it exists, and zero otherwise. Note that at least one of the a_i must be nonzero. Now define an element t_J of $GL_{2n}(q)$ as follows:

$$t_J = \left(\begin{array}{c|c|c|c} B_1 & & & \\ \hline & B_2 & & \\ \hline & & \ddots & \\ \hline & & & B_n \end{array}\right),$$

where

$$B_i = \begin{pmatrix} 1 & a_i \\ 0 & 1 \end{pmatrix}.$$

Consider the product $t_J t_J^T$ as a direct sum of elements in $GL_2(q)$. Each 2×2 block is either I_2, or has minimal polynomial $\chi^2 + a_i^2\chi + 1$ where $a_i \neq 0$. We may therefore apply the argument of Lemma 8.8 to see that $t_J t_J^T$ has odd order.

Suppose we interchange two rows of t, and then interchange the corresponding columns. This can be achieved by conjugating t by an invertible matrix r, where $r^{-1} = r^T$ (indeed, r can be identified with an element of the symmetric group $\mathrm{Sym}(2n)$). Furthermore, note that t can be transformed into t_J by a series of these operations. Hence there exists an invertible matrix s, with $s^{-1} = s^T$, such that $s^T t s = t_J$. Now consider the product tt^T. We have

$$\begin{aligned} o(tt^T) &= o(s^{-1}tt^Ts) = o(s^{-1}tss^{-1}t^Ts) \\ &= o(s^Ttss^Tt^Ts) = o(s^Tts(s^Tts)^T) \\ &= o(t_J t_J^T). \end{aligned}$$

Thus tt^T has odd order.

Now suppose $e \in \mathcal{E}$. By observing the configuration of any element of $\mathcal{E}$, and of t, it is easily seen that either $e \in C_G(t)$, or $e \in C_G(t^T)$. Since both t and t^T lie in Y, we have that $e \in \mathrm{Stab}_G(Y)$ for all $e \in \mathcal{E}$. But $\langle \mathcal{E} \rangle = G$, so $G = \mathrm{Stab}_G(Y)$. Hence $X = Y$, and $\mathcal{F}(G, X)$ is connected. □

As an immediate corollary, we have the following result concerning orthogonal groups of odd dimension.

Corollary 8.12. *If $G = O_n(q)$, where $n \geq 5$ is odd, q is even, and X is a G-conjugacy class of involutions. The $\mathcal{F}(G, X)$ is connected.*

Proof. Write $n = 2m + 1$. Then since q is even, $O_n(q) \cong Sp_{2m}(q)$ (see, for example, 11.9 of [62]), and the result follows from Theorem 8.11. □

8.4 Unitary Groups

We now move on to address the case of unitary groups. To begin with, we concentrate on the case when the dimension is even. Let $H = SU_{2m}(q) \cong SU(V)$, where the unitary form β on V has Gram matrix

$$J = \left(\begin{array}{c|c} & I_m \\ \hline I_m & \end{array}\right).$$

Denote by τ the involutary automorphism of $\mathbb{F}_{q^2}$ associated to β.

Theorem 8.13. *If $H = SU_{2m}(q) \cong SU(V)$ where q is even, and X is an H-conjugacy class of involutions, then $\mathcal{F}(H, X)$ is connected.*

Proof. By Lemma 8.1 and Theorem 7.13, involutions $x, y \in H$ are H-conjugate if and only if they have the same rank. Therefore we may index the H-conjugacy classes of involutions $\{X_i\}$, $1 \leq i \leq m$, where i is the rank, and for the class X_i choose representative

$$x_i = \left(\begin{array}{c|c} I_m & B_i \\ \hline 0 & I_m \end{array}\right)$$

where

$$B_i = \left(\begin{array}{c|c} I_i & \\ \hline & 0 \end{array}\right).$$

Denote by $\mathcal{A}$ the set of matrices of the form

$$\left(\begin{array}{c|c} I_m & \mu e_{ii} \\ \hline & I_m \end{array}\right), \left(\begin{array}{c|c} I_m & \\ \hline \mu e_{ii} & I_m \end{array}\right),$$

$$\left(\begin{array}{c|c} I_m & \lambda e_{ij} + \lambda^\tau e_{ji} \\ \hline & I_m \end{array}\right), \left(\begin{array}{c|c} I_m & \\ \hline \lambda e_{ij} + \lambda^\tau e_{ji} & I_m \end{array}\right),$$

where $\mu, \lambda \in \mathbb{F}_{q^2}$, and $\mu + \mu^\alpha = 0$. By Proposition 6.18 we have $H = \langle \mathcal{A} \rangle$. Notice that for every $a \in \mathcal{A}$, either $a \in C_H(x_i)$ or $a \in C_H(x_i^T)$. Since x_i, x_i^T are H-conjugate, and $x_i x_i^T$ has odd order (as in the proof of Theorem 8.11), the result follows. $\square$

Now suppose $H = SU_{2m+1}(q)$ where n is odd, and choose basis so that the unitary form has Gram matrix

$$J = \left(\begin{array}{c|c|c} & I_m & \\ \hline I_m & & \\ \hline & & 1 \end{array}\right).$$

Theorem 8.14. *If $G = SU_{2n+1}(q)$, and X is an H-conjugacy class of involutions, then $\mathcal{F}(H, X)$ is connected.*

Proof. Let $\mathcal{A}'$ be our set of generators from the even dimension case, considered as elements of H in the obvious way. Then $\mathcal{A}'$ generates a subgroup $K \leq H$, where $K \cong SU_{2m}(q)$. Notice that K stabilises a non-degenerate $2m$-space W of V. By Theorem 6.11, K lies in a unique maximal subgroup $M \leq H$, where $M = \mathrm{Stab}_H(W)$, and

$$SU_{2m}(q) \times SU_1(q) \leq M \leq GU_{2m}(q) \times GU_1(q).$$

Let $\alpha \in \mathbb{F}_{q^2}$ be such that $\alpha + \alpha^\tau = 1$, and define

$$y = \left(\begin{array}{c|c|c} I_n & \alpha e_{11} & e_{11} \\ \hline & I_n & \\ \hline & e_{11} & 1 \end{array}\right) \in SU_{2n+1}(q),$$

where e_{11} is the elementary $n \times n$ matrix with 1 in position $(1, 1)$. This element does not stabilise W, so by the maximality of M we have $H = \langle H, y \rangle$.

As in the $2m$-dimensional case there are n conjugacy classes of involutions which we may index by rank. For the class X_i choose representative

$$x_i = \left(\begin{array}{c|c|c} I_m & B_i & \\ \hline & I_m & \\ \hline & & 1 \end{array}\right)$$

where

$$B = \left(\begin{array}{c|c} I_i & \\ \hline & 0 \end{array}\right).$$

We have that $x_i \in K$ for all i, and so if Y is the connected component of $\mathcal{F}(H, X_i)$ which contains x_i, the by Theorem 8.13 we have $K \leq \mathrm{Stab}_H(Y)$. But also note that $y \in C_H(x_i)$ for all i. Hence $H = \langle K, y\rangle \leq \mathrm{Stab}_H(Y)$, as required. $\square$

The case of the projective unitary groups now follows very quickly, using a result of Dye.

Theorem 8.15. *If $G = PSU_n(q)$ and X is a G-conjugacy class of involutions, then $\mathcal{F}(G, X)$ is connected.*

Proof. By Theorem 3 of [33] the conjugacy classes of involutions of G are in one to one correspondence with those of H. The result now follows from Theorems 8.13 and 8.14. $\square$

8.5 Orthogonal Groups

Recall from Chapter 6 that an orthogonal group $O(V)$ preserves a non-singular quadratic form $Q : V \to \mathbb{F}_q$, and that Q defines a non-degenerate, symmetric, bilinear form β on V which $O(V)$ also preserves. Suppose now that q is even. By Corollary 8.12 we need only consider the case where $n = 2m$. Let $v \in V$ be any vector. Then

$$\beta(v, v) = 2Q(v) = 0,$$

and so β must be an alternating form. Hence, when q is even, we have $O_{2m}(q) \leq Sp_{2m}(q)$. In particular, every orthogonal group in even characteristic must have trivial centre (when $m \geq 3$), and its elements must have determinant 1.

Theorem 8.16. *If $G = \Omega^-_{2m}(q) \cong \Omega^-(V)$, where $m \geq 3$, and X is a G-conjugacy class of involutions, then $\mathcal{F}(G, X)$ is connected.*

Proof. Let $t \in X$ be an involution, with Y the connected component of $\mathcal{F}(G, X)$ which contains t, and let r be the dimension of the fixed space W of t in V. From [32] we have that $m \leq r \leq 2m - 1$. As the Witt index of G is equal to $m - 1$, there must exist $w \in W$ such that $Q(w) \neq 0$. Therefore t fixes a non-singular 1-space of V.

Let $M = \mathrm{Stab}_G(w)$. By Theorem 6.15 we have that M is a maximal subgroup of G, and

$$\Omega_{2m-1}(q) \times \Omega_1(q) \leq M \leq O_{2m-1}(q) \times O_1(q).$$

Since the elements of our orthogonal groups have determinant 1, and Corollary 8.12 yields $O_{2m-1}(q) \cong Sp_{2m-2}(q)$, we deduce that $M \cong Sp_{2m-2}(q)$. Now Theorem 8.11 tells us that $M \leq \mathrm{Stab}_G(Y)$. We wish to show that t fixes another non-singular 1-space of V. If $r \geq m+1$, then this is clear, so suppose $r = m$. Then there must exist $u \in W$ such that $Q(u) = 0$. Now t fixes $\lambda u + w$, where $\lambda \in \mathbb{F}_q$, and since $Q(\lambda u + w) = \lambda^2 Q(u) + \lambda\beta(u, w) + Q(w)$ we can choose λ so that $\lambda u + w$ is non-singular. Hence t does indeed fix another non-singular vector of V, and t therefore lies in another maximal subgroup, M' say, also isomorphic to $Sp_{2m-2}(q)$. Thus $M' \leq \mathrm{Stab}_G(Y)$. But M is maximal, so $\langle M, M' \rangle = G$, and we have $G = \mathrm{Stab}_G(Y)$. It follows that $\mathcal{F}(G, X)$ is connected. □

Theorem 8.17. *Let $G = \Omega^+_{2m}(q)$, where $m \geq 3$ is odd, and let X be a G-conjugacy class of involutions. Then $\mathcal{F}(G, X)$ is connected.*

Proof. We use the notation from the previous proof. In this case the Witt Index of G is equal to m. However, using [32] we have $m + 1 \leq r \leq 2m - 1$. By arguing as in the proof of Theorem 8.16, we see that t fixes two distinct non-singular 1-spaces of V, and thus lies in distinct maximal subgroups M and M', both of which are isomorphic to $Sp_{2m-2}(q)$. As previously, the result follows. □

Theorem 8.18. *Let $G = \Omega^+_{2m}(q)$, where $m \geq 4$ is even, and let X be a G-conjugacy class of involutions. Then $\mathcal{F}(G, X)$ is connected.*

Proof. Let $t \in X$. If $\mathrm{Rank}(t) < m$, then t stabilises a non-singular 1-space of V, and we may argue as in the proof of Theorem 8.16. However, we must be careful when $\mathrm{Rank}(t) = m$. Since $G \leq Sp_{2m}(q)$, we make use of Proposition 8.4. Adopting its notation, we see that in this case t is either of type a_m or c_m. Firstly, let $t = a_m$, and let V have basis $\{x_1, \ldots, x_{2m}\}$. Then

$$t = \left(\begin{array}{c|c} I_m & 0 \\ \hline I_m & I_m \end{array}\right)$$

and the symplectic form on V has Gram matrix

$$J = \left(\begin{array}{c|c} 0 & F \\ \hline F & 0 \end{array}\right)$$

where F is the $m \times m$ matrix with 1 in the $(2i, 2i-1)$ and $(2i-1, 2i)$ positions and 0 elsewhere. Furthermore, by 8.2 of [5] we have that $Q(x_i) = 0$ for $1 \leq i \leq 2m$.

Let $O = \{1 \leq i \leq 2m : i \text{ odd}\}$, and $E = \{1 \leq j \leq 2m : j \text{ even}\}$. Let $W = \langle x_i : i \in O\rangle$, and $W' = \langle x_j : j \in E\rangle$. Certainly it is the case that $V = W \oplus W'$, and both W and W' are totally singular. Furthermore, t fixes both W and W'. Thus $t \in \mathrm{Stab}_G(W \oplus W') = M_1$. By Theorem 6.14 we have that $M_1 \cong H : 2$, where $H \cong GL_m(q)$, and the outer automorphism is an involution σ which has the effect of swapping W and W'. As t fixes both W and W', we deduce that $t \in H$. Now Theorem 8.7 implies that $H \leq \mathrm{Stab}_G(Y)$. Also, since σ swaps W and W', the dimension of the fixed spaces of t and t^σ are the same. Proposition 8.4 now tells us that t and t^σ are H-conjugate, which yields $\sigma \in \mathrm{Stab}_G(Y)$, and so $M_1 \leq \mathrm{Stab}_G(Y)$.

We now partition $\{1, \ldots, 2m\}$ into four subsets, by defining

$$\begin{aligned} I_1 &= \{1, \ldots, m/2\}, \\ I_2 &= \{m/2+1, \ldots, m\}, \\ I_3 &= \{m+1, \ldots, 3m/2\}, \\ I_4 &= \{3m/2+1, \ldots, 2m\}. \end{aligned}$$

Note that this is possible since m is even. Now define

$$U = \langle x_i, x_j, x_k, x_l : i \in I_1 \cap O, j \in I_3 \cap O, k \in I_2 \cap E, l \in I_4 \cap E \rangle$$

and

$$U' = \langle x_i, x_j, x_k, x_l : i \in I_1 \cap E, j \in I_3 \cap E, k \in I_2 \cap O, l \in I_4 \cap O \rangle.$$

Once more we have that $V = U \oplus U'$, both U and U' are totally singular, $U^t = U$ and $(U')^t = U'$. Hence $t \in M_2$, where $M_2 \cong M_1$ and $M_2 \neq M_1$. Arguing as above we see that $M_2 \leq \mathrm{Stab}_G(Y)$, and so $\langle M_1, M_2 \rangle \leq \mathrm{Stab}_G(Y)$. But M_1 is maximal (as is M_2), so the result follows.

The other possibility is that $t = c_m$. Then

$$t = \left(\begin{array}{c|c} I_m & 0 \\ \hline I_m & I_m \end{array}\right)$$

and the symplectic form on V has Gram matrix

$$J = \left(\begin{array}{c|c} 0 & F \\ \hline F & 0 \end{array}\right),$$

where

$$F = \left(\begin{array}{c|c|c} & & 1 \\ \hline & E_{m-2} & \\ \hline 1 & & 1 \end{array}\right)$$

and E_{m-2} is the $(m-2) \times (m-2)$ matrix with 1 in the $(2i, 2i-1)$ and $(2i-1, 2i)$ positions and 0 elsewhere. We can see from this description that t stabilises a non-degenerate 4-space, namely

$$U = \langle x_1, x_m, x_{m+1}, x_{2m} \rangle.$$

Thus, using Theorem 6.15 with further details gleaned from [50], t lies in a maximal subgroup

$$M_1 \cong (L_1 \times L_2) : 2 = (\Omega_4^+(q) \times \Omega_{2m-4}^+(q)) : 2,$$

where the outer automorphism is $r = r_1 r_2$, a product of reflections in non-singular vectors in U and $U^\perp$, respectively. We wish to show that without loss of generality t can be chosen to lie in the base group $L = L_1 \times L_2$.

Let $h_1 \in L_1$, $h_2 \in L_2$ be involutions of type c_2 and c_{m-2} repectively, and let $s = h_1h_2$. Then s is an involution of G of rank $2 + (m-2) = m$. However, we do not yet know the type of s. Recall from Section 8.1 that

$$V(s) = \{v \in V : \beta(v, v^s) = 0\}.$$

This is a subspace of V of codimension 0 or 1. Since, for example, h_2 is of type c_{m-2}, we see from Proposition 8.4 that $V(h_2)$ has codimension 1. Now, since $V = U \oplus U^\perp$, it is easy to see that $V(s)$ must also have codimension 1. But now using Proposition 8.4 once more we see that this implies that s is G-conjugate to an involution of type c_m, so is therefore conjugate to t. Thus without loss we may take $t = s$.

From Proposition 2.9.1 of [50] we have that

$$\Omega_4^+(q) \cong PSL_2(q) \times PSL_2(q),$$

which has connected local fusion graphs by Theorem 3.1 and Lemma 1.18. Using Lemma 1.18 again, and induction, we now have that $L \leq \mathrm{Stab}_G(Y)$. We next show that $r \in \mathrm{Stab}_G(Y)$, whence $M_1 \leq \mathrm{Stab}_G(Y)$. It suffices to show that r does not fuse t^L with another class of H. As r fixes U and $U^\perp$, the problem reduces to showing non-fusion in the relevant classes of L_1 and L_2.

Suppose r_2 is the reflection in some non-singular vector $v \in U^\perp$. Then by definition we have

$$xr_2 = x - \frac{\beta(x, v)}{Q(v)}v,$$

for all $x \in U^\perp$, which in even characteristic simplifies to

$$xr_2 = x + \beta(x, v)v.$$

We observe from this that r_2 fixes U pointwise. Similarly, r_1 will fix $U^\perp$ pointwise. Thus when considering L_2, say, we need only consider the effect of conjugation by r_2.

Consider $h_2 \in L_2$. As the rank is invariant under conjugation, the only possibility for fusion is that $h_2^{r_2} = h_2'$ where h_2' has type a_{m-2}. Then h_2' stabilises a decomposition $U^\perp = W \oplus W'$, where both W and W' are totally singular subspaces of dimension $m-2$, and so h_2 must stabilise the decomposition $W^{r_2} \oplus (W')^{r_2}$. Since elements G

preserves Q, W^{r_2} and $(W')^{r_2}$ must also be totally singular. But this shows that h_2 has type a_{m-2}, a contradiction. Applying the same reasoning to the subgroup L_1, we have that r does not fuse the relevant classes of L. Thus $M_1 \leq \mathrm{Stab}_G(Y)$.

Now note that t stabilises another non-degenerate 4-space, for example

$$U' = \langle x_1, x_m, x_{m+1}, x_{2m-1} \rangle,$$

and thus lies in a maximal subgroup M_2 such that $M_2 \neq M_1$. We may apply the same argument as above to show that $M_2 \leq \mathrm{Stab}_G(Y)$, and so $G = \langle M_1, M_2 \rangle \leq \mathrm{Stab}_G(Y)$. Hence $\mathcal{F}(G, X)$ is connected. □

8.6 Exceptional and Twisted Groups

To conclude our investigations into the local fusion graphs of finite groups of Lie-type, we must consider the exceptional and twisted groups of Lie-type in even characteristic. The Suzuki groups are straightfoward to deal with.

Proposition 8.19. *If $G = Sz(q) \cong {}^2B_2(2^{2n+1})$, with X a G-conjugacy class of involutions, then $\mathcal{F}(G, X)$ is connected, and* $\mathrm{Diam}(\mathcal{F}(G, X)) = 2$.

Proof. This succinct proof is due to Ben Fairbairn. From [60] we have that G contains just a single class of involutions, and that if $x, y \in X$ then either x and y commute, or the product xy has odd order. Furthermore, if $x \in P$ where $P \in \mathrm{Syl}_2(G)$, then $C_G(x) \leq P$. Also, the number of involutions which lie in P is $q-1$. We therefore have that $|X \setminus \Delta_1(x)| = q-1$. Since $|X| > 2(q-1)$, the result follows by Lemma 1.16. □

Table 8.1 lists the number of involution classes of the remaining exceptional and twisted groups. This data is taken from [5].

Recall from Theorem 6.9 that in the majority of cases, if $G(q^r)$ is a finite group of Lie-type defined over the field $\mathbb{F}_{q^r}$ where r is prime, then $G(q)$, the group of the same type defined over $\mathbb{F}_q$, is a maximal subgroup of $G(q^r)$. We shall need the following two lemmas regarding involutions and their centralisers.

Table 8.1: Involutions in Exceptional and Twisted Groups - q even

Group	Involution Classes
$G_2(q)$	2
${}^3D_4(q)$	2
$F_4(q)$	4
${}^2F_4(2)'$	2
${}^2F_4(q)$	2
$E_6(q)$	3
${}^2E_6(q)$	3
$E_7(q)$	5
$E_8(q)$	4

Lemma 8.20. *Let $G = G(2^r)$ be an exceptional or twisted group of Lie-type, with X a G-conjugacy class of involutions. Then there exists $t \in X$ such that $t \in H$, where H is the subgroup of G naturally isomorphic to $G(2)$.*

Proof. In [5], representatives for every involution class in each exceptional or twisted group are given, in terms of products of involutions from commuting root groups. Since each of these involutions is defined using only the base field $\mathbb{F}_2$, these representatives lie in H. □

Lemma 8.21. *Let $G = G(q^r)$ be an exceptional or twisted group of Lie-type where q is even, and suppose that r is prime. Write H for the subgroup of G which is isomorphic to $G(q)$. If $t \in G$ is an involution, then $C_G(t) \nleq H$.*

Proof. Again we refer the representatives given in [5] in terms of root groups. Each of these root groups is isomorphic to the additive group of the field $\mathbb{F}_{q^r}$, and contains elements which do not lie in H. Since the root groups are abelian, and commute, such elements lie in $C_G(t)$. □

Theorem 8.22. *Let G be a finite, simple, exceptional or twisted group of Lie-type, defined over a field of even characteristic. If X is a G-conjugacy class of involutions, then $\mathcal{F}(G, X)$ is connected.*

Proof. First suppose that $q = 2$. In this case we can verify the result computationally, using MAGMA. For $G_2(2)'$, ${}^3D_4(2)$, $F_4(2)$, ${}^2F_4(2)'$, ${}^2F_4(q)$, $E_6(2)$ and ${}^2E_6(2)$

the complex character tables are known, so we may apply the method described in Chapter 5 for the sporadic simple groups. We can also check the case $G_2(2)$ using this method, in preparation for what follows.

For $E_7(2)$ and $E_8(2)$ we do not have access to the character tables. However, representations of both groups are stored on the online Atlas [1], where we are given matrices a, b such that $G = \langle a, b \rangle$. By using the command `Random` to find elements of G with even order, and then taking an appropriate power, we can find involutions from each conjugacy class of G, distinguishing them using fixed space dimension and Table 8.1. Now, for each representative involution $t \in G$, we use random conjugation to find elements $x_1, x_2, x_3, x_4 \in X = t^G$ such that tx_i has odd order for $i = 1, \ldots, 4$, $x_1^a = x_3$ and $x_2^b = x_4$. Hence $a, b \in \mathrm{Stab}_G(Y)$, and since $G = \langle a, b \rangle$ we have that $\mathcal{F}(G, X)$ is connected. Representatives for suitable elements to use in this process are available from the author on request.

Now suppose $G = G(2^r)$ where $r \geq 2$, and write $r = r_1 r_2 \cdots r_k$ as a product of primes. We proceed by induction on k. If $k = 1$ then by Lemma 8.20 we may choose $t \in X \cap H$, where $H \cong G(2)$. By the treatment of the cases above we have that $H \leq \mathrm{Stab}_G(Y)$. Clearly we also have $C_G(t) \leq \mathrm{Stab}_G(Y)$. But Lemma 8.21 implies that $C_G(t) \not\leq H$, and since r_1 is prime, by Theorem 6.9 H is a maximal subgroup of G, we deduce that $\langle H, C_G(t) \rangle = G$, and so $\mathcal{F}(G, X)$ is connected.

If $k \geq 2$, then let $H \leq G$ be such that $H \cong G(2^{r_1 \cdots r_{k-1}})$. Using induction, Lemmas 8.20 and 8.21 we again have that $\langle H, C_G(t) \rangle \leq \mathrm{Stab}_G(Y)$, and since r_k is prime the maximality of H yields $G = \mathrm{Stab}_G(Y)$, as required. $\square$

Chapter 9

Coprimality Graphs of Symmetric Groups

Thus far we have concentrated our study exclusively on local fusion graphs, where our vertex set consists of a conjugacy class of involutions. We now broaden our horizons, and consider coprimality graphs $\mathcal{C}_{p'}(G, X)$, where G is a symmetric group and X is a conjugacy class of elements of prime order p. Our aim is to find bounds on the diameter of $\mathcal{C}_{p'}(G, X)$. This turns out to be considerably more challenging than in the local fusion graph case. To determine whether or not $\mathcal{C}_{p'}(G, X)$ is connected, there is the following result.

Theorem 9.1 (Rowley)**.** *Suppose that $G = \mathrm{Sym}(n)$ and that x is an element of order p, p a prime. Let X be the G-conjugacy class of x. Then $\mathcal{C}_{p'}(G, X)$ is connected unless $n = 4$ and x has cycle type 2^2.*

Further to this are our results concerning the diameters of our coprimality graphs.

Theorem 9.2. *Suppose that $G = \mathrm{Sym}(n)$ and X is the G-conjugacy class of a p-cycle where p is an odd prime. Then $\mathrm{Diam}(\mathcal{C}_{p'}(G, X)) = 2$ unless $n = 3 = p$ when $\mathrm{Diam}(\mathcal{C}_{p'}(G, X)) = 1$.*

Theorem 9.3. *Suppose that $G = \mathrm{Sym}(n)$ and X is the G-conjugacy class of elements of cycle type p^r, where p is an odd prime. If $r < \sqrt{p}$, then $\mathrm{Diam}(\mathcal{C}_{p'}(G, X)) \leq 5$.*

Theorem 9.4. *Suppose that $G = \mathrm{Sym}(n)$ and X is the G-conjugacy class of elements of cycle type p^r, where $p \geq 5$ is prime. Let k be the least non-negative integer such that $r/2^k \leq \lfloor \sqrt{p} \rfloor$. Then* $\mathrm{Diam}(\mathcal{C}_{p'}(G, X)) \leq 5 + k$.

We begin by proving Theorem 9.2, as the proofs of Theorem 9.3 and Theorem 9.4 rely upon this result. As was the case when dealing with sporadic groups in Chapter 5, the class structure constants are of use to us. Suppose that $G = \mathrm{Sym}(n)$, where $n \geq 5$, and let X be the G-conjugacy class of t, an element of prime order p. Furthermore, suppose that $p = n$, $n-1$ or $n-2$. From our assumption on n, if $x \in X$ and $x \neq t$, then x lies outside $\Delta_1(t)$ if and only if $o(tx) = p$, so if and only if $tx \in X$ (note that tx must be an even permutation, so cannot be a product of a p-cycle and a transposition). If we can count the number of such elements, and show that it is not greater than $|X|/2$, then by Lemma 1.16 $\mathcal{C}_{p'}(G, X)$ will be connected, and $\mathrm{Diam}(\mathcal{C}_{p'}(G, X)) \leq 2$. By applying the formula for the class structure constants, we have an expression for this number, namely

$$\begin{aligned} |X - \Delta_1(t)| &= \frac{|X|^2}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \chi(t)\chi(t)\overline{\chi(t)}/\chi(1) \\ &= \frac{|G|}{|C_G(t)|^2} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(t)}{\chi(1)} |\chi(t)|^2. \end{aligned}$$

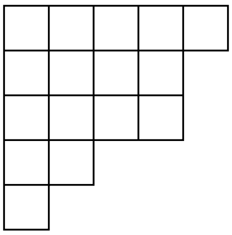
The study of these cases therefore reduce to the study of the character table of the symmetric group. Fortunately, an extensive theory exists on this topic. We briefly summarise the results which we require, and for a detailed treatment refer the reader to [58].

9.1 Representation Theory of the Symmetric Group

Let $n \in \mathbb{N}$. A *partition* of n is a sequence

$$\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$$

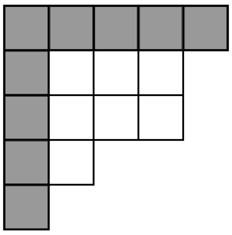
where the λ_i are weakly decreasing and $\sum_{i=1}^{k} \lambda_i = n$. The partitions of n are in one to one correspondence with the complex irreducible representations of the symmetric group $\mathrm{Sym}(n)$. To each partition λ we associate a *Young diagram* D_λ, consisting of n cells and k rows, left justified, with the length of row i equal to λ_i. For example, for the partition $(5, 4, 4, 2, 1)$ of 16, the corresponding Young diagram is shown below.



If (i, j) is a cell in the diagram D_λ of a partition λ, the *hook* $H_{i,j}$ is defined as

$$H_{i,j} = \{(i, j') : j' \geq j\} \cup \{(i', j) : i' \geq i\}.$$

We define the corresponding *hook length* as $h_{i,j} = |H_{i,j}|$. To illustrate, for our previous example, the hook $H_{1,1}$ is shaded, which has hook length $h_{1,1} = 9$.



We may now state the first of our required results, known as the 'hook formula'.

Theorem 9.5 (Frame, Robinson, Thrall)**.** *Let λ be a partition of a natural number n, with χ^λ the character afforded by the corresponding irreducible representation of* $\mathrm{Sym}(n)$*. Then*

$$\chi^\lambda(1) = \frac{n!}{\prod_{(i,j)\in D_\lambda} h_{i,j}}.$$

Again, we illustrate using our previous example. The length of each hook is displayed below.

9	7	5	4	1
7	5	3	2	
6	4	2	1	
3	1			
1				

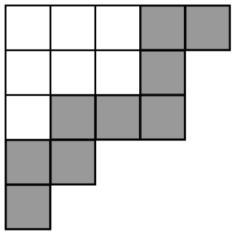
Now, the hook formula yields

$$\chi^{\lambda}(1) = \frac{16!}{9 \cdot 7^2 \cdot 6 \cdot 5^2 \cdot 4^2 \cdot 3^2 \cdot 2^2 \cdot 1^4} = 549120.$$

Let $H_{i,j}$ be a hook in the Young diagram associated with some partition λ. Then the *rim hook* $R_{i,j}$ is obtained by projecting $H_{i,j}$ along diagonals onto the lower-right boundary of our diagram. Note that $|R_{i,j}| = |H_{i,j}| = h_{i,j}$. The *leg length* of $R_{i,j}$ is defined as

$$ll(R_{i,j}) = (\text{number of rows of } R_{i,j}) - 1.$$

For our example, the rim hook $R_{1,1}$ is shown, for which $ll(R_{1,1}) = 4$.



Observe that if $h_{i,j} < n$, and we remove the rim hook $R_{i,j}$ from the diagram D_λ, what remains is a Young diagram associated with some partition of $n - h_{i,j}$. We denote this new diagram by $D_\lambda \setminus R_{i,j}$.

For a conjugacy class $\mathcal{K}$ of $\mathrm{Sym}(n)$, we can naturally associate a partition of n with $\mathcal{K}$ via the cycle type of elements of $\mathcal{K}$. We are now in a position to state the second of our required results, a combinatorial rule for calculating the values of irreducible characters of the symmetric group.

The Murnaghan-Nakayama Rule

Let λ be a partition of n, with corresponding irreducible character χ^λ of $\mathrm{Sym}(n)$. Let $\sigma \in \mathrm{Sym}(n)$ have cycle type with associated partition $\mu = (\mu_1, \mu_2, \ldots, \mu_r)$ of n. We generate a *branch* B, and a corresponding value $c_B \in \{-1, 0, 1\}$, by using the following iterative procedure.

Initially, set $c_0 = 1$ and $D_{\lambda_0} = D_\lambda$. For $k \geq 1$, the k-th step is as follows:

1. If $D_{\lambda_{k-1}}$ consists of zero cells, set $c_B = c_{k-1}$, and stop.

2. If possible, remove a rim hook R_k of length μ_k from $D_{\lambda_{k-1}}$, such that $D_{\lambda_{k-1}} \setminus R_k$ is a Young diagram, or consists of zero cells. If this is not possible, set $c_B = 0$, and stop.

3. Set $c_k = (-1)^{ll(R_k)} \cdot c_{k-1}$, and $D_{\lambda_k} = D_{\lambda_{k-1}} \setminus R_k$.

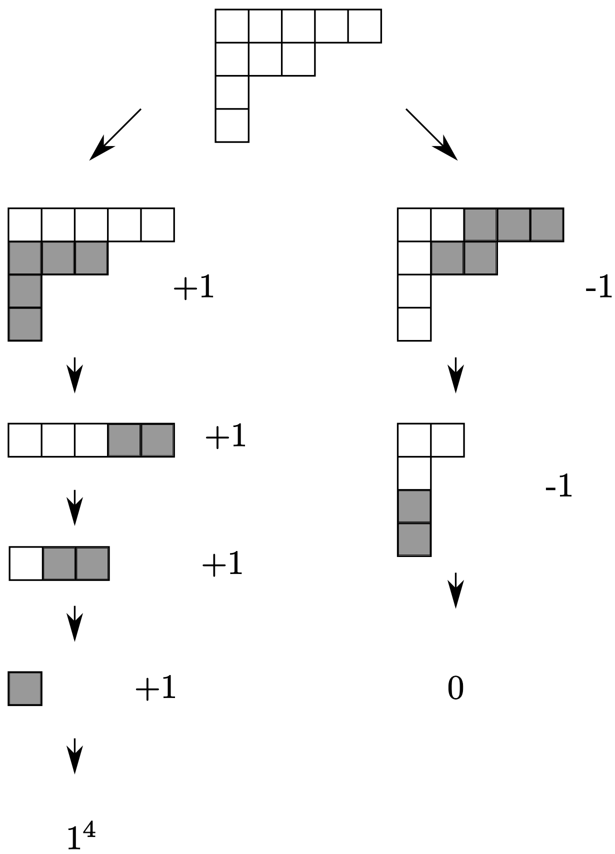
When applying this rule, at each step, different choices of rim hook removal yield distinct branches. The totality of these branches (those generated by all possible valid combinations of rim hook removals) can be considered to form a *tree* T associated with the pair (λ, μ). We have the following result.

Theorem 9.6 (Murnaghan-Nakayama)**.** *With the set-up as above, we have*

$$\chi^\lambda(\sigma) = \sum_B c_B,$$

where the sum runs over all distinct branches B of T.

We illustrate the Murnaghan-Nakayama rule with an example. Let $n = 10$, with partition $\lambda = (5, 3, 1, 1)$, and let $\sigma \in \mathrm{Sym}(n)$ have cycle type 5.2.2.1. The tree we generate is as follows:



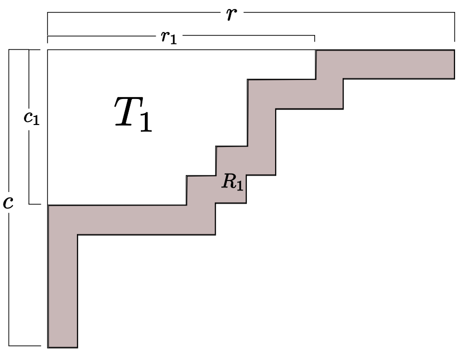
So for this example we have two branches to sum over, yielding $\chi^\lambda(\sigma) = 1 + 0 = 1$.

9.2 Applying Representation Theory

We now use the representation theory of the symmetric group to prove results about certain coprimality graphs. In particular, we examine the cases where $p = n, n-1$ or $n-2$. Firstly, we require some further results on Young diagrams.

Lemma 9.7. *Let T be a Young diagram consisting of n cells, and let $k > n/2$. Then there is at most one way of removing a rim hook of length k from T.*

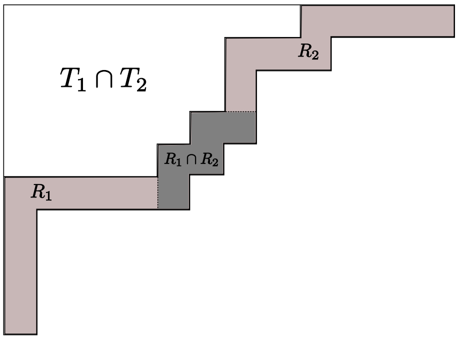
Proof. Suppose we have a way of removing a rim hook R_1 of length k from T. After removal, a diagram of $n-k$ cells remains, which we denote T_1. Let r and r_1 be the lengths of the top rows of T and T_1 respectively. Similarly, denote by c and c_1 the lengths of the first columns.



Note that since $k > n/2$, either $r > r_1$, $c > c_1$, or both. Firstly, suppose both hold. Then clearly R_1 is maximal in the sense that any other rim hook which can be removed from T is of length less than k. Thus R_1 is our only choice.

Suppose now that either $r = r_1$ or $c = c_1$. Since if necessary we may just reflect the diagram in the main diagonal, without loss of generality we may assume $c = c_1$. Let $H_{1,j}$ be the hook from which R_1 is projected, based at position $(1, j)$ in T. Suppose there exists another possible choice of rim hook, labelled R_2, with corresponding diagram T_2.

Any projection of a hook $H_{1,j-d}$, where $d \geq 1$, will have length greater than k, so is not suitable. Also, a projection of a hook $H_{i,j}$, where $i > 1$ and $j > 1$, will have length less than $n/2 < k$, again unsuitable. Thus R_2 must project from some position $(i, 1)$ where $i > 1$.



Note that R_1 and R_2 must intersect nontrivially, since otherwise

$$|T| \geq |R_1| + |R_2| = 2k > n,$$

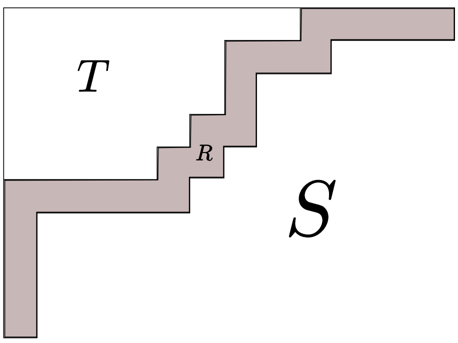
a contradiction. Since R_1 projects from $(1, j)$, and R_2 projects from $(i, 1)$, $R_1 \cap R_2$ must intersect in the empty set with both the first row and first column of T. Consequently we have $|T_1 \cap T_2| \geq |R_1 \cap R_2|$. Thus

$$|T| = |R_1 \cup R_2| + |T_1 \cap T_2| \geq |R_1 \cup R_2| + |R_1 \cap R_2| = 2k > n,$$

another contradiction. Therefore R_1 is the only suitable choice of rim hook. □

Lemma 9.8. *Let χ_S be the complex character of* $\mathrm{Sym}(n)$ *associated to a diagram S, and let χ_T be the complex character of* $\mathrm{Sym}(n-k)$ *associated to the diagram T, where T is obtained by removing a rim hook of length k from S, where $k > n/2$. Assume χ_S and χ_T are both nonlinear. Then $\chi_S(1) \geq 2\chi_T(1)$.*

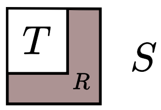
Proof. We use the Murnaghan-Nakayama rule to calculate $\chi_S(1)$. Denote by R the rim hook which we remove from S to obtain T.



Denote by r_T and r_S the lengths of the top rows of T and S repectively. Similarly denote by c_T and c_S the lengths of the first columns. As $k > n/2$, note that either $r_S > r_T$, $c_S > c_T$, or both. The first step in calculating $\chi_S(1)$ is to remove a single cell rim hook from S. Clearly it is possible to remove this cell from R.

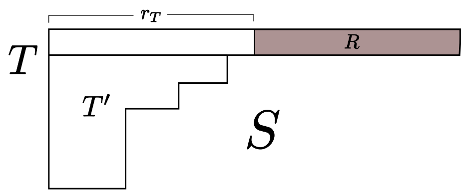
We now consider the following three cases: either $r_S \neq r_T + 1$ or $c_S \neq c_T + 1$ and R is not a single row (or column); both $r_S = r_T + 1$ and $c_S = c_T + 1$; or R consists of only a single row (or column). First, suppose that either $r_S \neq r_T + 1$ or $c_S \neq c_T + 1$, and that R does not consist only of a single row (or column). Then we have at least two choices of single cell rim hook removal from R. For each choice, we are able to continue to remove single cells from R until the diagram T remains. The value we calculate from this point onwards is $\chi_T(1)$. But now, the details of the Murnaghan-Nakayama rule yield $\chi_S(1) \geq 2\chi_T(1)$.

Suppose now that $r_S = r_T + 1$ and $c_S = c_T + 1$ (this situation can only occur when $n \leq 9$).



It is clear from the figure that after our first removal we have two choices of single cell removal. Arguing as above, we again have $\chi_S(1) \geq 2\chi_T(1)$.

Finally, suppose that R consists of only a single row (or column). Note that since χ_T and χ_S are both non-linear, T must have at least two rows (or columns).



In this case we use the hook formula, which yields

$$\chi_T(1) = \frac{(n-k)!}{\prod_{(i,j)\in T} h_{i,j}^T}$$

and

$$\chi_S(1) = \frac{n!}{\prod_{(i,j)\in S} h_{i,j}^S},$$

where $h^T_{i,j}$ denotes the length of the hook based at (i,j) in the diagram T, and $h^S_{i,j}$ the length of the hook based at (i,j) in the diagram S. By observing the position of the subdiagram T' in both T and S, we see that

$$\chi_T(1) = \frac{(n-k)(n-k-1)\cdots(|T'|+1)}{\prod_{(i,j)\in T\setminus T'} h^T_{i,j}} \cdot B$$

and

$$\chi_S(1) = \frac{n(n-1)\cdots(|T'|+1)}{\prod_{(i,j)\in S\setminus T'} h^S_{i,j}} \cdot B,$$

where

$$B = \frac{|T'|!}{\prod_{(i,j)\in T'} h^{T'}_{i,j}}.$$

We must therefore show that

$$\frac{n(n-1)\cdots(|T'|+1)}{\prod_{(i,j)\in S\setminus T'} h^S_{i,j}} \geq \frac{2\cdot(n-k)(n-k-1)\cdots(|T'|+1)}{\prod_{(i,j)\in T\setminus T'} h^T_{i,j}}.$$

Note that as $k > n/2$ and χ_T is non-linear, $r_T < k-1$. Hence we have

$$\begin{aligned} h^T_{1,r_T} &\geq h^S_{1,r_T+k}, \\ h^T_{1,r_T-1} &\geq h^S_{1,r_T+k-1}, \\ &\vdots \\ h^T_{1,1} &\geq h^S_{1,k+1}. \end{aligned}$$

Also

$$\begin{aligned} h^S_{1,1} &\leq n, \\ h^S_{1,2} &\leq n-2, \qquad \text{(as } \chi_T \text{ is non-linear)} \\ h^S_{1,3} &\leq n-3, \\ h^S_{1,4} &\leq n-4, \\ &\vdots \\ h^S_{1,k-1} &\leq n-k+1. \end{aligned}$$

Finally, note that $h^S_{1,k} = r_T + 1 \leq (n-1)/2$. Indeed,

$$n-1 \geq r_T + k > r_T + r_T + 1 = 2r_T + 1,$$

so $n-1 \geq 2r_T+2$. Hence we have

$$\frac{n(n-1)\cdots(|T'|+1)}{\prod_{(i,j)\in S\setminus T'} h_{i,j}^S} \geq \frac{2\cdot(n-k)(n-k-1)\cdots(|T'|+1)}{\prod_{(i,j)\in T\setminus T'} h_{i,j}^T},$$

as required. □

Lemma 9.9. *Let $G = \mathrm{Sym}(n)$, and let X be a conjugacy class of k-cycles in G, where $k > n/2$. Then for a non-linear complex irreducible character χ of G we have*

$$|\chi(x)| \leq \chi(1)/2$$

for all $x \in X$.

Proof. By the Murnaghan-Nakayama rule, the first step in calculating $\chi(x)$ is to remove a rim hook of length k (if possible) from the diagram T associated with χ. If this is not possible, then $\chi(x) = 0$, and the result clearly holds. Therefore suppose it is possible. Then by Lemma 9.7, there is only one way to do this.

If $k = n$, then clearly $\chi(x) = \pm 1$, and the result follows since χ is non-linear. So now suppose $k < n$. After removing our rim hook of length k, the Murnaghan-Nakayama rule tells us to remove single cell rim hooks from the remaining diagram T' in all possible ways. However, the hook formula also yields this value. Thus

$$\chi(x) = \pm\frac{(n-k)!}{\prod_{(i,j)\in T'} h_{i,j}^{T'}} = \pm\chi_{T'}(1)$$

where $\chi_{T'}$ is the character of $\mathrm{Sym}(n-k)$ associated with T'. But T' was obtained from T by removing a rim hook of length $k > n/2$. Hence Lemma 9.8 implies $\chi(1) \geq 2\chi_{T'}(1)$. Thus $|\chi(x)| \leq \chi(1)/2$. □

We are now in a position to apply our results to obtain information about our graphs in the cases when $p = n$, $n-1$ and $n-2$.

Theorem 9.10. *Let $G = \mathrm{Sym}(n)$, where $n \geq 5$, and let X be a conjugacy class of p-cycles in G, where $p = n$, $n-1$ or $n-2$. Then $\mathcal{C}_{p'}(G,X)$ is connected and* $\mathrm{Diam}(\mathcal{C}_{p'}(G,X)) = 2$.

Proof. When $n < 15$ we can check directly using MAGMA [18], so suppose $n \geq 15$. Let $t = (1, 2, \ldots, p)$ be our base point. As observed previously, since $p = n$, $n-1$ or $n-2$, $x \in X$ lies outside $\Delta_1(t)$ if and only if $o(tx) = p$, so if and only if $tx \in X$. The class structure constants yield the following:

$$\begin{aligned} |X - \Delta_1(t)| &= \frac{|X|^2}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \chi(t)\chi(t)\overline{\chi(t)}/\chi(1) \\ &= \frac{|G|}{|C_G(t)|^2} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(t)}{\chi(1)} |\chi(t)|^2. \end{aligned}$$

Since $G' \cong \mathrm{Alt}(n)$, we have $[G : G'] = 2$, so G has exactly two linear characters. Also, since p is odd, $\chi(t) = 1$ for both of these characters. Denote by $\mathrm{Irr}(G)^*$ the set of non-linear irreducible characters of G. Then

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(t)}{\chi(1)} |\chi(t)|^2 = 2 + \sum_{\chi \in \mathrm{Irr}(G)^*} \frac{\chi(t)}{\chi(1)} |\chi(t)|^2.$$

By Lemma 9.9, for non-linear $\chi \in \mathrm{Irr}(G)$ we have $|\chi(t)|/\chi(1) \leq 1/2$. Furthermore, as $n \geq 15$ we have $p \geq 13$, and there are at least 11 non-zero character values on X, and so at least 4 negative character values on X (this can be easily verified by considering possible Young diagrams and using the Murnaghan-Nakayama rule). Hence we may write

$$\begin{aligned} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(t)}{\chi(1)} |\chi(t)|^2 &\leq 2 + \frac{1}{2} \left(\sum_{\chi \in \mathrm{Irr}(G)^*} |\chi(t)|^2 - 4 \right) \\ &= \frac{1}{2} \sum_{\chi \in \mathrm{Irr}(G)^*} |\chi(t)|^2. \end{aligned}$$

Next, we apply column orthogonality, remembering that G has exactly two linear characters.

$$\begin{aligned} \frac{1}{2} \sum_{\chi \in \mathrm{Irr}(G)^*} |\chi(t)|^2 &= \frac{1}{2} \left(|C_G(t)| - 2 \right) \\ &= \frac{|C_G(t)|}{2} - 1 \\ &< \frac{|C_G(t)|}{2}. \end{aligned}$$

Therefore

$$|X - \Delta_1(t)| < \frac{|G|}{|C_G(t)|^2} \cdot \frac{|C_G(t)|}{2} = \frac{|X|}{2}.$$

By Lemma 1.16, the result follows. □

In certain cases we can go further, and obtain an exact expression for the size of the second disc.

Proposition 9.11. *Let $G = \mathrm{Sym}(p)$, where p is a prime, $p \geq 7$. Write $p = 2m+1$. Let X be the conjugacy class of p-cycles, with $t = (1, 2, \ldots, p)$. Then the number of elements $x \in X$ for which tx is a p-cycle is given by the following:*

$$|\Delta_2(t)| = \frac{2D}{p} - 1,$$

where

$$\begin{aligned} D &= (p-1)! - (p-2)! + (-1)^2 2!(p-3)! + (-1)^3 3!(p-4)! + \cdots \\ &\quad \cdots + (-1)^{m-1}(m-1)!(p-m)! + (-1)^m \frac{1}{2} m!(p-m-1)!. \end{aligned}$$

Proof. Notice that (under the present hypotheses) the number of elements $x \in X$ for which tx is a p-cycle is precisely $|\Delta_2(t)|$ in $\mathcal{C}_{p'}(G, X)$. From Theorem 9.10 we have that $\mathcal{C}_{p'}(G, X)$ is connected and has diameter 2, and that

$$|\Delta_2(t)| + 1 = \frac{|G|}{|C_G(t)|^2} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(t)}{\chi(1)} |\chi(t)|^2.$$

Furthermore, after a moment's consideration we deduce that $\chi(t) = \pm 1$ for exactly p irreducible characters (the 'L-shaped' diagrams, so those consisting of at most one row and one column), with the remainder yielding 0 on X. We use the hook formula to calculate $\chi(1)$ for each of these contributing characters.

Starting from the diagram of one single row, and adding one cell to the first column (and removing one cell from the top row) each time, the hook formula yields the following character degrees:

$$1, p-1, \frac{(p-1)(p-2)}{2}, \frac{(p-1)(p-2)(p-3)}{3 \cdot 2}, \ldots, \frac{(p-1)\cdots(p-r)}{r!}, \ldots,$$

where the sequence is symmetric around the $(m+1)$-th term. We also note that diagrams with an odd number of rows yield a character value of 1, while those with an even number of rows yield -1. Putting all this information together, along with the observations that $|G| = p!$ and $|C_G(t)| = p$, gives us the desired expression for $|\Delta_2(t)|$. □

9.3 Products of Permutations

Our aim in this section is to analyse in more detail what happens when we multiply two permutations. In particular, we are interested in the consequences of minor adjustments in the cycles of the permutations. First, however, we deal with the simple case of disjoint p-cycles.

Proposition 9.12. *Suppose $G = \mathrm{Sym}(n)$, and t is a p-cycle where $p \geq 3$ is prime. Let $X = t^G$. If $x \in X$ is disjoint from t, then there exists $y \in X$ with $d(t, y) = d(y, x) = 1$ in $\mathcal{C}_{p'}(G, X)$.*

Proof. Without loss of generality we assume

$$t = (1, 2, \ldots, p)$$

and

$$x = (p + 1, p + 2, \ldots, 2p).$$

Take

$$y = (1, 2, \ldots, p - 2, p + 1, p + 2) \in X.$$

Then

$$ty = (1, 3, 5, \ldots, p - 2, p - 1, p, 2, 4, 6, \ldots, p - 3, p + 1, p + 2)$$

and

$$yx = (1, 2, \ldots, p - 2, p + 2)(p - 1)(p)(p + 1, p + 3, p + 4, \ldots, 2p).$$

Hence ty has order $p + 2$ and yx has order $p - 1$, so proving the result. □

Suppose $x \in \mathrm{Sym}(\Omega)$, and that $\alpha \in \Omega$. We recall that $\mathcal{O}_x(\alpha)$ denotes the $\langle x \rangle$-orbit which contains α. The following lemma is the key to proving Theorems 9.2, 9.3 and 9.4.

Lemma 9.13. *Let $G = \mathrm{Sym}(n)$, with $x, y \in G$ distinct elements of order at least 3. Denote by Ω the set upon which G acts naturally. Suppose there exist distinct $\alpha, \beta, \gamma \in \Omega$ such that $\beta, \gamma \in \mathcal{O}_y(\alpha)$ but $\beta, \gamma \notin \mathcal{O}_{xy}(\alpha)$.*

(i) If $\gamma \notin \mathcal{O}_{xy}(\beta)$, then there exists $z \in G$, where $\langle z \rangle$ has the same orbits on Ω as $\langle y \rangle$, such that $|\mathcal{O}_{xz}(\alpha)| = |\mathcal{O}_{xy}(\alpha)| + |\mathcal{O}_{xy}(\beta)| + |\mathcal{O}_{xy}(\gamma)|$.

(ii) If $\gamma \in \mathcal{O}_{xy}(\beta)$, then there exists $z \in G$, where $\langle z \rangle$ has the same orbits on Ω as $\langle y \rangle$, such that $|\mathcal{O}_{xz}(\alpha)| = |\mathcal{O}_{xy}(\alpha)| + c$ and $|\mathcal{O}_{xz}(\gamma)| = |\mathcal{O}_{xy}(\gamma)| - c$, where $c \geq 1$.

(iii) If $|\mathcal{O}_y(\alpha) \cap (\mathcal{O}_{xy}(\alpha) \cup \mathcal{O}_{xy}(\beta))| = m$, where $m \geq 4$, then there exist

$$M = (m-1)(m-2)/2$$

distinct elements $z_1, \ldots, z_M$, which can be created by an application of (ii), where for $1 \leq i \leq M$ each $\langle z_i \rangle$ has the same orbits on Ω as $\langle y \rangle$. Moreover, there exist natural numbers $c_1 < c_2 < \cdots < c_{m-2}$, along with $c_0 := 0$, such that

$$\{|\mathcal{O}_{xz_k}(\alpha)| : 1 \leq k \leq M\} = \{c_i - c_j : 0 \leq j < i \leq m-2\},$$

and this set has cardinality at least $m-2$.

Proof. Without loss of generality we may suppose y contains the cycle

$$\sigma = (\delta_1, \alpha, \delta_3, \ldots, \delta_k, \beta, \delta_{k+2}, \ldots, \delta_l, \gamma, \delta_{l+2}, \ldots).$$

Firstly, suppose that β and γ lie in separate orbits of $\langle xy \rangle$. Then xy contains the following cycles:

$$(\delta_1^{x^{-1}}, \alpha, \ldots)(\delta_k^{x^{-1}}, \beta, \ldots)(\delta_l^{x^{-1}}, \gamma, \ldots),$$

where $\delta_1^{x^{-1}}$ denotes the inverse image of δ_1 under x, $\delta_k^{x^{-1}}$ the inverse image of δ_k under x and $\delta_l^{x^{-1}}$ the inverse image of δ_l under x. Now let

$$\overline{\sigma} = (\delta_1, \beta, \delta_{k+2}, \ldots, \delta_l, \alpha, \delta_3, \ldots, \delta_k, \gamma, \delta_{l+2}, \ldots),$$

and let z be equal to y but with the cycle σ replaced by $\overline{\sigma}$. We have changed the images of precisely three elements in $\mathrm{supp}(\sigma)$, namely δ_1, δ_k and δ_l, and so in the product xz only the images of $\delta_1^{x^{-1}}$, $\delta_k^{x^{-1}}$ and $\delta_l^{x^{-1}}$ have been changed from those in xy. Therefore xz contains the cycle

$$(\delta_1^{x^{-1}}, \beta, \ldots, \delta_k^{x^{-1}}, \gamma, \ldots, \delta_l^{x^{-1}}, \alpha, \ldots),$$

and we have $|\mathcal{O}_{xz}(\alpha)| = |\mathcal{O}_{xy}(\alpha)| + |\mathcal{O}_{xy}(\beta)| + |\mathcal{O}_{xy}(\gamma)|$. This proves statement (i).

Now suppose that $\gamma \in \mathcal{O}_{xy}(\beta)$, so we may assume xy contains the cycles

$$(\delta_1^{x^{-1}}, \alpha, \ldots)(\delta_k^{x^{-1}}, \beta, \ldots, \delta_l^{x^{-1}}, \gamma, \ldots).$$

Once more we set

$$\overline{\sigma} = (\delta_1, \beta, \delta_{k+2}, \ldots, \delta_l, \alpha, \delta_3, \ldots, \delta_k, \gamma, \delta_{l+2}, \ldots),$$

and let z be equal to y but with the cycle σ replaced by $\overline{\sigma}$. As previously, in the product xz only the images of $\delta_1^{x^{-1}}$, $\delta_k^{x^{-1}}$ and $\delta_l^{x^{-1}}$ have been changed from those in xy. Hence xz contains the cycle

$$(\delta_1^{x^{-1}}, \beta, \ldots, \delta_l^{x^{-1}}, \alpha, \ldots),$$

and so $|\mathcal{O}_{xz}(\alpha)| = |\mathcal{O}_{xy}(\alpha)| + |\beta \cdots \delta_l^{x^{-1}}|_{xy}$, where $|\beta \cdots \delta_l^{x^{-1}}|_{xy}$ denotes the distance between β and $\delta_l^{x^{-1}}$ in the relevant cycle of xy (reading inclusively from left to right). As a consequence, we have that $|\mathcal{O}_{xz}(\gamma)| = |\mathcal{O}_{xy}(\gamma)| - |\beta \cdots \delta_l^{x^{-1}}|_{xy}$. This proves statement (ii).

Now let $|\mathcal{O}_y(\alpha) \cap (\mathcal{O}_{xy}(\alpha) \cup \mathcal{O}_{xy}(\beta))| = m$, where $m \geq 4$, and suppose without loss of generality that β is the first element of $\mathcal{O}_{xy}(\beta)$ which we encounter when reading from left to right in the cycle σ, starting at α. If there exists $\mu_1 \in \mathcal{O}_y(\beta)$ such that $\mu_1 \neq \alpha$ but $\mu_1 \in \mathcal{O}_{xy}(\alpha)$, we may apply (ii) to find an element $y_1 \in G$ such that $|\mathcal{O}_{xy_1}(\beta)| > |\mathcal{O}_{xy}(\beta)|$ and $\alpha \notin \mathcal{O}_{xy_1}(\beta)$ (here β is playing the role of α in the application of (ii)). Now, if there exists $\mu_2 \in \mathcal{O}_{y_1}(\beta)$ such that $\mu_2 \neq \alpha$ but $\mu_2 \in \mathcal{O}_{xy_1}(\alpha)$, we may apply (ii) again to find y_2 such that $|\mathcal{O}_{xy_2}(\beta)| > |\mathcal{O}_{xy_1}(\beta)|$ and $\alpha \notin \mathcal{O}_{xy_2}(\beta)$. Continuing in this way, we eventually find an element y_s such that the only element of $\mathcal{O}_{y_{s-1}}(\beta) \cap (\mathcal{O}_{xy_{s-1}}(\alpha) \cup \mathcal{O}_{xy_{s-1}}(\beta))$ which lies outside $\mathcal{O}_{xy_s}(\beta)$ is α.

There are now $m-1$ elements of $\mathcal{O}_{xy_s}(\beta)$ which also lie in $\mathcal{O}_{y_s}(\alpha)$. We wish to apply (ii) once more, with different choices for β and γ, which we label β' and γ'. We have $m-2$ choices of element β' to play the role of β in the application of (ii). After choosing a β', the only requirement for choosing an element $\gamma' \in \mathcal{O}_{xy_s}(\beta')$ is that γ' lies between β' and α in the relevant cycle of y_s, when we read from left to right starting at β'. So for the first possible β' (reading from left to right in y_s starting at α), there are $m-2$ choices for γ'. For the second possible β' there are $m-3$ choices for γ', and so on. Therefore the total number of choices M we have is

$$M = (m-2) + (m-3) + \cdots + 2 + 1 = (m-1)(m-2)/2,$$

which leads to the elements $z_1, \ldots, z_M$ as in statement (iii). Moreover, after fixing a β', each susequent choice of γ' leads to a different value of c in (ii). As noted, we had $m-2$ choices for γ' when β' was our first possible choice. Let $c_1, \ldots, c_{m-2}$ be the values of c arising from these choices, labelled so that $c_j < c_i$ if $j < i$. Suppose xy_s contains the cycle

$$(\beta_1, \ldots, \delta_{\gamma_j}^{x^{-1}}, \gamma_j, \ldots, \delta_{\gamma_i}^{x^{-1}}, \gamma_i, \ldots),$$

and that $c_i = |\beta_1 \cdots \delta_{\gamma_i}^{x^{-1}}|_{xy_s}$ and $c_j = |\beta_1 \cdots \delta_{\gamma_j}^{x^{-1}}|_{xy_s}$. Then if we choose $\beta' = \gamma_j$ and $\gamma' = \gamma_i$ when applying (ii), we get

$$c = |\gamma_j \cdots \delta_{\gamma_i}^{x^{-1}}|_{xy_s} = |\beta_1 \cdots \delta_{\gamma_i}^{x^{-1}}|_{xy_s} - |\beta_1 \cdots \delta_{\gamma_j}^{x^{-1}}|_{xy_s} = c_i - c_j.$$

As every possible value of c must arise in this way, we see that the penultimate statement in (iii) holds. The final statement follows since $c_1, \ldots, c_{m-2}$ are all distinct. This completes the proof. $\square$

Let us illustrate Lemma 9.13 with a brief example. Suppose $G = \mathrm{Sym}(16)$,

$$x = (1, 9, 8, 14, 15, 4, 5)(2, 3, 6, 7, 10, 11, 16)$$

and

$$y = \lambda\sigma = (1, 2, 3, 4, 5, 6, 7)(8, 9, 10, 11, 12, 13, 14).$$

Then

$$xy = (1, 10, 12, 13, 14, 15, 5, 2, 4, 6)(3, 7, 11, 16)(8)(9).$$

Let $\alpha = 8$ and $\beta = 10$. Then

$$\mathcal{O}_y(8) \cap (\mathcal{O}_{xy}(8) \cup \mathcal{O}_{xy}(10)) = \{8, 10, 12, 13, 14\},$$

and (iii) tells us there exist $4 \cdot 3/2 = 6$ distinct elements $z_1, \dots, z_6$, where for each i the orbits of $\langle z_i \rangle$ are the same as those of $\langle y \rangle$, and that $\{|\mathcal{O}_{xz_i}(8)| : 1 \leq i \leq 6\}$ has cardinality at least $5 - 2 = 3$. Explicitly, we apply (ii) by adjusting the cycle σ of y to the following:

$$\begin{aligned}
\sigma_1 &= (10, 11, 8, 9, 12, 13, 14) \\
\sigma_2 &= (10, 11, 12, 8, 9, 13, 14) \\
\sigma_3 &= (10, 11, 12, 13, 8, 9, 14) \\
\sigma_4 &= (12, 8, 9, 10, 11, 13, 14) \\
\sigma_5 &= (12, 13, 8, 9, 10, 11, 14) \\
\sigma_6 &= (13, 8, 9, 10, 11, 12, 14).
\end{aligned}$$

Setting $z_i = \lambda \sigma_i$, for $1 \leq i \leq 6$, we have

$$\begin{aligned}
xz_1 &= (1, 12, 13, 14, 15, 5, 2, 4, 6)(3, 7, 11, 16)(8, 10)(9) \\
xz_2 &= (1, 13, 14, 15, 5, 2, 4, 6)(3, 7, 11, 16)(8, 10, 12)(9) \\
xz_3 &= (1, 14, 15, 5, 2, 4, 6)(3, 7, 11, 16)(8, 10, 12, 13)(9) \\
xz_4 &= (1, 10, 13, 14, 15, 5, 2, 4, 6)(3, 7, 11, 16)(8, 12)(9) \\
xz_5 &= (1, 10, 14, 15, 5, 2, 4, 6)(3, 7, 11, 16)(8, 12, 13)(9) \\
xz_6 &= (1, 10, 12, 14, 15, 5, 2, 4, 6)(3, 7, 11, 16)(8, 13)(9),
\end{aligned}$$

and we see that $\{|\mathcal{O}_{xz_i}(8)| : 1 \leq i \leq 6\} = \{1, 2, 3\}$.

Notice that in Lemma 9.13, the elements x and y need not be G-conjugate. Also, the proof can be easily modified to give a corresponding result regarding the adjustment of the orbits of $\langle x \rangle$. We are now in a position to deal with the case of single p-cycles.

Proof of Theorem 9.2. When $p = 3$ the result is clear, so assume $p \geq 5$. Let $t = (1, 2, \dots, p)$ be our base point, and let $x \in X$. Suppose that t and x are disjoint cycles. Then by Proposition 9.12, $d(t, x) \leq 2$. So we may assume $|\mathrm{supp}(t) \cup \mathrm{supp}(x)| < 2p$.

Write $y = x^{-1}$. Clearly y is adjacent to x in $\mathcal{C}_{p'}(G, X)$, but suppose t and y are not adjacent. Then we must have $ty = \sigma\mu$, where σ is a p-cycle disjoint from μ, a product of cycles of length less than p.

Suppose we have $\mathrm{supp}(t) = \mathrm{supp}(\sigma)$. Then we claim that $\mathrm{supp}(t) = \mathrm{supp}(y)$. Indeed, suppose not. Then since $\mathrm{supp}(y) = \mathrm{supp}(x^{-1}) = \mathrm{supp}(x)$, and $\mathrm{supp}(x) \cap \mathrm{supp}(t) \neq \emptyset$, there exists $\alpha \in \mathrm{supp}(y)$ such that $\alpha \notin \mathrm{supp}(t)$ but $\alpha^y \in \mathrm{supp}(t)$. Then $\alpha^{ty} = \alpha^y \in \mathrm{supp}(t) = \mathrm{supp}(\sigma)$, and since σ and μ are disjoint, this implies that α^{ty} is fixed by μ. We therefore have

$$\alpha = (\alpha^{ty})^{y^{-1}t^{-1}} = (\alpha^{ty})^{\mu^{-1}\sigma^{-1}} = (\alpha^{ty})^{\sigma^{-1}},$$

and hence $\alpha \in \mathrm{supp}(\sigma) = \mathrm{supp}(t)$, a contradiction, and the claim holds. Now Theorem 9.10 tells us that $d(t, x) \leq 2$.

So let $\beta \in \mathrm{supp}(y) \cap \mathrm{supp}(\sigma)$. Suppose there exist distinct $\gamma, \delta \in \mathrm{supp}(y)$ such that $\gamma, \delta \notin \mathrm{supp}(\sigma)$. Then we may apply Lemma 9.13(i) or (ii) to obtain $z \in X$ such that tz contains a cycle of length greater than p. Hence t and z are adjacent in $\mathcal{C}_{p'}(G, X)$. But $\langle z \rangle$ and $\langle x \rangle$ have the same orbits, and at least one element of the p-cycle of x is fixed by zx (since $x = y^{-1}$, and z was obtained from y by changing the images of at most three points). Hence z is also adjacent to x. Thus $d(t, x) \leq 2$ in this case.

Now suppose $\gamma \in \mathrm{supp}(y)$ is the only such point for which $\gamma \notin \mathrm{supp}(\sigma)$. Then we may apply Lemma 9.13 to obtain z such that $|\mathcal{O}_{tz}(\gamma)| > |\mathcal{O}_{ty}(\gamma)|$. Furthermore, by Lemma 9.13(iii) we have enough freedom of choice in choosing z to ensure that $|\mathcal{O}_{tz}(\gamma)| \neq p$. Hence t and z are adjacent, as are z and x. Therefore $d(t, x) \leq 2$ in this final case, and the proof is complete. □

Corollary 9.14. *Let $G = \mathrm{Sym}(n)$, where $n \geq 4$, with X the conjugacy class of a p-cycle, where $p \geq 3$ is prime. Suppose $t, x \in X$ are adjacent in $\mathcal{C}_{p'}(G, X)$. Then there exists $z \in X$ such that $d(t, z) = 1$ and $d(z, x) = 1$.*

Proof. Set $y = x^{-1}$. If y is adjacent to t then clearly we may let $z = y$. Otherwise we may argue as in the proof of Theorem 9.2 to find a suitable z, by adjusting y using Lemma 9.13. □

When addressing the case of products of pairwise disjoint p-cycles, we wish to decompose elements into pieces which are in some sense minimal, and thus easier to work with. This motivates what follows.

Definition 9.15. Let $G = \mathrm{Sym}(n)$, with $x, y \in G$ elements of order of prime order p, not necessarily G-conjugate. Write $x = x_1 x_2 \cdots x_r$ and $y = y_1 y_2 \cdots y_s$ as products of pairwise disjoint p-cycles, and denote by A the set of non-trivial orbits of $\langle x \rangle$ and $\langle y \rangle$. We say the pair (x, y) is *disentangled* if we can write $A = B \cup C$, where B and C are nonempty subsets of A such that

$$\left(\bigcup_{b \in B} b \right) \cap \left(\bigcup_{c \in C} c \right) = \emptyset.$$

If this is not possible we say (x, y) is *tangled*.

If we allow the 'empty permutation', which we denote by $(\emptyset)$, then for every pair (x, y) there exists a decomposition $x = x^{(1)} \cdots x^{(k)}$, $y = y^{(1)} \cdots y^{(k)}$ such that each pair $(x^{(i)}, y^{(i)})$ is tangled.

To illustrate the above we give some examples. Suppose that $G = \mathrm{Sym}(30)$, and let

$$x = (1, 2, 3, 4, 5)(6, 7, 8, 9, 10)(11, 12, 13, 14, 15)(16, 17, 18, 19, 20)$$

and

$$y = (1, 3, 6, 8, 21)(2, 9, 10, 23, 28)(11, 22, 12, 14, 16)(18, 29, 19, 26, 27).$$

Then (x, y) is disentangled, with decomposition

i	$x^{(i)}$	$y^{(i)}$
1	$(1, 2, 3, 4, 5)(6, 7, 8, 9, 10)$	$(1, 3, 6, 8, 21)(2, 9, 10, 23, 28)$
2	$(11, 12, 13, 14, 15)(16, 17, 18, 19, 20)$	$(11, 22, 13, 14, 16)(18, 29, 19, 26, 27)$

Now let

$$y = (1, 7, 4, 12, 15)(26, 28, 22, 30, 29).$$

Then (x, y) is again disentangled, with decomposition

i	$x^{(i)}$	$y^{(i)}$
1	$(1,2,3,4,5)(6,7,8,9,10)(11,12,13,14,15)$	$(1,7,4,12,15)$
2	$(16,17,18,19,20)$	$(\emptyset)$
3	$(\emptyset)$	$(26,28,22,30,29)$

Lemma 9.16. *Let $G = \mathrm{Sym}(\Omega)$, and let $x, y \in G$ be elements of order $p \geq 3$ such that (x, y) is tangled. Let $|\mathrm{supp}(x) \cup \mathrm{supp}(y)| = m$, and suppose that xy is not an m-cycle. Then for any cycle σ in the product xy, we may find a cycle ρ of either x or y with $\alpha, \beta \in \mathrm{supp}(\rho)$ such that $\alpha \in \mathrm{supp}(\sigma)$ but $\beta \notin \mathrm{supp}(\sigma)$.*

Proof. First we write x and y as products of pairwise disjoint cycles thus $x = x_1x_2 \dots x_s$ and $y = y_1y_2 \dots y_r$. For a contradiction suppose the result does not hold for some cycle σ of xy. Then if $\mathcal{O}$ is any orbit of $\langle x \rangle$ or $\langle y \rangle$, then either $\mathcal{O}$ is disjoint from $\mathrm{supp}(\sigma)$, or $\mathcal{O} \subseteq \mathrm{supp}(\sigma)$. Thus if A is the set of orbits of $\langle x \rangle$ and $\langle y \rangle$, then we may write $A = B \cup C$, where B is the set of orbits which lie in $\mathrm{supp}(\sigma)$ and $C = A \setminus B$. Clearly B is nonempty and, since xy is not an m-cycle, C must also be nonempty. Since by the above observation we have

$$\left(\bigcup_{b \in B} b\right) \cap \left(\bigcup_{c \in C} c\right) = \emptyset,$$

this implies the pair (x, y) is disentangled, which is the desired contradiction. □

9.4 The proof of Theorems 9.3 and 9.4

We now begin our attack on Theorem 9.3 and Theorem 9.4, and work under the following hypothesis:

Hyposthesis 9.17. Let $G = \mathrm{Sym}(n)$, with $x, y \in G$ such that $x = x_1x_2 \dots x_r$ and $y = y_1y_2 \dots y_s$ are products of pairwise disjoint p-cycles, where $p \geq 7$ is an odd prime. Furthermore, suppose that (x, y) is tangled, and that $r, s < \sqrt{p}$.

Lemma 9.18. *Suppose Hypothesis 9.17 holds, and additionally that $|\mathrm{supp}(x) \cup \mathrm{supp}(y)| = kp$ for some $k \in \mathbb{N}$, and that xy is a kp-cycle. Then there exist elements $x' \in x^G$,*

$y' \in y^G$ such $\langle x \rangle$ and $\langle x' \rangle$ have the same orbits on Ω, $\langle y \rangle$ and $\langle y' \rangle$ have the same orbits on Ω, and the order of the product $x'y'$ is coprime to p.

Proof. We first show that since $r, s < \sqrt{p}$, (x, y) is tangled and $|\text{supp}(x) \cup \text{supp}(y)| = kp$, there must exist cycles λ_x, λ_y, of x and y respectively, with $|\text{supp}(\lambda_x) \cap \text{supp}(\lambda_y)| \geq 2$. For suppose this is not the case. Then

$$|\text{supp}(x) \cup \text{supp}(y)| \geq rp + sp - sr > (r+s)p - \sqrt{p} \cdot \sqrt{p} = (r+s-1)p.$$

On the other hand, again since (x, y) is tangled, we have that

$$|\text{supp}(x) \cup \text{supp}(y)| < (r+s)p.$$

However, by assumption, $|\text{supp}(x) \cup \text{supp}(y)|$ is a multiple of p, so this is a contradiction. Therefore we may choose $\alpha, \beta \in \text{supp}(\lambda_x) \cap \text{supp}(\lambda_y)$ with $\alpha \neq \beta$. We may write

$$\lambda_x = (\delta_1, \alpha, \delta_3, \ldots, \delta, \beta, \delta_{k+2}, \ldots).$$

Then we construct an element $x' \in x^G$, containing a cycle $\lambda_{x'}$, by adjusting the position of β in the cycle λ_x so that $\beta = \alpha^{\lambda_{x'}}$ (if this is already the case, we set $x' = x$). So

$$\lambda_{x'} = (\delta_1, \alpha, \beta, \delta_3, \ldots, \delta, \delta_{k+2}, \ldots).$$

We now show that

(3.1) when considered as an element of $\text{Sym}(\text{supp}(x) \cup \text{supp}(y))$, $x'y$ is either a single cycle or a product of exactly three cycles.

Firstly, note that if $x = x'$, then $x'y = xy$ is already a single kp-cycle, so assume that this is not the case. Then we have changed the image under λ_x of exactly three elements, namely α, β and δ. So all but these three elements in $\text{supp}(x'y)$ will have the same image under $x'y$ as under xy. In view of this, $x'y$ cannot be a product of more than three cycles. Suppose $\alpha^{xy} = \gamma_1$, $\beta^{xy} = \gamma_2$ and $\delta^{xy} = \gamma_3$. We can therefore write either

(3.1.1) $xy = (\alpha, \gamma_1, \ldots, \beta, \gamma_2, \ldots, \delta, \gamma_3, \ldots)$, or

(3.1.2) $xy = (\alpha, \gamma_1, \ldots, \delta, \gamma_3, \ldots, \beta, \gamma_2, \ldots)$.

(Note that it might be the case that $\{\alpha, \beta, \delta\} \cap \{\gamma_1, \gamma_2, \gamma_3\} \neq \emptyset$).

Since in both (3.1.1) and (3.1.2) we have $\delta^x = \beta$ and $\delta^{xy} = \gamma_3$, it must be that $\beta^y = \gamma_3$. Now, as $\alpha^{x'} = \beta$, we deduce that $\alpha^{x'y} = \gamma_3$. Consequently, we must have $\beta^{x'y} = \gamma_1$ and $\delta^{x'y} = \gamma_2$. Hence if (3.1.1) holds we have

$$x'y = (\alpha, \gamma_3, \ldots)(\delta, \gamma_2, \ldots)(\beta, \gamma_1, \ldots).$$

On the other hand, if xy is as in (3.1.2), we see that

$$x'y = (\alpha, \gamma_2, \ldots, \beta, \gamma_1, \ldots, \delta, \gamma_3, \ldots).$$

Thus (3.1) holds.

Now we construct an element $y' \in y^G$ by adjusting the position of β in the cycle λ_y so that $\alpha = \beta^{\lambda_{y'}}$. If this is already the case, we set $y' = y$ (note that if we set $x = x'$ above, then it cannot be the case that $y = y'$, since this would imply that α and β are fixed points of xy, which contradicts their lying in the kp-cycle of xy). We may write

$$\lambda_y = (\epsilon_1, \alpha, \epsilon_3, \ldots, \epsilon_l, \beta, \epsilon, \ldots)$$

and

$$\lambda_{y'} = (\epsilon_1, \beta, \alpha, \epsilon_3, \ldots, \epsilon_l, \epsilon, \ldots).$$

Next, we show that

(3.2) when considered as an element of $\mathrm{Sym}(\mathrm{supp}(x) \cup \mathrm{supp}(y))$, $x'y'$ is a product of exactly three cycles.

If $x'y$ is a single cycle, then a similar argument to that above shows that $x'y'$ is either a single cycle, or a product of exactly three cycles. But α is fixed by $x'y'$, so $x'y'$ cannot be a single cycle, and hence the result holds in this case. We may therefore assume that $x'y$ is a product of exactly three cycles.

In our rearrangement of λ_y we have changed the preimage under λ_y of exactly three elements, which are α, β and ϵ. Suppose that $\zeta_1^{x'y} = \alpha$, $\zeta_2^{x'y} = \beta$ and $\zeta_3^{x'y} = \epsilon$. We may write

$$x'y = (\zeta_1, \alpha, \gamma_3, \ldots)(\delta, \gamma_2, \ldots)(\zeta_2, \beta, \gamma_1, \ldots).$$

As a consequence of our rearrangement, the images of ζ_1, ζ_2, and ζ_3, are also changed under $x'y'$. As $\zeta_3^{x'y} = \epsilon$, and $\beta^y = \epsilon$, we must have that $\zeta_3^{x'} = \beta$. Since $\beta^{y'} = \alpha$ we have that $\zeta_3^{x'y'} = \alpha$, but α is fixed by $x'y'$, so it must be that $\zeta_3 = \alpha$. Consequently, $\epsilon = \gamma_3$, $\zeta_1^{x'y'} = \beta$ and $\zeta_2^{x'y'} = \epsilon$. Since only three elements of $\operatorname{supp}(x'y)$ have different images under $x'y'$ than under $x'y$, we deduce that

$$x'y' = (\alpha)(\zeta_1, \beta, \gamma_1, \ldots, \zeta_2, \epsilon, \ldots)(\delta, \gamma_2, \ldots).$$

This proves (3.2).

Thus, when considered as an element of $\operatorname{Sym}(\operatorname{supp}(x) \cup \operatorname{supp}(y))$, $x'y'$ is a product of exactly three cycles, one of which is a 1-cycle. If p does not divide the length of either of the other cycles, then x' and y' satisfy the conclusions of the lemma. So suppose σ_{wp} is a cycle of $x'y'$ of length wp where $1 \leq w < k$, and let ρ be the remaining non-trivial cycle of $x'y'$. Note that since $|\operatorname{supp}(x) \cup \operatorname{supp}(y)| = kp$, this means that p cannot divide the length of the cycle ρ. Since (x, y), and hence (x', y'), is tangled, and $x'y'$ is not a kp-cycle, we may apply Lemma 9.16 to see that there exists some cycle λ of either x' or y' with $\mu, \nu \in \operatorname{supp}(\lambda)$ such that $\mu \in \operatorname{supp}(\sigma_{wp})$ but $\nu \notin \operatorname{supp}(\sigma_{wp})$.

Without loss of generality suppose λ is a cycle of y', and suppose we may choose ν so that $\nu \neq \alpha$. Then since $\mathcal{O}_{x'y'}(\mu) \cup \mathcal{O}_{x'y'}(\nu)$ covers all of $\operatorname{supp}(x) \cup \operatorname{supp}(y)$ except α, and $\operatorname{supp}(y') = \operatorname{supp}(y)$, we have

$$|\mathcal{O}_{y'}(\mu) \cap (\mathcal{O}_{x'y'}(\mu) \cup \mathcal{O}_{x'y'}(\nu))| \geq p - 1.$$

Now apply Lemma 9.13(ii) to construct an element y'' such that $|\mathcal{O}_{x'y''}(\mu)| > |\mathcal{O}_{x'y'}(\mu)|$. This will ensure coprimality, unless the element y'' which we construct yields $x'y''$ with

$|\mathcal{O}_{x'y''}(\mu)| = up$ or $|\mathcal{O}_{x'y''}(\nu')| = vp$, where $1 \leq u, v \leq k-1$, and ν' lies in the other cycle of $x'y'$ whose length has been adjusted by applying Lemma 9.13(ii). Since, by assumption, we are already in the situation where $|\mathcal{O}_{x'y'}(\mu)| = wp$, and applying Lemma 9.13 adjusts the length of this orbit, we deduce that there are $2k-3$ possible problem cases.

By Lemma 9.13(iii) we have at least $p-3$ choices of y'' which yield distinct values of c so that $|\mathcal{O}_{x'y''}(\mu)| = |\mathcal{O}_{x'y'}(\mu)| + c$. Since (x, y) is tangled (so x and y are not disjoint), $2k - 3 \leq 2(r + s - 1) - 3$. When $p \geq 17$ then $4 < \sqrt{p}$, and since $r, s < \sqrt{p}$ we have

$$2(r + s - 1) - 3 < 4\sqrt{p} - 5 < p - 3.$$

The number of problem cases is therefore fewer than the number of possibilities for c, so we may choose y'' to ensure coprimality. When $p = 7$, 11 or 13, we may explicitly count the number of problem cases as at most 3, 7 and 7 respectively, which are less than $p-3$ in each case. So again we may choose y'' to ensure coprimality.

On the other hand, it may be the case that we are forced to take $\nu = \alpha$. However, we then apply Lemma 9.13(ii) to adjust the lengths of $\mathcal{O}_{x'y'}(\mu)$ and $\mathcal{O}(\alpha)$, and again use Lemma 9.13(iii) in a similar way to that above to show we can ensure coprimality. $\square$

We now drop our assumptions on the size of $\mathrm{supp}(x) \cup \mathrm{supp}(y)$ and cycle type of xy.

Lemma 9.19. *Suppose Hyposthesis 9.17 holds. Then there exists elements $x' \in x^G$, $y' \in y^G$ such that $\langle x' \rangle$, respectively $\langle y' \rangle$, has the same orbits on Ω as $\langle x \rangle$, respectively $\langle y \rangle$, and the product $x'y'$ has order coprime to p.*

Proof. If xy has order coprime to p, then clearly setting $x' = x$, $y' = y$ satisfies the lemma, so assume this is not the case. As in the proof of Lemma 9.18 we consider xy as an element of $\mathrm{Sym}(\mathrm{supp}(x) \cup \mathrm{supp}(y))$. Firstly, suppose that $xy = \sigma_{kp} \prod_{i=1}^{l} \rho_i$, where σ_{kp} is a cycle of length kp, and $\rho_1, \ldots, \rho_l$ are cycles of length coprime to p (possibly 1-cycles). If no such ρ_i exist, then xy is a kp-cycle and $|\mathrm{supp}(x) \cup \mathrm{supp}(y)| = kp$, so we may apply Lemma 9.18 to obtain suitable elements x' and y'. Thus we may assume there is at least one ρ_i. By Lemma 9.16 there exists a cycle λ of either x or y, with $\alpha, \beta \in \mathrm{supp}(\lambda)$ such that $\alpha \in \mathrm{supp}(\sigma_{kp})$ and $\beta \notin \mathrm{supp}(\sigma_{kp})$. Without loss of generality we suppose that λ is a cycle of y, and that $\beta \in \mathrm{supp}(\rho_1)$.

We now apply Lemma 9.13(i) (if possible) to increase the length of σ_{kp} by 'merging' it with some of the ρ_i, and we do this as many times as we can until it becomes impossible to apply (i). We therefore get an element y' such that either xy' is a single cycle, or all elements of λ which do not lie in $\mathcal{O}_{xy'}(\alpha)$ lie in only one other orbit of $\langle xy' \rangle$, which without loss we assume to be $\mathcal{O}_{xy'}(\beta)$. In the case where xy' is a single cycle, we either have coprimality, or if p divides this cycle length we may apply Lemma 9.18 to establish the result. In the latter case we either have coprimality, or at least one of $|\mathcal{O}_{xy'}(\alpha)|$ and $|\mathcal{O}_{xy'}(\beta)|$ is divisible by p. Notice that $|\mathcal{O}_{y'}(\alpha) \cap (\mathcal{O}_{xy'}(\alpha) \cup \mathcal{O}_{xy'}(\beta))| = p$. We now apply Lemma 9.13(ii) to adjust the lengths of these two cycles of xy'. Note that no other cycles of xy' are affected by this. This will ensure coprimality unless the element y'' which we construct yields product xy'' with $|\mathcal{O}_{xy''}(\alpha)| = up$ or $|\mathcal{O}_{xy''}(\gamma)| = vp$, where $1 \leq u, v < (r+s)$, and $\mathcal{O}_{xy''}(\gamma)$ is the other orbit whose length we affect. By Lemma 9.13(iii) we have at least $(p-1)(p-2)/2$ choices of element y'' for which $|\mathcal{O}_{xy''}(\alpha)| = |\mathcal{O}_{xy'}(\alpha)| + c$, and there are at least $p-2$ distinct possibilities for c.

Suppose that both $|\mathcal{O}_{xy'}(\alpha)|$ and $|\mathcal{O}_{xy'}(\beta)|$ are divisible by p. Then if we construct y'' so that $|\mathcal{O}_{xy''}(\alpha)|$ is a mutiple of p, then $|\mathcal{O}_{xy''}(\gamma)|$ must also be a multiple of p. Since we have assumed that we start with $|\mathcal{O}_{xy'}(\alpha)|$ a multiple of p, there are $(r+s-1)-1 = r+s-2$ problem cases in this situation. But for $p \geq 7$, $r+s-2 < p-2$, so we can choose y'' so that neither $|\mathcal{O}_{xy''}(\alpha)|$ nor $|\mathcal{O}_{xy''}(\gamma)|$ is divisible by p, thus ensuring coprimality.

Now suppose that only one of $|\mathcal{O}_{xy'}(\alpha)|$ and $|\mathcal{O}_{xy'}(\beta)|$ is divisible by p. Without loss we assume that $|\mathcal{O}_{xy'}(\alpha)| = wp$ for some $w \in \mathbb{N}$, and that $|\mathcal{O}_{xy'}(\beta)| = l$ where $l \in \mathbb{N}$ is coprime to p. When applying Lemma 9.13(ii), we will ensure coprimality unless $c = ap$ or $c = b(p-l)$, where there are at most $r+s-1$ possibilities each for $a, b \in \mathbb{N}$. There are a possible $2(r+s-1)-1 = 2(r+s)-3$ problem cases here. Let $\{c_1, c_2, \ldots, c_{p-2}\}$ be the set of $p-2$ distinct values of c we can guarantee by Lemma 9.13(iii), ordered so that $c_i > c_j$ when $i > j$. Since $r + s - 1 < p - 2$, it must be the case that $\{c_1, c_2, \ldots, c_{p-2}\}$ includes both a multiple of p and a multiple of $p-l$. But since p and $p-l$ are coprime, and by Lemma 9.13(iii) the set of possible values for c is

$$\{c_i - c_j : 0 \leq j < i \leq p-2\},$$

we see there must in fact be at least $2p-5$ distinct choices for c, which ensures coprimality.

Now suppose that $xy = \sigma_1 \ldots \sigma_m \prod_{i=1}^{l} \rho_i$, where $\sigma_1, \ldots, \sigma_m$ are cycles with lengths divisible by p, and $m \geq 2$. By Lemma 9.16 there exists a cycle λ of either x or y, with $\alpha, \beta \in \mathrm{supp}(\lambda)$ such that $\alpha \in \mathrm{supp}(\sigma_1)$ and $\beta \notin \mathrm{supp}(\sigma_1)$. Without loss of generality we suppose that λ is a cycle of y. As in the previous case we apply Lemma 9.13(i) (if possible) to increase the length of σ_1. Again, we do this multiple times until it becomes impossible to apply (i). Then we get an element y' such that either the number of cycles with length divisible by p in xy' is less than the number in xy, or all elements of λ which do not lie in $\mathcal{O}_{xy'}(\alpha)$ lie in only one other orbit of xy', which without loss we assume to be $\mathcal{O}_{xy'}(\beta)$. In the former case, by induction the lemma holds for the pair (x, y'). But since $\langle y \rangle$ and $\langle y' \rangle$ have the same orbits on Ω, this implies that the lemma also holds for (x, y). In the latter case, then as previously we may apply Lemma 9.13(ii) to adjust the lengths of $\mathcal{O}_{xy'}(\alpha)$ and a subsequent orbit $\mathcal{O}_{xy'}(\gamma)$. Lemma 9.13(iii) tells us that we can construct an element y'' such that for xy'' neither $|\mathcal{O}_{xy''}(\alpha)|$ nor $|\mathcal{O}_{xy''}(\gamma)|$ is divisible by p. Thus the number of cycles of xy'' with length divisible by p is less than that of xy. By induction the lemma holds for (x, y''), whence it also holds for (x, y). □

Lemma 9.20. *Let (x, y) be a tangled pair, with $x, y \neq (\emptyset)$, and suppose that x contains more p-cycles than y. Then there exists a cycle λ of x such that $(x\lambda^{-1}, y)$ is still a tangled pair.*

Proof. Since (x, y) is tangled, and x contains more cycles than y, there must exist cycles λ and ρ of x such that for every cycle of y with which λ has a non-empty intersection, ρ also has a non-empty intersection. But now if $(x\lambda^{-1}, y)$ were disentangled, then (x, y) would also be disentangled, a contradiction. Thus $(x\lambda^{-1}, y)$ is tangled. $\square$

We have reached the point where we can prove Theorem 9.3, which we now restate.

Theorem 9.21. *Let* $G = \mathrm{Sym}(n)$*, with* X *a conjugacy class of elements of cycle type* p^r*, where* p *is an odd prime and* $r < \sqrt{p}$*. Then* $\mathrm{Diam}(\mathcal{C}_{p'}(G, X)) \leq 5$*.*

Proof. When $p = 3$ we must have $r = 1$, so we may apply Theorem 9.2 to see that $\mathrm{Diam}(\mathcal{C}_{3'}(G, X)) \leq 2$, where X is the unique G-conjugacy class of 3-cycles. Now suppose that $p = 5$, so $r = 1$ or 2. When $r = 1$ we can again apply Theorem 9.2 to show the result holds in this case. Assume then that $r = 2$. Let $t \in X$ be our base point, and let $x \in X$, where $X = t^G$. Clearly we have $10 \leq |\mathrm{supp}(t) \cup \mathrm{supp}(x)| \leq 20$. Using MAGMA [18] and the class structure constants described in Chapter 5, it is straightforward to verify that for $10 \leq n \leq 20$, $\mathrm{Diam}(\mathcal{C}_{5'}(\mathrm{Sym}(n), X') = 2$, where X' is the $\mathrm{Sym}(n)$-conjugacy class of elements with cycle type 5^2. (This is done by calculating that $|\Delta_1(t)| > |X'|/2$ in each case, and applying Lemma 1.16). Consequently there exists a path of length 2 between t and x in $\mathcal{C}_{5'}(G, X)$.

We may therefore proceed on the assumption that $p \geq 7$. Assume $t = t_1 \dots t_k$, $x = x_1 \dots x_k$ is a decomposition of (t, x) into tangled pairs. Note that some of these pairs may be of the form $(t_i, (\emptyset))$ or $((\emptyset), x_i)$. Suppose there are m_1 such pairs $(t_i, (\emptyset))$ and m_2 such pairs $((\emptyset), x_i)$, and without loss of generality assume that $m_2 \geq m_1$. By pairing up such cycles, we can get m_1 pairs (t_i, x_j) of disjoint p-cycles, which leaves us with $m_2 - m_1$ cycles x_j which have not yet been paired up. Note that the support of any one of these cycles intersects in the empty set with the remainder of the support of t and x. For each such x_j, choose a tangled pair (t_i, x_i) for which t_i has more cycles than x_i (such a pair must exist since t and x have the same cycle type), and remove a cycle σ from t_i in such a way that $(t_i\sigma^{-1}, x_i)$ remains tangled (this is possible by Lemma 9.20). Thus (σ, x_j) is a pair of disjoint p-cycles. In this way we get a new decomposition $t = t_1 \dots t_l t_{l+1} \dots t_v$, $x = x_1 \dots x_l x_{l+1} \dots x_v$ of (t, x), where (t_i, x_i) is tangled for $1 \leq i \leq l$ and consists of two disjoint p-cycles for $l + 1 \leq i \leq v$.

By Lemma 9.19, for each tangled pair $(t^{(i)}, x^{(i)})$ there exist elements t_i', x_i' such that $\langle t_i' \rangle$, respectively $\langle x_i' \rangle$, has the same orbits on Ω as $\langle t_i \rangle$, respectively $\langle x_i \rangle$, and for which the product $t_i' x_i'$ has order coprime to p. By Theorem 9.2 the distance between such elements t_i and t_i' in the relevant coprimality graph of $\mathrm{Sym}(\mathrm{supp}(t_i))$ is at most 2, and using Corollary 9.14 if necessary there is a path of length exactly 2. Also, for the disjoint pairs (t_j, x_j), Proposition 9.12 implies the existence of a p-cycle y_j adjacent to both in the relevant coprimality graph of $\mathrm{Sym}(\mathrm{supp}(t_j) \cup \mathrm{supp}(x_j))$. Let $t' = t_1' \dots t_l' x_{l+1} \dots x_v$. Since the cycles $x_{l+1}, \dots, x_v$ are disjoint from t, this element has cycle type p^r, and so lies in X. Also, by the above observations, $d(t, t') \leq 2$ in $\mathcal{C}_{p'}(G, X)$. Now let $x' = x_1' \dots x_l' x_{l+1}^{-1} \dots x_v^{-1}$. This is adjacent to t' in $\mathcal{C}_{p'}(G, X)$, and now using Corollary 9.14 if necessary we see that $d(x', x) \leq 2$. We therefore have a path of length at most 5 between t and x. Thus $\mathrm{Diam}(\mathcal{C}_{p'}(G, X)) \leq 5$. □

Now let X be the G-conjugacy class of elements with cycle type p^r, where $p \geq 5$. Write $r = 2m$ or $r = 2m+1$ if r is even or odd respectively. For $z \in X$, after fixing a left-to-right ordering of the disjoint cycles of z, denote by Λ_z the support of the first m cycles, and by Φ_z the support of the remaining cycles.

Lemma 9.22. *Let $t, x \in X$. Then there exists an element $y \in X$ such that $\Lambda_t \cup \Lambda_y$ is disjoint from $\Phi_t \cup \Phi_y$, and $d(x, y) = 1$ in $\mathcal{C}_{p'}(G, X)$.*

Proof. Let

$$x = (x_{1,1}, \dots, x_{1,p})(x_{2,1}, \dots, x_{2,p}) \dots (x_{r,1}, \dots, x_{r,p}).$$

Then set

$$y = x^{-1} = (x_{1,p}, \dots, x_{1,1})(x_{2,p}, \dots, x_{2,1}) \dots (x_{r,p}, \dots, x_{r,1}).$$

Fix an ordering of the cycles of t. Choose m cycles of y such that the intersection of the support of these cycles with $\Lambda = \Lambda_t$ is as large as possible. Without loss of generality we assume y is labelled so that these cycles are $y_1, \dots, y_m$.

We wish to rearrange the elements of $\mathrm{supp}(y)$ and the cycles of y to get an element $y' \in X$, such that $d(x, y') = 1$, and the support of the first m cycles of y' contains only Λ and elements of $\mathrm{fix}(t)$. Let

$$\Psi = \mathrm{supp}(y) \cap \mathrm{fix}(t),$$

and let $l = |\Lambda \cap \mathrm{supp}(y)|$. Reading y from left to right, collect the first $mp - l$ elements which lie in Ψ into a set Σ'. We now define

$$\Sigma = (\Lambda \cap \mathrm{supp}(y)) \cup \Sigma'.$$

We aim to have the support of the first m cycles of y' equal to Σ, which will ensure y' satisfies the first requirement of the lemma.

(3.3) For each cycle $y_1, \ldots, y_m$ at least one element lies in Σ.

For a contradiction suppose some cycle y_i does not contain an element of Σ. If an element of Λ lies in any cycle $y_{m+1}, \ldots, y_r$, then swapping this cycle with y_i contradicts our choice of the first m cycles of y. The only other possibility is that

$$\mathrm{supp}(y_i) \cup \mathrm{supp}(y_{m+1}) \cup \ldots \cup \mathrm{supp}(y_r) \subseteq \mathrm{supp}(t_{m+1}) \cup \ldots \cup \mathrm{supp}(t_r)$$

which is a contradiction since the cycles of y are disjoint. This proves (3.3).

Suppose there is some cycle y_j of y, where $j > m$, and $\mathrm{supp}(y_j) \subseteq \Sigma$. We then choose a cycle y_i, $i \leq m$, where $\mathrm{supp}(y_i) \nsubseteq \Sigma$ (such a cycle certainly exists, since $|\Sigma| = mp$), and swap the positions of these cycles in y. We do similarly for all such cycles. Therefore by (3.3), after the reordering of cycles, and possible reordering of individual cycles, we may assume without loss that $y_{1,p}, \ldots, y_{m,p} \in \Sigma$, and $y_{m+1,1}, \ldots, y_{r,1} \notin \Sigma$. We now fix this expression for y, so we do not allow any further reordering of cycles, or of elements within cycles.

Set $y = y^{(1)}$. Reading $y^{(1)}$ from left to right, take the first element of $\Lambda_{y^{(1)}}$ which does not lie in Σ, and the first element of $\Phi_{y^{(1)}}$ which does lie in Σ, and swap these to get an element $y^{(2)}$. Now, reading $y^{(2)}$ from left to right, take the first element of $\Lambda_{y^{(2)}}$ which does not lie in Σ, and the first element of $\Phi_{y^{(2)}}$ which does lie in Σ, and swap these to get an element $y^{(3)}$, and so on. Continuing in this fashion, we will eventually get an element $y' = y^{(q)}$ where $\Lambda_{y^{(q)}} = \Sigma$.

We must now show that $d(x, y') = 1$. We claim that any cycle of xy' has length at most 3. Suppose α_k is an element of some cycle of z which also lies in the cycle α of x. Let x be labelled so that it acts in the standard way on the indices $\{1, \ldots, k\}$, so $\alpha_i x = \alpha_{i+1}$ (modulo p). Since $y = x^{-1}$, we have $\alpha_i y = \alpha_{i-1}$.

Suppose that α_{k+1} has been swapped (so $k \neq p-1$) with an element β_{s+1} of some cycle β of x. Note our expression for y ensures that $s \neq 0$. Now β_s may also have been swapped, but since we read from left to right and β_s comes after β_{s+1} in y, this swap must have been with some element to the right of α_{k+1} in y. If this element is α_k, then clearly α_k is fixed by xy'. So suppose it is a different element γ_u from a cycle γ, another of the first m cycles of y (note the possibility that $\gamma = \alpha$). By our expression for y, $u \neq p$. But now γ_{u+1} cannot have been swapped, since if it were it would have to be with an element between β_s and β_{s+1}, a contradiction. Similarly, α_k also cannot be swapped. We thus have

$$y' = \ldots(\ldots, \beta_{s+1}, \alpha_k, \ldots)\ldots(\ldots, \gamma_{u+1}, \beta_s, \ldots)\ldots(\ldots, \alpha_{k+1}, \gamma_u, \ldots)\ldots,$$

(where only the relevant cycles of y' are shown). So α_k is contained in a 3-cycle, namely $(\alpha_k, \gamma_u, \beta_s)$.

It is of course possible that not all elements in the above description have been swapped. However, by similar reasoning to that above, the effect of any non-swapping either gives another 3-cycle or decreases the length of the cycle containing α_k. Thus the length of any cycle in z is at most 3. Since 3 and p are coprime, this shows that $d(x, y') = 1$, and completes the proof of the lemma. $\square$

Finally, with Lemma 9.22 to hand, we may prove Theorem 9.4, which, again for the reader's convenience, we restate.

Theorem 9.23. *Let $G = \mathrm{Sym}(n)$. Suppose $p \geq 5$ is prime. Let X be the conjugacy class of elements with cycle type p^r, and let k be the least non-negative integer such that $r/2^k \leq \lfloor\sqrt{p}\rfloor$. Then $\mathrm{Diam}(\mathcal{C}_{p'}(G, X)) \leq 5 + k$.*

Proof. When $r \leq \lfloor\sqrt{p}\rfloor$ we have $k = 0$, and the result holds by Theorem 9.3. So suppose $r > \lfloor\sqrt{p}\rfloor$, and let $t, x \in X$. Write $r = 2m$ or $r = 2m + 1$ if r is even or odd respectively. By Lemma 9.22 there exists an element y such that $d(x, y) = 1$, and we can write $t = t_1t_2$, $y = y_1y_2$, where t_1, y_1 have cycle type p^m, t_2, y_2 have cycle type p^m or p^{m+1}, and the support Λ of t_1 and y_1 is disjoint from the support Φ of t_2 and y_2. If $r = 2m$, then since $r/2^k \leq \lfloor\sqrt{p}\rfloor$, we have $m/2^{k-1} \leq \lfloor\sqrt{p}\rfloor$. Furthermore, if $r = 2m + 1$, it is also the case that $(m + 1)/2^{k-1} \leq \lfloor\sqrt{p}\rfloor$. Indeed, since $(2m + 1)/2^k \leq \lfloor\sqrt{p}\rfloor$ we have $2m + 1 \leq 2^k\lfloor\sqrt{p}\rfloor$. But since $2^k\lfloor\sqrt{p}\rfloor$ is even, this implies that $2m+2 \leq 2^k\lfloor\sqrt{p}\rfloor$, whence $(m+1)/2^{k-1} \leq \lfloor\sqrt{p}\rfloor$. Therefore, by induction there exist paths of length at most $5 + (k - 1)$ in the relevant coprimality graphs of $\mathrm{Sym}(\Lambda)$ and $\mathrm{Sym}(\Phi)$. Since Λ and Φ are disjoint, the products of elements from these paths are elements of X. We therefore have a path of length at most $5 + (k - 1) + 1$ from t to x, as required. □

9.5 The proof of Theorem 9.1

For completeness, we conclude this chapter with a proof of Theorem 9.1, due to Peter Rowley.

Proof of Theorem 9.1. Let $t \in X$ be such that $t = t_1t_2 \cdots t_r$, where t_i is the p-cycle

$$((i - 1)p + 1, (i - 1)p + 2, \ldots, ip)$$

for $i = 1, \ldots, r$. Also $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r$ will denote the orbits of $\langle t\rangle$ on Ω of length p. So

$$\mathcal{O}_i = \{(i - 1)p + 1, (i - 1)p + 2, \ldots, ip\}.$$

Set $\Phi = \bigcup_{i=1}^{r} \mathcal{O}_i$ and $\Lambda = \Omega \setminus \Phi$. Let Y denote the connected component of t in $\mathcal{C}_{p'}(G, X)$, and set $K = \mathrm{Stab}_G(Y)$. By Theorem 2.3 $\mathcal{F}(G, X)$ is connected for $n \geq 5$, and by checking the cases $n < 5$ we see the theorem holds for $p = 2$. So we may suppose p is odd. Let $x \in X$. If $\langle x\rangle$ has the same orbits on Ω as $\langle t\rangle$, then $x \in Y$ by Theorem 9.2. Let H denote the stabilizer in G of the partition of Ω given by the orbits of $\langle t\rangle$. We note that $H = J \times L$, where $J \cong \mathrm{Sym}(p) \wr \mathrm{Sym}(r)$ (with the base group being $\mathrm{Sym}(\mathcal{O}_1) \times \cdots \times \mathrm{Sym}(\mathcal{O}_r)$) and $L = \mathrm{Sym}(\Lambda)$. Thus we have $H \leq K$. We next show that $\mathrm{Sym}(\Phi) \times \mathrm{Sym}(\Lambda) \leq K$. If $r = 1$, then we have this immediately. So we may suppose $r \geq 2$. Let $y = y_1 y_2 \cdots y_r$ be the product of pairwise disjoint cycles y_i, where

$$\begin{aligned} y_1 &= (2, 1, p+1, p+2, \ldots, 2p-2), \\ y_2 &= (2p-1, 2p, 3, 4, \ldots, p) \end{aligned}$$

and $y_j = t_j^{-1}$ for $j \geq 3$. So $y \in X$ and

$$\begin{aligned} xy &= (1)(2, 4, 6, \ldots, p-1, 2p-1, 3, 5, \ldots \\ &\qquad \ldots, p, p+1, p+3, p+5, \ldots, 2p-2, 2p, p+2, p+4, \ldots, 2p-3) \end{aligned}$$

which has order $2p-1$. As a result x and y are adjacent in $\mathcal{C}_{p'}(G, X)$ and we infer that $y \in K$. Since $y \in \mathrm{Sym}(\Phi) \setminus J$ and J is a maximal subgroup of $\mathrm{Sym}(\Phi)$, we deduce that $\mathrm{Sym}(\Phi) \times \mathrm{Sym}(\Lambda) \leq K$.

If $\Lambda = \emptyset$, then we obtain $K = G$ whence $\mathcal{C}_{p'}(G, X)$ is connected. So we now suppose $\Lambda \neq \emptyset$ and select $\alpha \in \Lambda$. Consider $z = z_1 z_2 \cdots z_r \in X$, where

$$z_1 = (2, 3, \ldots, p, \alpha)$$

and $z_j = t_j^{-1}$ for $j \geq 2$. Then

$$tz = (1, 3, 5, \ldots, p-2, p)(2, 4, \ldots, p-1, \alpha)$$

which has order $(p-1)/2$. So t and z are adjacent and thus $z \in K$. But $z \notin \mathrm{Sym}(\Phi) \times \mathrm{Sym}(\Lambda)$, which is a maximal subgroup of G. Therefore $K = G$ and $\mathcal{C}_{p'}(G, X)$ is connected, so proving the theorem. $\square$

Chapter 10

A Computational Application of Local Fusion Graphs

In this final chapter our focus returns to local fusion graphs, as we describe a computational algorithm which makes use of them to produce elements of the centraliser of a given involution. The material presented here also appears in [9]. The importance of centralisers of involutions in understanding finite groups of even order was first indicated by the celebrated paper of Brauer and Fowler [19]. Subsequently, the study of involution centralisers played a fundamental role in the proof of the Classification of Finite Simple Groups. In more recent years, the importance of involutions centralisers has also been seen in computational group theory, with examples to be found in [2], [43], [44] and [54].

When working with a specific finite group G in a computational algebra package, such as Magma [18] or GAP [36], it is most common to make use of either a matrix or permutation representation of G. When G is, say, a symmetric group or linear group, then G comes hand-in-hand with a natural representation. However, there are often a large number of representations of a given group to choose from, some of which may be of particular use in certain situations. Numerous examples of such representations can be found on the online Atlas [1]. Given an involution $t \in G$, it is often desirable to construct $C_G(t)$ as a subgroup of G. To this end, both Magma and GAP have inbuilt commands `Centraliser(G)`, which make use of efficient computational algorithms.

However, when the group, or representation used, is very large, these algorithms can often fail to produce $C_G(t)$ due to insufficient computational power. Indeed, it is often effectively impossible to construct $C_G(t)$ as a subgroup of G by any means. In these situtations, the next best thing is often to produce a 'useful' subset of elements of $C_G(t)$.

10.1 Bray's Algorithm

One of the standard algorithms for producing elements of an involution centraliser is due to John Bray [20]. Suppose that G is a finite group and X is a G-conjugacy class of involutions. Let $h \in G$, $x \in X$ and k be the order of $[x,h]$. Bray's algorithm involves the elements $\beta_0(x,h)$ and $\beta_1(x,h)$ where

$$\beta_0(x,h) = [x,h]^{k/2}$$

if k is even and

$$\beta_1(x,h) = h[x,h]^{(k-1)/2}$$

if k is odd. Then, as is straightforward to check, $\beta_0(x,h), \beta_0(x,h^{-1}) \in C_G(x)$ (if k is even) and $\beta_1(x,h) \in C_G(x)$ (if k is odd). Thus, given an element h of G, Bray's algorithm is guaranteed to output an element of $C_G(x)$. This method is widely used, appearing in [15], [54] and [55] to cite but three examples, and is very efficient in practice. It is also shown in [20] that the centraliser elements $\beta_1(x,h)$ produced by the algorithm are uniformly distributed in $C_G(x)$, provided the input elements are randomly distributed in G. However, in the standard implementation of Bray's method, the ratio of input elements of G to output elements of $C_G(x)$ is relatively low. Thus, in situations where the cost of producing random elements is high (for example when working with a very large matrix or permutation representation), Bray's algorithm loses some of its efficiency. It is therefore desirable to have a method for producing elements of $C_G(x)$ which relies on a smaller set of random elements as input. This is where local fusion graphs appear on the scene.

10.2 Finding Centraliser Elements

Recall from Chapter 1 our observation that if

$$x = x_1 \to x_2 \to \cdots \to x_m = z$$

is a path from x to z in $\mathcal{F}(G,X)$, then $g_1 g_2 \cdots g_{m-1}$ conjugates x to z, where $g_i \in \langle x_i, x_{i+1} \rangle$ for $1 \leq i \leq m-1$. If it is the case that $z = x$, we have a cycle γ in $\mathcal{F}(G,X)$, and $g(\gamma, x) = g_1 g_2 \cdots g_{m-1}$ conjugates x to x, so lies in $C_G(x)$. Also, if $g_i = (x_i x_{i+1})^{(k_i-1)/2}$, then $g_i' = x_i g$ also conjugates x_i to x_{i+1}, so replacing various of the g_j in g by g_j' will potentially yield further elements of $C_G(x)$. Thus foraging for cycles in $\mathcal{F}(G,X)$ may produce elements of $C_G(x)$.

In practice, our method is as follows. Let t be a fixed involution in X. To find elements in $C_G(t)$ we first choose r random elements $h_1, \ldots, h_r$ of G, and calculate $x_i = t^{h_i}$. Then we determine the subgraph $\mathcal{G}$ of $\mathcal{F}(G,X)$ which has

$$\{t\} \cup \{x_i : i = 1, \ldots, r\}$$

as its vertex set. For each vertex x of $\mathcal{G}$ we itemize the cycles in $\mathcal{G}$ based at x (and we may also place a limit on the lengths of these cycles). As already indicated each such cycle based at x delivers elements of $C_G(x)$. If $x = t$, then we have elements of $C_G(t)$, otherwise for $x = x_i$ we conjugate these cycle elements by h_i^{-1} to obtain elements of $C_G(t)$. We can also extract the last drop of blood by creating elements at x_i using Bray's algorithm, namely $\beta_0(x_i, h_j), \beta_0(x_i, h_j^{-1})$ and $\beta_1(x_i, h_j)$, and then conjugating them by h_i^{-1} to yield elements of $C_G(t)$. Of course we also have the Bray elements at t. Finally we observe that, just as for the Bray algorithm, the above procedure works with black box groups.

Evidently, $\mathcal{G}$ having few (or no) cycles will result in slim pickings. Indeed, in our implementation of this algorithm, after having constructed the relevant piece of the local fusion graph we count the number of edges, and if this is small we then discard some of the vertices whose valency is low. We then seek to replace these by vertices of larger valency, and then move on to calculate the cycle elements. However, there are many groups in which we can expect the number of edges in our subgraph to be relatively high. For example, if G is a group of Lie-type in odd characteristic, lower bounds on the number of edges in the local fusion graphs of G have been determined by Parker and Wilson in Theorems 1 and 2 of [54]. These lower bounds are not sharp, but they conjecture that for an exceptional group of Lie-type in odd characteristic the number of edges in $\mathcal{F}(G, X)$ is at least $|X|/8$. Also recall from Chapter 5 that the valencies of the local fusion graphs of the sporadic simple groups have been calculated. We note that in all but four cases the valency of $\mathcal{F}(G, X)$ is at least $|X|/4$. The exceptions are $(G, X) = (He, 2A)$, $(Co_2, 2C)$, $(M_{24}, 2A)$ and $(\mathbb{B}, 2A)$, with the latter having the smallest valency of approximately $|X|/5.72$

One benefit of the method described here is that, under favourable circumstances, a comparatively large number of elements of $C_G(t)$ are obtained from a small number of random elements of G. Hence this procedure is particularly useful when working with matrix groups or permutation groups of very large dimension/degree, where the cost of computing random elements is high. In such groups it may be near impossible to check whether a set of given elements generates the whole centraliser of an involution. Hence the next best thing is to be able to manufacture a diverse and large set of elements of the involution centraliser. In truth, it is hard to analyse the elements which are produced by this algorithm, apart from the Bray elements $\beta_0(t, h)$ and $\beta_1(t, h)$ (which are uniformly distributed in $C_G(t)$ if the input elements h are randomly distributed in G). For one thing, the algorithm only examines a very small fragment of the local fusion graph, and so very little can be said. Moreover it is also not clear how randomly generated are the other kind of Bray elements $\beta_0(x_i, h_j)$, $\beta_0(x_i, h_j^{-1})$ and $\beta_1(x_i, h_j)$. However, as we shall see in Section 10.4, it can often be the case that, given a set of random elements, the cycle elements produced by the algorithm lie outside the group generated by the Bray elements at t.

10.3 Calculating Cycle Elements

Input: The black box group G, an involution t of G and natural numbers v and k;

(i) Set $h_1 = 1$. Calculate $v-1$ random elements $h_2, \ldots h_v$ of G and then determine

$x_i = t^{h_i}$. Store both the $\{x_i\}$ and $\{h_i\}$ in a matrix.

(ii) Calculate the subgraph $\mathcal{G}$ of $\mathcal{F}(G, X)$ (where $X = t^G$) with vertex set $\{x_1 = t, x_2, \ldots, x_v\}$. This involves finding the order of products $x_i x_j$, which are stored in a matrix. From this matrix the adjacency matrix of $\mathcal{G}$ can be found.

(iii) Store the set of neighbours for each vertex in $\mathcal{G}$. Note that these are stored as graph vertices and not as group elements.

(iv) For each vertex x of $\mathcal{G}$, calculate all cycles of $\mathcal{G}$ which have length at most k and are based at x.

(v) For each vertex x and cycle γ obtained in (iv) calculate $g(\gamma, x)$.

Output: elements of $C_G(t)$:

$$g(\gamma, x_i)^{h_i^{-1}}, \beta_0(x_i, h_j)^{h_i^{-1}}, \beta_0(x_i, h_j^{-1})^{h_i^{-1}}, \beta_1(x_i, h_j)^{h_i^{-1}} \text{ and } \mathcal{G}$$

It should be emphasized that we view cycles as having a particular start and finish vertex. Let γ be a cycle in $\mathcal{G}$ that contains vertices x and y. So these give rise to the elements $g(\gamma, x)$ and $g(\gamma, y)$ which of course are conjugate elements of G, and at first sight are not so different. Yet, letting h_x, respectively h_y, be the random element giving $x = t^{h_x}$, respectively $y = t^{h_y}$, it is $g(\gamma, x)^{h_x^{-1}}$ and $g(\gamma, y)^{h_y^{-1}}$ which are in $C_G(t)$, and these can be very different. However, we observe that the 'orientation' of a cycle is unimportant. For, if $\widehat{\gamma}$ denotes the cycle γ with its orientation reversed and x is a vertex of γ, then $g(\widehat{\gamma}, x) = g(\gamma, x)^{-1}$.

Suppose we have a local fusion graph $\mathcal{F}(G, X)$ which has valency approximately $|X|/m$. Then it is possible to give an estimate of the number of k-cycles (that is, cycles of length k) in a subgraph $\mathcal{G}$ which we construct, and hence estimate the number of elements of $C_G(t)$ which our algorithm will produce. Let v be the number of vertices of $\mathcal{G}$. Each k-cycle corresponds to an ordered k-tuple of vertices of $\mathcal{G}$, and there are $v(v-1)\cdots(v-k+1)$ such k-tuples. Since the probability of two random elements of X having odd order product is approximately $1/m$, and we disregard cycles which are reverses of previously considered cycles, the approximate number of k-cycles in $\mathcal{G}$ is

$$\frac{v(v-1)\cdots(v-k+1)}{2m^k}.$$

Note that we are assuming here that v is negligible in comparison to $|X|$.

Now suppose we wish to generate a certain number of elements of $C_G(t)$ using the algorithm described above. To achieve this, we must make choices for the number of vertices v, the maximum path length k to consider, and the number of times to run the algorithm. It is natural to ask which choices will produce the required number of elements of $C_G(t)$ in the shortest time. It is possible to give an indication of the optimal choice of k. Let r be the least integer such that

$$r\sum_{i=3}^{k}\frac{v(v-1)\cdots(v-i+1)}{2m^i} \geq \sum_{i=3}^{k+1}\frac{v(v-1)\cdots(v-i+1)}{2m^i}.$$

Let $t(\mathcal{G})$ be the average time taken to construct $\mathcal{G}$. Note that this depends on the number of vertices v, the cost of calculating random elements in G, and the cost μ of multiplying elements in G. We also denote by χ the average time taken to calculate the conjugating element g_i which sends x_i to to the next element x_{i+1} in a particular cycle. This value depends on both μ and the order of the product x_ix_{i+1}. Then it is worth increasing the maximum length of path considered to $k+1$ if

$$r\left(t(\mathcal{G})+\chi\sum_{i=3}^{k}\frac{iv(v-1)\cdots(v-i+1)}{2m^i}\right) > t(\mathcal{G})+\chi\sum_{i=3}^{k+1}\frac{iv(v-1)\cdots(v-i+1)}{2m^i},$$

which we may rearrange to give the following condition on $t(\mathcal{G})$:

$$t(\mathcal{G}) > \frac{\chi(k+1)v(v-1)\cdots(v-k)}{2m^{k+1}(r-1)} - \chi\sum_{i=3}^{k}\frac{iv(v-1)\cdots(v-i+1)}{2m^i}.$$

10.4 Experimental Data

In this section we give some experimental data to demonstrate how the algorithm performs in practice. We approach this from two directions: firstly, we analyse the speed of our algorithm in producing centraliser elements when working with very large representations; and secondly, we address the likelihood of our algorithm producing a generating set for the centraliser of a given involution.

Table 10.1 contains information regarding the speed of our algorithm, with comparisons to Bray's method. In our implementation of the algorithm here, we have only used the elements $g(\gamma, x)$. Calculations were performed on a Unix machine with 8GB of memory and a 3.2GHz processor, running Magma version 2.11-15. The representations of the groups used in each case were taken from the online Atlas [1], and are as follows: the sporadic group M^cL as a permutation group on 299376 points; the exceptional group of Lie-type $E_8(2)$ as a group of 248-dimensional matrices over $\mathbb{F}_2$; the Tits group ${}^2F_4(2)'$ as a group of 109-dimensional matrices over $\mathbb{F}_{25}$; the Lyons group Ly as a group of 111-dimensional matrices over $\mathbb{F}_5$; the sporadic group Fi_{22} as a group of 572-dimensional matrices over $\mathbb{F}_2$; the sporadic group J_4 as a group of 112-dimensional matrices over $\mathbb{F}_2$; the sporadic Baby Monster group $\mathbb{B}$ as a group of 4072-dimensional matrices over $\mathbb{F}_2$; and the triple cover $3^{\cdot}Fi_{24}$ (a maximal subgroup of the Monster group) as a group of 1566-dimensional matrices over $\mathbb{F}_2$.

The first two columns of the table list the group and conjugacy class of involutions used, in Atlas notation [26], while the third column gives the average time (over ten tests) to calculate a random element of G. The fourth column lists the number of vertices of the subgraph of $\mathcal{F}(G, X)$ which we generate, with the fifth displaying the maximum length of cycle we consider. The sixth column lists the average number of centraliser elements produced by our algorithm over fifty runs (with the exception of $\mathbb{B}$, which was over ten runs). The penultimate column shows the average time taken (in seconds) over these runs for the algorithm to complete. Finally, for comparison we display the average time taken (in seconds, over ten runs) to produce this number of centraliser elements just using Bray's algorithm.

In the last line of the table above $2C^\dagger$ denotes the conjugacy class which projects to the class $2C$ in Fi_{24}. The representations used have been chosen to demonstrate the capabilities of our algorithm when dealing with large permutation and matrix representations. It is worthwhile to note, however, that in the cases of $E_8(2)$ and B the representations used are in fact the minimal dimension matrix representations over the field $\mathbb{F}_2$.

The optimal value of k can be calculated for the cases analysed in Table 10.1

Table 10.1: Comparative Speeds

G	t	T(Random)	v	k	No. of elements	T(Cycles)	T(Bray)
M^cL	$2A$	1.35	8	4	49.64	14.63	65.35
M^cL	$2A$	1.35	8	5	171.38	28.57	234.98
$E_8(2)$	$2A$	0.07	11	4	318.62	8.26	34.09
$E_8(2)$	$2A$	0.07	12	4	431.92	12.63	49.79
$E_8(2)$	$2A$	0.07	13	4	659.48	18.21	70.03
${}^2F_4(2)'$	$2A$	0.31	8	3	12.42	6.08	5.77
${}^2F_4(2)'$	$2A$	0.31	8	4	41.5	12.66	20.11
${}^2F_4(2)'$	$2A$	0.31	8	5	100.60	26.76	58.23
Ly	$2A$	0.15	9	3	35.00	6.92	11.13
Ly	$2A$	0.15	9	4	156.52	22.90	52.46
Ly	$2A$	0.15	9	5	539.02	90.37	154.51
Fi_{22}	$2A$	0.65	8	3	88.58	16.12	67.66
Fi_{22}	$2A$	0.65	8	4	428.28	92.49	381.66
J_4	$2B$	0.33	10	3	68.68	1.43	2.84
J_4	$2B$	0.33	10	4	342.26	4.28	8.54
J_4	$2B$	0.33	10	5	1587.82	54.53	66.52
B	$2C$	165.80	12	3	38.00	5152.91	8076.62
$3^{\cdot}Fi_{24}$	$2C^{\dagger}$	15.20	8	4	675.36	1922.57	11737.99

using the method described in Section 10.3. For example, in the case of Ly when v is chosen to be 9, the optimal value of k is predicted to be 4, which agrees with the experimental data shown. On the other hand, in the case of M^cL where v is 8, the optimal value of k is 5, despite the number of vertices being lower than in the Ly case. This is explained by the relatively high cost of computing random elements in the very large permutation representation of M^cL, in comparison to the cost of multiplying elements.

We now move on to consider the likelihood of our algorithm producing a generating set for the centraliser of an involution. The data contained in Table 10.2 covers a number of groups, including some of those studied in Table 10.1. The groups chosen have relatively small permutation representations, in which it is possible to construct $C_G(t)$ using standard Magma commands. This allows us to check with ease the size of subgroups generated by sets of elements. The representations used are again taken from the online Atlas [1].

The first two columns of Table 10.2 list the group and conjugacy class of involutions used, while the third and fourth show the number of vertices used and maximum length of cycle considered in the subgraph of $\mathcal{F}(G, X)$. The next four columns detail the results of the implementation of four variations on our algorithm and Bray's method. For a given group G, each makes use of the same set of random elements $\{h_1, \ldots, h_{v-1}\}$. The fifth column gives the probability (as a percentage) that the elements $g(\gamma, x)$ produced by our algorithm generate the whole of $C_G(t)$; the sixth column gives the probability that the Bray elements at t generate the whole of $C_G(t)$; the seventh column gives the probability that the elements $g(\gamma, x)$ and the Bray elements at t together generate the whole of $C_G(t)$; and the final column gives the probability that the elements $g(\gamma, x)$, the Bray elements at t, and the Bray elements at t^{h_i} conjugated by h_i^{-1} all together generate the whole of $C_G(t)$. For each group, to obtain these percentages the algorithm was run 1000 times.

Table 10.2: Probability of generating $C_G(t)$

G	t	v	k	P(Cycles)	P(Bray)	P(C+B)	P(C+B$^+$)
M^cL	$2A$	5	4	68.9	89.3	93.7	100
$^2F_4(2)'$	$2A$	6	4	89.7	84.2	96.7	100
Fi_{22}	$2A$	3	3	34.2	74.0	74.2	99.8
J_3	$2A$	4	4	62.4	79.4	89.9	100
$^3D_4(2)$	$2A$	5	4	94.2	84.4	96.1	100
$^3D_4(2)$	$2B$	6	4	46.3	51.4	85.3	100
$G_2(4)$	$2A$	5	4	98.8	84.4	99.5	100
$G_2(4)$	$2B$	6	4	83.4	75.1	97.4	100
Co_3	$2A$	4	4	14.5	59.4	61.0	100
J_2	$2A$	4	4	69.9	59.6	80.3	99.5
$Sz(32)$	$2A$	5	4	57.2	0	97.4	100

For each group in Table 10.2, v has been chosen so that there is a reasonable chance that the Bray elements at t do not generate the whole of $C_G(t)$. Note that in each row of Table 10.2 it is the case that $\mathrm{P(C+B)} > \mathrm{P(Bray)}$. Therefore for each of the groups tested it is possible to find cycle elements $g(\gamma, x)$ which lie outside the group generated by the Bray elements at t. For a number of the pairs (G, t) we observe that $\mathrm{P(Cycles)} > \mathrm{P(Bray)}$. This may be explained by these groups having highly connected local fusion graphs, and consequently the algorithm producing a comparatively large supply of cycle elements of $C_G(t)$ from a small source of random elements. An extreme case is when $G = Sz(32)$, where we have P(Bray) = 0, since in this situation $C_G(t)$ is a Sylow 2-subgroup of order 1024 which requires at least 5 generators.

In contrast we have the cases $(Fi_{22}, 2A)$ and $(Co_3, 2A)$, where not only is P(Bray) > P(Cycles), but P(C + B) is only very slightly greater than P(Bray), implying that in this case the majority of elements $g(\gamma, x)$ are in fact already contained in the group generated by the Bray elements at t.

10.5 Implementation in Magma

To conclude, we give an implementation of the cycles algorithm in Magma.

```
function Cycles(G,t,v,k)


A:=[]; B:=[];
Append(~A,y); Append(~B,h);
end for;


M:=MatrixRing(Integers(),v);
s1:=<>; s2:=<>;
for j:=1 to v do
 a:=A[j];
 for k:=1 to v do
  b:=A[k];
  if not a eq b and IsOdd(Order(a*b)) then
   Append(~s1,1); Append(~s2,Order(a*b));
   else Append(~s1,0); Append(~s2,Order(a*b));
  end if;
 end for;
```

```
end for;

m:=M![s1[l] : l in [1 .. v^2]];
n:=M![s2[l] : l in [1 .. v^2]];

GG1:=Graph<v | m>;
V:=VertexSet(GG1);

C:={};
N:=[];
Val:=0;
for i:=1 to v do
 Ni:=Neighbours(V.i);
 Append(~N,Ni);
 Val:=Val + #Ni;
end for;

if Val/v le v/4 then
return {},GG1,{},B;
else

GG2:={};
j2:=0;
repeat
 j1:=0;
 for k:=2 to v do
  if #N[k] le v/5 then
   h:=Random(G);y:=t^h;
   Remove(~A,k);Insert(~A,k,y);Remove(~B,k);Insert(~B,k,h);
   q1:=[];q2:=[];
```

```
   for l:=1 to v do
    a:=A[l];
    if not a eq y and IsOdd(Order(a*y)) then
     Append(~q1,1); Append(~q2,Order(a*y));
     else Append(~q1,0); Append(~q2,Order(a*y));
    end if;
   end for;
   for p:=1 to v do
    m[k,p]:=q1[p];n[k,p]:=q2[p];
   end for;
   for p:=1 to v do
    m[p,k]:=q1[p];n[p,k]:=q2[p];
   end for;
   else j1:=j1+1;
  end if;
 end for;
 j2:=j2+1;
 GG2:=Graph<v | m>;
 V:=VertexSet(GG2);
 N:=[];
 for i:=1 to v do
  Ni:=Neighbours(V.i);
  Append(~N,Ni);
 end for;
until j1 eq v-1 or j2 eq 3;

for k:=2 to v do
 if #N[k] le v/5 then
  return {}, GG1,GG2,B;
 end if;
```

```
end for;

for w in V do

Thread:={ [w] };
U:={};

for r in N[Index(w)] do
 y:=Append([w],r);
 U:=U join {y};
end for;

Thread:=U;

for i:=2 to k do
 U:={};
 for s in Thread do
  for r in N[Index(s[i])] do
   if not r eq s[i-1] then
    y:=Append(s,r);
    U:=U join {y};
    if r eq w then
     if not Reverse(y) in U then
      el:=Id(G);
      for j:=2 to i+1 do
       a:=Index(y[j-1]);b:=Index(y[j]);
       d:=(n[a,b]-1)/2;
       e:=IntegerRing()!d;
       f:=(A[b]*A[a])^e;
       el:=el*f;
```

```
      end for;
      g:=el^(B[Index(w)]^-1);
      Include(~C,g);
     end if;
    end if;
   end if;
  end for;
 end for;
 Thread:=U;
end for;

end for;

return C,GG1,GG2,B;

end if;

end function;
```

Bibliography

[1] R. Abbott, J. Bray, S. Linton, S. Nickerson, S. Norton, R. Parker, I. Suleiman, J. Tripp, P. Walsh, and R. Wilson: `http://brauer.maths.qmul.ac.uk/Atlas/v3/`

[2] C. Altseimer, A. V. Borovik: *Probabilistic recognition of orthogonal and symplectic groups, Groups and computation III* (Columbus, OH, 1999), 120, Ohio State Univ. Math. Res. Inst. Publ., 8, de Gruyter, Berlin, 2001.

[3] M. Aschbacher: *Finite group theory*, Second edition. Cambridge Studies in Advanced Mathematics, 10. Cambridge University Press, Cambridge, 2000.

[4] M. Aschbacher: *Sporadic groups*, Cambridge Tracts in Mathematics, 104. Cambridge University Press, Cambridge, 1994.

[5] M. Aschbacher, G. Seitz: *Involutions in Chevalley Groups over Fields of Even Order*, Nagoya Math. J., 1976.

[6] J. Ballantyne: *On Local Fusion Graphs of Finite Coxeter Groups*, submitted.

[7] J. Ballantyne, N. Greer, P. Rowley: *Local Fusion Graphs for Symmetric Groups*, submitted.

[8] J. Ballantyne, N. Greer, P. Rowley: *On Coprimality Graphs for Symmetric Groups*, submitted.

[9] J. Ballantyne, P. Rowley: *A Note on Computing Involution Centralizers*, submitted.

[10] C. Bates, D. Bundy, S. Perkins, P. Rowley: *Commuting Involution Graphs for Symmetric Groups*, J. Algebra 266 (2003), 133–153.

[11] C. Bates, D. Bundy, S. Perkins, P. Rowley. *A Note on Commuting Graphs for Symmetric Groups*, Elec. J. Combinatorics 16 (2009), R6.

[12] C. Bates, D. Bundy, S. Perkins, P. Rowley: *Commuting Involution Graphs for Finite Coxeter Groups*, J. Group Theory 6 (4) (2003), 461–476.

[13] C. Bates, D. Bundy, S. Perkins, P. Rowley: *Commuting involution graphs in special linear groups*, Comm. Algebra 32 (2004), no. 11, 4179–4196.

[14] C. Bates, D. Bundy, S. Perkins, P. Rowley: *Commuting Involution Graphs for Sporadic Groups*, J. Algebra 316 (2007), 849 - 868.

[15] C. Bates, P. Rowley: *Involutions in Conway's largest simple group*, LMS J. Comput. Math. 7 (2004), 337–351.

[16] C. Bates, P. Rowley: *Normalizers of p-subgroups in finite groups*, Arch. Math. (Basel) 92 (2009), no. 1, 7–13.

[17] B. Baumeister, A. Stein: *Commuting graphs of odd prime order elements in simple groups*, arXiv:0908.2583.

[18] W. Bosma, J. Cannon, C. Playoust: *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24(3-4) (1997), 235-265.

[19] R. Brauer, K. A. Fowler: *On groups of even order*, Ann. of Math. (2) 62 (1955), 565–583.

[20] J. N. Bray: *An improved method for generating the centralizer of an involution*, Arch. Math. 74 (2000), 241–245.

[21] N. Burgoyne, R. Griess, R. Lyons: *Maximal subgroups and automorphisms of Chevalley groups*, Pacific J. Math. 71 (1977), no. 2, 365–403.

[22] P. J. Cameron: *Permutation Groups*, London Mathematical Society Student Texts, 45. Cambridge University Press, Cambridge, 1999. x+220 pp.

[23] R. W. Carter: *Conjugacy classes in the Weyl group*, Compositio Math. 25, 1972.

[24] R. W. Carter: *Simple groups of Lie type*, reprint of the 1972 original. Wiley Classics Library. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York (1989). x+335 pp.

[25] R. W. Carter: *Finite groups of Lie type. Conjugacy classes and complex characters*, Reprint of the 1985 original. Wiley Classics Library. A Wiley-Interscience Publication. John Wiley and Sons, Ltd., Chichester, 1993. xii+544 pp.

[26] J H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson: *Atlas of Finite Groups*, Clarendon, Oxford (1985).

[27] B. Cooperstein: *Maximal Subgroups of* $G_2(2^n)$, Journal of Algebra, 1981.

[28] H. S. M. Coxeter: *The complete enumeration of finite groups of the form* $r_i^2 = (r_i r_j)^{k_{ij}} = 1$, J. London Math. Soc. 10, 1935.

[29] R. T. Curtis: *A new combinatorial approach to* M_{24}, Math. Proc. Cambridge Philos. Soc. 79 (1976), no. 1, 25–42.

[30] A. Devillers, M. Giudici: *Involution graphs where the product of two adjacent vertices has order three*, J. Aust. Math. Soc. 85 (2008), no. 3, 305–322.

[31] A. Devillers, M. Giudici, C. H. Li, C. E. Praeger: *Some graphs related to the small Mathieu groups*, European J. Combin. 31 (2010), no. 1, 336–348.

[32] R. H. Dye: *On the Conjugacy Classes of Involutions of Simple Orthogonal Groups over Perfect Fields of Characteristic* 2, Journal of Algebra, 1971.

[33] R. H. Dye: *On the Conjugacy Classes of Involutions of the Unitary Groups* $U_m(K)$, $SU_m(K)$, $PU_m(K)$, $PSU_m(K)$ *over Perfect Fields of Characteristic* 2, Journal of Algebra, 1973.

[34] A. Everett: *Commuting Involution Graphs for 3-Dimensional Unitary Groups*, Electron. J. Combin. 18 (2011), no. 1, 103.

[35] B. Fischer: *Finite groups generated by 3-transpositions*, I. Invent. Math. 13 (1971), 232–246.

[36] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4.12; 2008. (http://www.gap-system.org)

[37] M. Geck: *An introduction to algebraic geometry and algebraic groups*, Oxford Graduate Texts in Mathematics, 10. Oxford University Press, Oxford, 2003. xii+307 pp.

[38] D. Gorenstein: *Finite groups*, Second edition. Chelsea Publishing Co., New York (1980).

[39] D. Gorenstein, R. Lyons, R. Solomon: *The classification of the finite simple groups, Number 4, Part II, Chapters 14., Uniqueness theorems*, Mathematical Surveys and Monographs, 40.4. American Mathematical Society, Providence, RI, 1999. xvi+341 pp.

[40] R. L. Griess, Jr.: *A construction of F_1 as automorphisms of a* $196,883$-*dimensional algebra*, Proc. Nat. Acad. Sci. U.S.A. 78 (1981), no. 2, part 1, 686–691.

[41] S. Guest: *A solvable version of the Baer-Suzuki theorem*, Trans. Amer. Math. Soc. 362 (2010), no. 11, 5909–5946.

[42] R. M. Guralnick, G. R. Robinson: *On extensions of the Baer-Suzuki theorem*, Israel J. Math. 82 (1993), no. 1-3, 281–297.

[43] P. E. Holmes, S. A. Linton, E. A. O'Brien, A. J. E. Ryba, R. A. Wilson: *Constructive membership in black-box groups*, J. Group Theory 11 (2008), no. 6, 747–763.

[44] D. F. Holt, B. Eick, E. A. O'Brien: *Handbook of computational group theory, Discrete Mathematics and its Applications* (Boca Raton), Chapman and Hall/CRC, Boca Raton, FL, 2005. xvi+514 pp.

[45] S. Hoory, N. Linial, A. Wigderson: *Expander graphs and their applications*, Bull. Amer. Math. Soc. (N.S.) 43 (2006), no. 4, 439–561 (electronic).

[46] J. E. Humphreys: *Reflection Groups and Coxeter Groups*, Cambridge studies in advanced mathematics 29, Cambridge University Press (1990).

[47] C. Jordan: *Theoremes sur les groupes primitifs*, J. Math. Pures Appl. 16 (1871), 383–408.

[48] P. Kleidman: *Low Dimensional Finite Classical Groups and Their Subgroups*, Addison-Wesley Longman (1989).

[49] P. Kleidman: *The Maximal Subgroups of the Steinberg Triality Groups* $^3D_4(q)$ *and of Their Automorphism Groups*, Journal of Algebra, 1988.

[50] P. Kleidman, M. Liebeck: *The Subgroup Structure of the Finite Classical Groups*, LMS Lecture Note Series, 1990.

[51] E. L. Mathieu: *Mmoire sur l'tude des fonctions de plusieurs quantits, sur la manire de les former et sur les substitutions qui les laissent invariables*, J. Math. Pures Appl. (Liouville) (2) VI, 1861, pp. 241–323.

[52] E. L. Mathieu: *Sur la fonction cinq fois transitive de 24 quantits*, Liouville Journ., (2) XVIII., 1873, pp. 25–47.

[53] O. T. O'Meara: *Symplectic Groups*, AMS, 1978.

[54] C. W. Parker, R. A. Wilson: *Recognising simplicity of black-box groups by constructing involutions and their centralisers*, J. Algebra 324 (2010), no. 5, 885–915.

[55] P. Rowley, P. Taylor: *Normalizers of 2-subgroups in black-box groups*, LMS J. Comput. Math. 13 (2010), 307–319.

[56] P. Rowley, P. Taylor: *Point-line collinearity graphs of two sporadic minimal parabolic geometries*, J. Algebra 331 (2011), 304–310.

[57] P. Rowley, P. Taylor: *Involutions in Janko's Simple Groups* J_4, MIMS preprint, http://eprints.ma.man.ac.uk/1365/

[58] B. Sagan: *The symmetric group. Representations, combinatorial algorithms, and symmetric functions*, Second edition. Graduate Texts in Mathematics, 203. Springer-Verlag, New York (2001). xvi+238 pp.

[59] A. I. Sozutov: *On a generalization of the Baer-Suzuki theorem* (Russian), Sibirsk. Mat. Zh. 41 (2000), no. 3, 674–675, iv; translation in Siberian Math. J. 41 (2000), no. 3, 561–562.

[60] M. Suzuki: *On a Class of Doubly Transitive Groups*, Annals of Mathematics, 1962.

[61] M. Suzuki: *Group theory I*, Translated from the Japanese by the author. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 247. Springer-Verlag, Berlin-New York, 1982. xiv+434 pp.

[62] D. E. Taylor: *The Geometry of the Classical Groups*, Heldermann Verlag Berlin, 1992.

[63] J. Tits: *Algebraic and abstract simple groups*, Ann. of Math. (2) 80 1964 313–329.

[64] G. E. Wall: *On the conjugacy classes in the unitary, symplectic and orthogonal groups*, J. Austral. Math. Soc. 3 1963 1–62.

[65] R. A. Wilson: *The Finite Simple Groups*, Springer-Verlag London Ltd, 2009.