Topics in Computational Group Theory:
Primitive permutation groups and
matrix group normalisers

Hannah J. Coutts

December 2010
Contents

1 Introduction and important theorems 1
  1.1 Computational group theory .......................... 1
    1.1.1 What is to come ............................. 2
  1.2 Notation and definitions ........................... 3
    1.2.1 Notation .................................. 3
    1.2.2 Definitions ................................. 4
  1.3 The classification of finite simple groups .......... 8
  1.4 Schur’s lemma .................................... 9
  1.5 The classical groups ............................... 10
    1.5.1 Introduction ................................ 10
    1.5.2 Forms ..................................... 10
    1.5.3 Linear .................................... 13
    1.5.4 Symplectic ................................ 14
    1.5.5 Unitary .................................... 15
    1.5.6 Orthogonal ................................ 16
    1.5.7 The simple classical groups .................. 17
  1.6 Aschbacher’s theorem ............................... 20
    1.6.1 $C_1$: Reducible ............................. 20
    1.6.2 $C_2$: Imprimitive ........................... 20
    1.6.3 $C_3$: Semilinear ........................... 21
    1.6.4 $C_4$: Tensor Product ....................... 21
    1.6.5 $C_5$: Subfield ............................. 21
    1.6.6 $C_6$: Extraspecial Normaliser ............... 22
    1.6.7 $C_7$: Tensor Induced ....................... 22
    1.6.8 $C_8$: Classical ............................ 23
    1.6.9 $C_9$: Almost Simple ......................... 23
    1.6.10 Common variants on the theorem ................. 23

I The primitive permutation groups of degree less than
    4096 24

2 Introduction to primitive permutation groups 25
<table>
<thead>
<tr>
<th>Section</th>
<th>Subsection</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0.11</td>
<td>Primitive groups</td>
<td>25</td>
</tr>
<tr>
<td>2.1</td>
<td>History</td>
<td>25</td>
</tr>
<tr>
<td>2.2</td>
<td>Preliminary results</td>
<td>27</td>
</tr>
<tr>
<td>2.2.1</td>
<td>The O’Nan–Scott Theorem</td>
<td>27</td>
</tr>
<tr>
<td>2.2.2</td>
<td>Maximal subgroups and point stabilisers</td>
<td>28</td>
</tr>
<tr>
<td>2.2.3</td>
<td>Permutation isomorphism</td>
<td>29</td>
</tr>
<tr>
<td>2.2.4</td>
<td>Cohorts</td>
<td>30</td>
</tr>
<tr>
<td>3</td>
<td>Affine type groups</td>
<td>32</td>
</tr>
<tr>
<td>3.1</td>
<td>Introduction</td>
<td>32</td>
</tr>
<tr>
<td>3.2</td>
<td>Method</td>
<td>35</td>
</tr>
<tr>
<td>4</td>
<td>Almost simple groups</td>
<td>39</td>
</tr>
<tr>
<td>4.1</td>
<td>Introduction</td>
<td>39</td>
</tr>
<tr>
<td>4.2</td>
<td>Alternating and symmetric groups</td>
<td>40</td>
</tr>
<tr>
<td>4.3</td>
<td>Classical groups</td>
<td>43</td>
</tr>
<tr>
<td>4.3.1</td>
<td>Groups with CS socles</td>
<td>45</td>
</tr>
<tr>
<td>4.3.2</td>
<td>Groups with non-CS socles: reduction of actions</td>
<td>49</td>
</tr>
<tr>
<td>4.3.3</td>
<td>Actions on reducible subgroups</td>
<td>53</td>
</tr>
<tr>
<td>4.3.4</td>
<td>Actions on irreducible subgroups</td>
<td>59</td>
</tr>
<tr>
<td>4.4</td>
<td>Exceptional groups</td>
<td>66</td>
</tr>
<tr>
<td>4.5</td>
<td>Sporadic Groups</td>
<td>71</td>
</tr>
<tr>
<td>4.6</td>
<td>Tables</td>
<td>72</td>
</tr>
<tr>
<td>5</td>
<td>Product action groups</td>
<td>77</td>
</tr>
<tr>
<td>5.1</td>
<td>Introduction</td>
<td>77</td>
</tr>
<tr>
<td>5.2</td>
<td>Making the groups</td>
<td>78</td>
</tr>
<tr>
<td>6</td>
<td>Diagonal type groups</td>
<td>82</td>
</tr>
<tr>
<td>6.1</td>
<td>Introduction and preliminary results</td>
<td>82</td>
</tr>
<tr>
<td>6.2</td>
<td>Making the groups</td>
<td>85</td>
</tr>
<tr>
<td>7</td>
<td>Loose ends</td>
<td>88</td>
</tr>
<tr>
<td>7.1</td>
<td>A group missing from previous databases</td>
<td>88</td>
</tr>
<tr>
<td>7.2</td>
<td>Permutation isomorphism of groups</td>
<td>88</td>
</tr>
<tr>
<td>7.3</td>
<td>Accuracy checks and assumptions</td>
<td>89</td>
</tr>
<tr>
<td>7.4</td>
<td>Further work</td>
<td>90</td>
</tr>
<tr>
<td>II</td>
<td>Normalisers of matrix groups</td>
<td>91</td>
</tr>
<tr>
<td>8</td>
<td>Background and introduction</td>
<td>92</td>
</tr>
<tr>
<td>8.1</td>
<td>History and motivation</td>
<td>92</td>
</tr>
<tr>
<td>8.1.1</td>
<td>Base and strong generating set</td>
<td>92</td>
</tr>
<tr>
<td>8.1.2</td>
<td>Backtrack search</td>
<td>94</td>
</tr>
</tbody>
</table>
8.1.3 Normalisers ................................. 95
8.2 General methods .............................. 97
  8.2.1 Preserving precisely $n$ structures ........ 97
  8.2.2 Recursion ............................... 98
  8.2.3 Normaliser of derived group .............. 98
  8.2.4 Derived group scalar ..................... 99
8.3 When our algorithms fail ...................... 99
8.4 The algorithm: NormaliserGL .................. 100

9 $C_1$: Reducible Groups ........................ 106
  9.1 Introduction ............................... 106
     9.1.1 Change of basis matrix ................. 110
  9.2 Finding Overgroups .......................... 111
     9.2.1 Wreath Product case .................... 111
     9.2.2 Tensor Product case .................... 112
     9.2.3 Problem case .......................... 115
     9.2.4 Direct Product case .................... 115
     9.2.5 Submodule Stabiliser case ............... 116
  9.3 The algorithm: NormaliserReducible .......... 117
  9.4 Timings .................................... 119

10 $C_2$: Imprimitive groups ...................... 121
  10.1 Introduction ................................ 121
  10.2 Finding normalisers of $C_2$-groups ........ 122
     10.2.1 Groups stabilising one block system ... 123
     10.2.2 Groups stabilising two block systems ... 124
     10.2.3 Groups stabilising more than two block systems ... 124
  10.3 Computational methods ...................... 125
     10.3.1 The algorithm: NormaliserImprimitive ... 125
  10.4 Timings .................................... 126

11 $C_3$: Semilinear groups ....................... 130
  11.1 Introduction ................................ 130
     11.1.1 Conway polynomials ..................... 130
  11.2 Defining groups over larger fields ........... 131
     11.2.1 Embedding $GL_{n/s}(q^s)$ in $GL_n(q)$ .... 132
  11.3 Aschbacher class $C_3$ ...................... 133
  11.4 Case 1: $G$ is not absolutely irreducible ... 134
     11.4.1 Algorithm 1 ............................ 135
  11.5 Case 2: $G$ is absolutely irreducible .......... 136
     11.5.1 One embedding .......................... 137
     11.5.2 Two or more embeddings ................. 138
     11.5.3 Algorithm 2 ............................ 138
     11.5.4 The algorithm: NormaliserSemilinear .... 138
11.6 Timings ................................................. 139

12 $C_5$: Subfield groups ........................................... 142
  12.1 Introduction ........................................... 142
  12.2 Overgroup for $N_{\text{GL}_n(q)}(G)$ when $G \in \mathcal{A}$ ........................................... 142
    12.2.1 Subfield groups not in $\mathcal{A}$ ........................................... 143
  12.3 The algorithm: NormaliserSubfield ........................................... 144
  12.4 Timings ........................................... 144

13 $C_8$: Classical Groups ........................................... 147
  13.1 Preliminaries ........................................... 147
  13.2 Forms and normalisers ........................................... 148
  13.3 Normaliser of a $C_8$-group ........................................... 150
  13.4 Class $C'_8$ ........................................... 153
  13.5 The algorithm: NormaliserClassical ........................................... 153
    13.5.1 NormaliserClassical in NormaliserGL ........................................... 154
  13.6 Timings ........................................... 155

14 Future work ........................................... 161
  14.1 $C_6$: Extraspecial normalisers ........................................... 161
  14.2 $C_1$: Further recursion ........................................... 162
  14.3 Characteristic subgroups ........................................... 162
  14.4 Future work ........................................... 163
List of Tables

1.1 Indices of the linear-type groups ........................................ 14
1.2 Indices of the symplectic-type groups ................................. 15
1.3 Indices of the unitary-type groups ...................................... 15
1.4 Indices of the orthogonal-type groups in odd dimension .......... 17
1.5 Indices of the orthogonal-type groups in even dimension ....... 17
1.6 Outer automorphism groups of classical groups $G$ .................. 19

3.1 Groups contained in $L$ ...................................................... 37
3.2 Primitive groups of affine type ........................................... 37

4.1 Socles of almost simple classical groups $G$ with $P(Soc(G)) < 4096$ ............................................................ 44
4.2 Potentially maximal reducible subgroups ............................... 55
4.3 Maximal subgroups $M$ of groups $G$ with socle $T := PΩ_q^+ (3)$ 66
4.4 Orders of the exceptional groups ........................................ 67
4.5 $l(G, p)$, for a simple exceptional group $G$ .......................... 68
4.6 Largest order of a maximal subgroup $M$ of a simple exceptional group $G$ .......................................................... 68
4.7 Primitive almost simple groups with alternating socle ............ 73
4.8 Primitive almost simple groups with socle $L_2(q)$ .................... 74
4.9 Primitive almost simple groups with other classical socles ....... 75
4.10 Primitive almost simple groups with exceptional socle .......... 76
4.11 Primitive almost simple groups with sporadic socle ............... 76

5.1 Almost simple and diagonal type primitive groups $P$ of degree less than 64 ......................................................... 79
5.2 Primitive product action groups ........................................... 81

6.1 Primitive diagonal type groups ........................................... 87

9.1 Time to compute $N_{GL_n(q)}(G)$, for $G \in C_1$ (100 trials) ...... 120
10.1 Time to compute $N_{GL_n(q)}(G)$, for $G \in C_2$ in irreducible matrix group database (100 trials) ................................. 128
10.2 Time to compute $N_{\text{GL}_n(q)}(G)$, for $G \in C_2$ generated using 
**ClassicalMaximals** (100 trials) ........................................ 129

11.1 Time to compute $N_{\text{GL}_n(q)}(G)$, for $G \in C_3$ in irreducible matrix 
group database (100 trials) ................................................. 140

11.2 Time to compute $N_{\text{GL}_n(q)}(G)$, for $G \in C_3$ generated using 
**ClassicalMaximals** (100 trials) ............................................. 141

12.1 Time to compute $N_{\text{GL}_n(q)}(G)$, for $G \in C_5$ (100 trials) ......... 146

13.1 $N_{\text{GL}_n(q)}(C)$ for quasisimple classical group $C$ ..................... 150

13.2 $N_{\text{GL}_n(q)}(C) = F_{q^u}.C.A$ for quasisimple classical group $C$ .... 152

13.3 Time to compute $N_{\text{GL}_n(q)}(G)$, for $G \in C_8$ containing $\text{SL}_n(q)$ 
(20 trials) ............................................................................... 156

13.4 Time to compute $N_{\text{GL}_n(q)}(G)$, for $G \in C_8$ containing $\text{Sp}_n(q)$ 
(20 trials) ............................................................................... 157

13.5 Time to compute $N_{\text{GL}_n(q)}(G)$, for $G \in C_8$ containing $\text{SU}_n(q)$ 
(20 trials) ............................................................................... 157

13.6 Time to compute $N_{\text{GL}_n(q)}(G)$, for $G \in C_8$ containing $\Omega_n(q)$ 
(20 trials) ............................................................................... 157

13.7 Time to compute $N_{\text{GL}_n(q)}(G)$, for $G \in C_8$ containing $\Omega^+_n(q)$ 
(20 trials) ............................................................................... 158

13.8 Time to compute $N_{\text{GL}_n(q)}(G)$, for $G \in C_8$ containing $\Omega^-_n(q)$ 
(20 trials) ............................................................................... 158

13.9 Time to compute $N_{\text{GL}_n(q)}(G)$, for $G \in C_8'$ preserving a sym-
plectic form (25 trials) ............................................................ 158

13.10 Time to compute $N_{\text{GL}_n(q)}(G)$, for $G \in C_8'$ preserving a unitary 
form (25 trials) ........................................................................ 159

13.11 Time to compute $N_{\text{GL}_n(q)}(G)$, for $G \in C_8'$ preserving an or-
thogonal form in odd dimension (25 trials) ................................. 159

13.12 Time to compute $N_{\text{GL}_n(q)}(G)$, for $G \in C_8'$ preserving an or-
thogonal plus form (25 trials) .................................................... 159

13.13 Time to compute $N_{\text{GL}_n(q)}(G)$, for $G \in C_8'$ preserving an or-
thogonal minus form (25 trials) .................................................. 160
My immense gratitude goes to my supervisor and friend Colva Roney-Dougal, who suggested that I do a PhD. She has been my inspiration and a kind mistress and this thesis would never have existed without her. I would also like to thank Martyn Quick for his mathematical support and enduring patience with my stupid questions. A special thank you to my father Jack Coutts for bringing me up so well and being a constant source of love and support, for encouraging me when I was low, and for trying to read the maths. Chris Coutts, Emma Casserley, Alex Imrie, Nicky Simmons and all of my friends and family have provided invaluable encouragement and support and my gratitude goes especially to Fiona Brunk for listening to a lot of whining. Thank you also to Angela Tawse and Liz Porter for providing cake when it was needed and to Sarah Brassey for much needed girl time. The companionship of Spike the horse also contributed much towards my mental health.

Finally but most importantly, I would like to thank Kevin Thomson, who believed the thesis would never be finished, but supported me anyway. He suffered a lot for this work and his love gave me the strength I needed.

This thesis is dedicated to my mother Adrienne Coutts, who gave me my hunger for knowledge and always encouraged me to ask questions. I hope one day to be as wise as her.
Abstract

Part I of this thesis presents methods for finding the primitive permutation groups of degree $d$, where $2500 \leq d < 4096$, using the O’Nan–Scott Theorem and Aschbacher’s theorem. Tables of the groups $G$ are given for each O’Nan–Scott class. For the non-affine groups, additional information is given: the degree $d$ of $G$, the shape of a stabiliser in $G$ of the primitive action, the shape of the normaliser $N$ in $S_d$ of $G$ and the rank of $N$.

Part II presents a new algorithm NormaliserGL for computing the normaliser in $GL_n(q)$ of a group $G \leq GL_n(q)$. The algorithm is implemented in the computational algebra system Magma and employs Aschbacher’s theorem to break the problem into several cases. The attached CD contains the code for the algorithm as well as several test cases which demonstrate the improvement over Magma’s existing algorithm.
Chapter 1

Introduction and important theorems

As the title suggests, this work is in two parts, focusing on two problems in computational group theory (CGT). We set the scene with a brief introduction to CGT and an overview of what to expect from the body of the work.

1.1 Computational group theory

The ability to concisely describe certain groups in terms of generators and relations makes them relatively easy to manipulate computationally, and computational group theorists exploit this property to answer algorithmic questions about groups. The inception of CGT in the early 1900s arose from Dehn’s proposition of, and partial solution to, the word problem: given a group $G$ described in terms of generators $X$ and relations $R$, find an algorithm to determine whether a word in $X$ represents the identity. For a nice introduction to CGT see [63]. The fruits of CGT are implemented in computational algebra systems such as Magma [5] and GAP [23]. We make heavy use of Magma throughout this work, and the database and algorithm we produce will be added to Magma.

The main areas of CGT include permutation groups, matrix groups, black box groups and representation theory. This work focuses on problems from two of these areas: permutation groups in Part I and matrix groups in Part II. The theory for dealing with permutation groups is well developed and most structural properties of permutation groups of ‘reasonable’ degree and order can be readily computed. (Here ‘reasonable’ means degree in the low hundred thousands and log of order in the low hundreds.) Part I of this thesis extends the database of primitive permutation groups to those of degree less than 4096.

In comparison, matrix groups are hard to manipulate computationally
and efficient algorithms are in demand. The international Matrix Group Recognition Project aims to produce and implement effective algorithms for computing with matrix groups and in Part II we contribute to this project by describing an algorithm for computing the normaliser in the general linear group of a matrix group. In theoretical computer science, a universally accepted measure of efficiency is polynomial-time computation, that is computation running in time polynomial in the input size. We shall not analyse the complexity of our algorithms, but will give brief, heuristic justifications for their efficiency.

1.1.1 What is to come

The rest of this chapter presents some notation and definitions which will hold in general for this thesis. This is followed by some well-known theorems and facts which will be repeatedly referred to throughout the work. In Part I we classify the primitive permutation groups of degree less than 4096, using the O’Nan–Scott Theorem as a framework, and in Part II we present an algorithm which uses Aschbacher’s theorem to compute the normaliser of a matrix group in the general linear group.
1.2 Notation and definitions

The following statements and notation apply throughout this work, unless otherwise stated. Many of these definitions and notations are standard but given for clarification. In general we assume all groups to be finite, however some results also hold for infinite groups.

1.2.1 Notation

The identity element of $G$ is written $\text{id}_G$ or $1$. The cyclic group $\mathbb{Z}_n$ is often denoted by its order $n$. The notation $Z(G)$ denotes the centre of a group $G$. The notation $H \leq_{\text{max}} G$ indicates that $H$ is a maximal subgroup of $G$. Let $n$ be positive integer, then the dihedral group of order $2n$ is denoted $D_{2n}$ and $[n]$ denotes an unspecified soluble group of order $n$, after the notation of [32]. The greatest common divisor of integers $a$ and $b$ is denoted by $(a,b)$.

Maps are usually written on the right and it will be clearly stated when this is not the case. Conjugation is sometimes written in exponential notation.

Magma All MAGMA functions are written in this font. A group $G$ is $CS$ if it has computable subgroups in MAGMA V2.14–12, that is the function $\text{HasComputableSubgroups}(G)$ returns true. In this thesis we make frequent use of the MAGMA function $\text{MaximalSubgroups}(G)$, which computes conjugacy class representatives of the maximal subgroups of a matrix group $G$, as follows. If $G$ is soluble, then its maximal subgroups are computed directly. If $G$ has a non-abelian composition factor $C$, then MAGMA uses a database to find the maximal subgroups of $C$ before calculating suitable preimages of these groups in $G$, which correspond to maximal subgroups of $G$.

All computations were performed in MAGMA on a standard postgraduate desktop computer with the Linux operating platform.

Matrix groups Let $q$ be a prime power. We denote the Galois field of order $q$ by $\mathbb{F}_q$ and the multiplicative group of this field by $\mathbb{F}_q^\ast$. The group $\text{GL}_n(q) = \text{GL}_n(\mathbb{F}_q)$ consists of all invertible $n \times n$ matrices with entries in the field $\mathbb{F}_q$ and $I_n$ denotes the $n \times n$ identity matrix. The centre of $\text{GL}_n(q)$ consists of all scalar matrices with entries in $\mathbb{F}_q^\ast$. Hence $\mathbb{F}_q^\ast \cong Z(\text{GL}_n(q))$ and we sometimes identify these objects.

The $n$-dimensional vector space over $\mathbb{F}_q$ will typically be denoted by $V$ and we frequently denote the standard or natural basis

$$\{(1,0,\ldots,0),(0,1,\ldots,0),\ldots,(0,0,\ldots,1)\}$$

of $V$ by $\{e_1,e_2,\ldots,e_n\}$. We denote the additive group associated with $V$ by $V^+$, and $\text{id}_{V^+} = 0_V$. The transpose of a vector or matrix $x$ is denoted by $x^T$ and we define $x^{-T} := (x^{-1})^T$. We sometimes denote by $(a_{ij})_{n \times m}$ the
with $a_{ij}$ in the $i$th row and $j$th column. Given a vector space $V$ we denote by $\text{GL}(V)$ the group of all invertible matrices corresponding to linear transformations of $V$. We use the notation of [32] for all classical groups with a few stated exceptions. The linear, symplectic and unitary simple groups are denoted $L_n(q)$, $S_{2m}(q)$ and $U_n(q)$ respectively.

**Permutation groups** Cycle notation $(a_1 \ a_2 \ldots a_n)$ is used for permutations. The symmetric group of all permutations of the set $\Omega$ is denoted by $\text{Sym}(\Omega)$, or $S_n$, where $\Omega = \{1, 2, \ldots, n\}$.

### 1.2.2 Definitions

**Group actions** Let $G$ act on the set $\Omega$. The *(setwise)* stabiliser in $G$ of a subset $\Delta \subset \Omega$ is $G_{\Delta} := \{g \in G : \delta^g \in \Delta, \text{ for all } \delta \in \Delta\}$. This is also written $\text{Stab}_G(\Delta)$. The orbit of $\Delta$ under the action of $G$ is the set $\Delta^g = \{\delta^g : g \in G, \delta \in \Delta\}$. We usually use this exponential notation for group actions. The following theorem is well-known.

**Theorem 1.2.1** *(Orbit-Stabiliser Theorem).* The size of the orbit of $\alpha \in \Omega$ is equal to $|G : G_{\alpha}|$.

The action of $G$ on $\Omega$ is **faithful** if the only element of $G$ which stabilises every element of $\Omega$ pointwise is $\text{id}_G$, in other words, $G$ is isomorphic to a subgroup of $\text{Sym}(\Omega)$. The action of $G$ on $\Omega$ is **transitive** if it has precisely one orbit and **intransitive** otherwise. The action of $G$ is **regular** if it is transitive and $G_{\alpha} = \{\text{id}_G\}$ for all $\alpha \in \Omega$, that is, $|G| = |\Omega|$. When the action is implicit, we will often say that the group itself is faithful, transitive or regular.

The **rank** of $G$ is the number of orbits of a point stabiliser of $G$. We refer to the action of groups $A_n$ and $S_n$ on the set $\{1, \ldots, n\}$ as their **natural action**.

Let $G$ be a group acting on a vector space $V := F_q^n$. Then $V$ is a $G$-module if $(\alpha v + \beta w)^g = \alpha(v^g) + \beta(w^g)$, for all $g \in G$, all $v, w \in V$ and all $\alpha, \beta \in F_q$.

**Group extensions** Let $K \trianglelefteq G$ and suppose $G/K \cong H$. Then $G$ is an extension of $H$ by $K$ and we write $G = H.K$. Let $H$ and $K$ be two groups and fix a homomorphism $\phi : H \rightarrow \text{Aut}(K)$. Let $G := \{(h, k) : h \in H \text{ and } k \in K\}$ and define a product on $G$ as follows

$$(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1^{h_2\phi}k_2)$$

for all $h_1, h_2 \in H$ and $k_1, k_2 \in K$. It is easy to check that $G$ is a group with identity element $(\text{id}_H, \text{id}_K)$ and $(h, k)^{-1} = (h^{-1}, (k^{-1})^{(h\phi)^{-1}})$. The group $G$ is the semidirect product or split extension of $K$ by $H$ (with action $\phi$) and we write $G = K : H$. The following is well-known.
Lemma 1.2.2. Let $G = H \cdot K$, then $H \trianglelefteq G$, $H \cap K = 1$ and each element $g \in G$ can be uniquely expressed in the form $hk$, for some $h \in H$ and some $k \in K$, that is $G = HK$.

Unless otherwise stated, $\phi$ is the conjugation action of $H$ on $K$ and we do not mention it specifically. A group extension which is not split is called non-split and is denoted $H \cdot K$. Let $K \leq \text{Sym}(\Omega)$ where $|\Omega| = m$. The wreath product $H \wr K$ is defined to be $H^m \cdot K$ where $H^m = H \times \cdots \times H$, the $m$th direct power of $H$, and $K$ acts on the $m$ copies of $H$ in the same way that it acts on $\Omega$.

Group structures Let $H \leq G$, then

$$N_G(H) := \{ g \in G : g^{-1}hg \in H, \text{ for all } h \in H \}$$

denotes the normaliser of $H$ in $G$ and

$$C_G(H) := \{ g \in G : gh = hg, \text{ for all } h \in H \}$$

denotes the centraliser of $H$ in $G$.

The automorphism group $\text{Aut}(G)$ is the group of automorphisms of the group $G$. The inner automorphism group $\text{Inn}(G) \leq \text{Aut}(G)$ consists of all automorphisms which are induced by conjugation and $\text{Aut}(G)/\text{Inn}(G) = \text{Out}(G)$, the outer automorphism group of $G$.

A $G$-module $V = \mathbb{F}_q^n$ is reducible if it has a proper non-zero $G$-submodule $W$. A $G$-module which is not reducible is called irreducible. A matrix group whose natural module is reducible (or irreducible) is called a reducible (respectively, irreducible) group. If $G$ is irreducible when acting naturally on $\mathbb{F}_q^n$, for all $e$, then $G$ is absolutely irreducible.

A non-trivial group is simple if it has no proper, non-trivial normal subgroups. A group $G$ is almost simple if

$$\text{Inn}(T) \lhd G \leq \text{Aut}(T),$$

for some non-abelian simple group $T$. Note that $T \cong \text{Inn}(T)$.

Let $G$ be a finite group and suppose

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G,$$

where each composition factor $G_{i+1}/G_i$ is simple. This is a composition series for $G$ and the set of composition factors of a composition series for
$G$ is unique up to isomorphism and permutation, by the Jordan–Hölder Theorem. The group $G$ is soluble if all of its composition factors are abelian and a group which is not soluble is insoluble.

A chief series of $G$ is a finite chain of normal subgroups of $G$

$$1 = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_n = G,$$

such that for $i \in \{1, \ldots, n - 1\}$ there is no normal subgroup $H$ of $G$ such that $N_i < H < N_{i+1}$. The chief factor $N_{i+1}/N_i$ is a minimal non-trivial normal subgroup of $G/N_i$. The set of chief factors of $G$ is unique up to permutation and isomorphism between the factors.

**Aschbacher structures** The following definitions will be referred to when describing the classes of Aschbacher’s theorem.

**Definition 1.2.3.** Let $V := \mathbb{F}_q^n$, then a map $\phi : V \to V$ is semilinear if there exists some $\sigma \in \text{Aut}(\mathbb{F}_q)$ such that

$$(v + w)\phi = v\phi + w\phi$$

and

$$(\lambda v)\phi = (\lambda \sigma)(v\phi)$$

for all $v, w \in V$ and all $\lambda \in \mathbb{F}_q$. The set of all invertible semilinear transformations of $V$ forms $\Gamma L_n(q)$, the semilinear group of $V$.

Note that the field automorphism $\sigma$ is uniquely determined by the map $\phi$.

The Kronecker product of matrices $X$ and $Y$ is defined as follows. Let $X = (x_{ij})$ and $Y = (y_{kl})$ be two square matrices of dimensions $n$ and $m$, respectively. The Kronecker product $X \otimes Y$ is given by

$$X \otimes Y = \begin{pmatrix} x_{11}Y & x_{12}Y & \cdots & x_{1n}Y \\ x_{21}Y & x_{22}Y & \cdots & x_{2n}Y \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1}Y & x_{n2}Y & \cdots & x_{nn}Y \end{pmatrix},$$

where

$$x_{ij}Y = \begin{pmatrix} x_{ij}y_{11} & x_{ij}y_{12} & \cdots & x_{ij}y_{1m} \\ x_{ij}y_{21} & x_{ij}y_{22} & \cdots & x_{ij}y_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ x_{ij}y_{m1} & x_{ij}y_{m2} & \cdots & x_{ij}y_{mm} \end{pmatrix}.$$
where $X := \{(\lambda, \lambda^{-1}) : \lambda \in \mathbb{Z}(H), \lambda^{-1} \in \mathbb{Z}(K)\}$.

Let $\mathbb{F}_r \subset \mathbb{F}_q$ and let $G \leq \text{GL}_n(q)$. If $G$ is conjugate to a subgroup of $\text{GL}_n(r)$ we say that $G$ can be \textit{written over} $\mathbb{F}_r$.

This concludes our notation and definitions. We will repeatedly refer to this section in subsequent chapters.
1.3 The classification of finite simple groups

Simple groups are essentially the building blocks of all groups, since every finite group can be composed from simple groups by using group extensions. The following theorem is one of the most important in finite group theory and is fundamental to our study.

**Theorem 1.3.1** (The Classification of the Finite Simple Groups). Let $G$ be a finite simple group, then $G$ belongs to at least one of the following categories.

1. The cyclic groups $\mathbb{Z}_p$, of prime order $p$: the abelian simple groups.
2. The alternating groups $A_n$, for $n \geq 5$.
3. The simple groups of Lie type: including classical groups and exceptional groups.
4. One of 26 sporadic groups.

The proof of this theorem is the result of work by hundreds of authors, extending over thousands of pages. It will be used throughout the thesis.

The cyclic and alternating groups are well understood and the simple classical groups of Lie type are described in detail in Section 1.5. The exceptional groups are made up of ten families, each of which is derived from a Lie algebra of specific dimension. Using the notation of the ATLAS of Finite Simple Groups [15], the untwisted exceptional groups are:

$$E_6(q), E_7(q), E_8(q), F_4(q) \text{ and } G_2(q),$$

and the twisted exceptional groups are:

$$2B_2(2^{2m+3}), 3D_4(q), 2G_2(3^{2m+3}), 2F_4(2^{2m+3}) \text{ and } 2E_6(q),$$

where $q$ is a prime power and $m \geq 0$. The groups $2B_2(q)$ are also known as the Suzuki groups (Suz$(q)$) and $2F_4(2)'$ is also called the Tits group. The groups $2F_4(2^{2m+3})$ and $2G_2(3^{2m+3})$ are also known as Ree groups of characteristic 2 and 3, respectively.

The 26 sporadic groups are:

$$M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, J_1, J_2, J_3, J_4, Co_1, Co_2, Co_3,$$

$$Fi_{22}, Fi_{23}, Fi'_{24}, HS, McL, He, Ru, Suz, O'N, HN, Ly, Th, B, M.$$

Detailed information on the finite simple groups can be found in [15].
1.4 Schur’s lemma

The following lemma is very important in representation theory. A proof can be found in [34, Theorem 1.4].

**Lemma 1.4.1** (Schur’s lemma). Let \( A : G \to \text{GL}_n(F) \) and \( B : G \to \text{GL}_n(F) \) be two irreducible matrix representations, of dimension \( n \), of a group \( G \) over a (finite or infinite) field \( F \) and suppose there exists a matrix \( L \), such that \( LA(g) = B(g)L \) for all \( g \in G \). Then either \( L = 0 \) or \( L \) is non-singular and hence invertible.

We use Schur’s Lemma 1.4.1 to prove a useful result.

**Corollary 1.4.2.** Let \( G \leq \text{GL}_n(q) \) be absolutely irreducible. Then the centraliser of \( G \) in \( \text{GL}_n(q) \) is \( \mathbb{F}_q^* \), the scalar subgroup of \( \text{GL}_n(q) \).

**Proof.** We apply Lemma 1.4.1 to \( G \) and let \( A = B \). Since \( G \) is absolutely irreducible it is irreducible over the algebraic closure of \( \mathbb{F}_q \), which we write as \( \overline{\mathbb{F}}_q \). Let \( L \in \text{GL}_n(\overline{\mathbb{F}}_q) \) such that \( LA(g) = A(g)L \), for all \( g \in G \). Then since \( \overline{\mathbb{F}}_q \) is algebraically closed, the matrix \( L \) has an eigenvalue; call it \( \lambda \). By definition, \( (L - \lambda I_n) \) is not invertible and for all \( g \in G \)

\[
LA(g) - \lambda A(g) = A(g)L - \lambda A(g)
\]

\[
(L - \lambda I_n)A(g) = A(g)(L - \lambda I_n)
\]

so \( (L - \lambda I_n) = 0 \) by Lemma 1.4.1 and hence \( L \) is a scalar matrix. We deduce that \( C_{\text{GL}_n(\overline{\mathbb{F}}_q)}(G) \leq \mathbb{F}_q^* \) and therefore

\[
C_{\text{GL}_n(q)}(G) = C_{\text{GL}_n(\overline{\mathbb{F}}_q)}(G) \cap \text{GL}_n(q) \leq \mathbb{F}_q^*.
\]

Note that \( \lambda I_n \) centralises \( G \), for all \( \lambda \in \mathbb{F}_q^* \), and hence \( C_{\text{GL}_n(q)}(G) = \mathbb{F}_q^* \). \( \Box \)

This result will be used numerous times in the chapters to come.
1.5 The classical groups

1.5.1 Introduction

The simple classical groups form part of one of the families of groups given in the Classification of Finite Simple Groups, Theorem 1.3.1. In this section we introduce some more general notation and definitions, before describing the classical groups and then the simple classical groups. We give some facts relating to these groups which will be needed in later chapters.

Throughout this chapter, \( n \) is a positive integer, \( q \) is a prime power and \( V := \mathbb{F}_q^n \).

1.5.2 Forms

A classical group consists of matrices which preserve a classical form. We now define some forms and explain what it means for a group to preserve a form.

Definition 1.5.1. A sesquilinear form is a map \( f : V \times V \to \mathbb{F}_q \) such that for all \( v, v_1, v_2, w, w_1, w_2 \in V \), for all \( \lambda, \mu \in \mathbb{F}_q \) and for some fixed \( \sigma \in \text{Aut}(\mathbb{F}_q) \) the following hold:

1. \((v_1 + v_2, w)f = (v_1, w)f + (v_2, w)f, \)
2. \((v, w_1 + w_2)f = (v, w_1)f + (v, w_2)f, \)
3. \((\lambda v, w)f = \lambda (v, w)f, \)
4. \((v, \mu w)f = \mu \sigma (v, w)f. \)

A form \( f : V \times V \to \mathbb{F}_q \) is bilinear if it is linear in both variables. This is a special case of the sesquilinear form where \( \sigma \) is the identity map. A form \( f : V \times V \to \mathbb{F}_q \) is symmetric if \((v, w)f = (w, v)f\) for all \( v, w \in V \).

The group \( G \leq \text{GL}_n(q) \) preserves a sesquilinear form \( f \) if \((vg, wg)f = (v, w)f\) for all \( v, w \in V \) and all \( g \in G \). We say \( G \) preserves \( f \) up to scalar multiplication if for each \( g \in G \) there exists \( \lambda \in \mathbb{F}_q^* \) such that \((vg, wg)f = \lambda (v, w)f. \)

Fix a sesquilinear form \( f \) and let \( \{e_1, e_2, \ldots, e_n\} \) be the standard basis for \( V \)

\[
\{(1, 0, \ldots, 0), (0, 1, \ldots, 0), \ldots, (0, 0, \ldots, 1)\}.
\]

We can represent \( f \) by the matrix \( F := ((e_i, e_j)f)_{n \times n} \). This is the \( n \times n \) matrix with \((i, j)\)th entry \((e_i, e_j)f\).

Let \( w \in V \) and let \( \sigma \in \text{Aut}(\mathbb{F}_q) \). Suppose \( w = (b_1, b_2, \ldots, b_n) \), for some \( b_i \in \mathbb{F}_q \), then we define \( w\sigma = (b_1\sigma, b_2\sigma, \ldots, b_n\sigma) \).

Lemma 1.5.2. Let \( v, w \in V \) and \( \sigma \) be the automorphism of \( \mathbb{F}_q \) associated with \( f \). Then \( vF(w)F^T = (v, w)f \).
Proof. Let \( v = (a_1, a_2, \ldots, a_n) \) and \( w = (b_1, b_2, \ldots, b_n) \) and note that \( w^T \sigma = (w \sigma)^T \). The matrix \( F \) is

\[
\begin{pmatrix}
(e_1, e_1)f & (e_1, e_2)f & \cdots & (e_1, e_n)f \\
(e_2, e_1)f & (e_2, e_2)f & \cdots & (e_2, e_n)f \\
\vdots & \vdots & \ddots & \vdots \\
(e_n, e_1)f & (e_n, e_2)f & \cdots & (e_n, e_n)f
\end{pmatrix}
\]

We refer to the conditions given in Definition 1.5.1.

\[
vF(w \sigma)^T = (a_1, \ldots, a_n)F(w^T \sigma)
\]

\[
= \left( \sum_{i=1}^n a_i (e_i, e_1)f, \ldots, \sum_{i=1}^n a_i (e_i, e_n)f \right) (w^T \sigma)
\]

\[
= \left( \sum_{i=1}^n a_i e_i, e_1)f, \ldots, \sum_{i=1}^n a_i e_i, e_n)f \right) (w^T \sigma) \quad \text{by conditions 1 and 3.}
\]

\[
= ((v, e_1)f, \ldots, (v, e_n)f) (w^T \sigma)
\]

\[
= \sum_{j=1}^n b_j \sigma (v, e_j)f
\]

\[
= (v, \sum_{j=1}^n b_j e_j)f \quad \text{by condition 4.}
\]

\[
= (v, w)f.
\]

The form \( f \) and its associated matrix \( F \) uniquely determine one another and we say that \( F \) is the matrix of \( f \). Let \( \sigma \in \text{Aut}(F_q) \) and let \( g \in \text{GL}_n(q) \), then we write \( g \sigma \) for the matrix obtained by applying \( \sigma \) to the entries of \( g \).

Lemma 1.5.3. Suppose \( G \leq \text{GL}_n(q) \) preserves the form \( f \), then \( gF(g^T \sigma) = F \), for all \( g \in G \).

Proof. Note that \((g \sigma)^T = g^T \sigma \). Let \( v, w \in V \), then

\[
v(gFg^T \sigma)(w^T \sigma) = vgF(wg)^T \sigma
\]

\[
= (vg, wg)f
\]

\[
= (v, w)f,
\]

so \( gF(g^T \sigma) = F \), since \( F \) is uniquely determined by \( f \).

Similarly, \( G \) preserves \( f \) up to scalar multiplication if and only if there exists \( \lambda \in F_q \) such that \( gFg^T \sigma = \lambda F \) for all \( g \in G \). We now define another type of form.
Definition 1.5.4. The map $Q : V \to \mathbb{F}_q$ is a quadratic form if there exists a symmetric bilinear form $f_Q$ such that for all $v, w \in V$

$$(v, w)f_Q = (v + w)Q - vQ - wQ,$$

and $(\lambda v)Q = \lambda^2(vQ)$ for all $v \in V$ and all $\lambda \in \mathbb{F}_q$. The form $f_Q$ is the associated symmetric form of $Q$.

When $q$ is odd, $Q$ is uniquely determined by $f_Q$, since

$$(v, v)f_Q = (v + v)Q - 2(vQ) = (2v)Q - 2(vQ) = 2(vQ).$$

We can deduce from the quadratic form $Q$ a matrix $M_Q = (m_{ij})_{n \times n}$ such that for all $v \in V$

$$vQ = vM_Qv^T,$$

however there are many possible choices for $M_Q$, so it is useful to define a standardised version.

Let $M := (m_{ij})_{n \times n}$ and $M' := (m'_{ij})_{n \times n}$ be two matrices representing the form $Q$ and let $v = (a_1, a_2, \ldots, a_n)$, then

$$vQ = \sum_{j=1}^{n} \sum_{i=1}^{n} a_im_{ij}a_j = \sum_{j=1}^{n} \sum_{i=1}^{n} a_im'_{ij}a_j,$$

so $m_{ii} = m'_{ii}$ for all $i$ and $m_{ij} + m_{ji} = m'_{ij} + m'_{ji}$ for all $i, j$. We standardise $M_Q$ to the unique upper triangular matrix $M^*_Q = (m^*_{ij})_{n \times n}$ given by

$$m^*_{ij} = \begin{cases} m_{ii} & i = j \\ m_{ij} + m_{ji} & i < j \\ 0 & i > j, \end{cases}$$

then $vM^*_Qv^T = vM_Qv^T$.

As in the sesquilinear case, a group $G \leq \text{GL}_n(q)$ preserves the quadratic form $Q : V \to \mathbb{F}_q$ if and only if $vQ = (vg)Q$ for all $v \in V$ and all $g \in G$. Then $(vg)M^*_Q(vg)^T = vM^*_Qv^T$ and hence

$$(gM^*_Qg^T)^* = (gM_Qg^T)^* = M^*_Q,$$

for all $g \in G$.

Lemma 1.5.5. Let $Q$ be a quadratic form with associated matrix $M_Q$ and let $M^*_Q$ be as defined above. Then $v(M^*_Q + M^*_Q^T)w^T = (v, w)f_Q$, the associated symmetric form of $Q$. 

12
Proof. First consider

\[(v + w)Q = (v + w)M_Q(v + w)^T\]
\[= (v + w)M_Q(v^T + w^T)\]
\[= vM_Qv^T + vM_Qw^T + wM_Qv^T + wM_Qw^T.\]

Therefore

\[(v, w)f_Q = (v + w)Q - vQ - wQ\]
\[= vM_Qw^T + wM_Qv^T\]
\[= vM_Qw^T + (wM_Qv^T)^T \quad \text{since } wM_Qv^T \text{ is a scalar value}\]
\[= vM_Qw^T + vM_Q^Tw^T\]
\[= v(M_Q + M_Q^T)w^T\]
\[= v(M_Q^* + M_Q^{*T})w^T,\]

since \(M_Q + M_Q^T = M_Q^* + M_Q^{*T}\). Thus the claim is proved.

The next definition gives a criterion for a form to be “well-behaved”.

**Definition 1.5.6.** A sesquilinear form \(f\) is **non-degenerate** if

- for each \(0 \neq v \in V\) there exists \(w \in V\) such that \((v, w)f\) is non-zero, and
- for each \(0 \neq w \in V\) there exists \(v \in V\) such that \((v, w)f\) is non-zero.

A quadratic form is non-degenerate if its associated symmetric form is non-degenerate.

A sesquilinear form is **reflexive** if

\[(v, w)f = 0 \quad \text{if and only if} \quad (w, v)f = 0.\]

It can be shown that there are essentially only three different types of reflexive non-degenerate sesquilinear forms: symmetric bilinear, symplectic and unitary. See, for example, [69, Theorem 7.1]. We now introduce the classical groups along with the forms they preserve.

1.5.3 Linear

The **general linear group** \(\text{GL}_n(q)\) consists of all invertible \(n \times n\) matrices with entries in \(\mathbb{F}_q\). This group preserves the trivial bilinear form \((v, w)f = 0\) for all \(v, w \in V\).

There is a chain of subgroups

\[\text{SL}_n(q) \leq \text{GL}_n(q) \leq \Gamma \text{L}_n(q) \leq \Gamma \text{L}2_n(q).\]
The special linear group $\text{SL}_n(q)$ is the subgroup of $\text{GL}_n(q)$ consisting of matrices of determinant 1. Recall from Definition 1.2.3 that the group $\Gamma L_n(q)$ consists of all invertible semilinear transformations of $V$. When $n \geq 3$ the group $\text{SL}_n(q)$ admits an inverse transpose automorphism, $\iota \in \text{Aut}(V)$, given by $g\iota = g^{-T}$ for all $g \in \text{GL}_n(q)$. We define the group $\Gamma L_2^n(q) := \{ \Gamma L_n(q) : \langle \iota \rangle \}$.

The order of $\text{GL}_n(q)$ is $q^{n(n-1)/2} \prod_{i=1}^{n}(q^i - 1)$. Let $e$ be the integer such that $q = p^e$, for prime $p$, and let $n \geq 2$. Table 1.1 gives the indices of the linear-type groups in relation to each other. For proofs, see [32, Section 2.2].

| $\text{GL}_n(q) : \text{SL}_n(q)$ | $q - 1$ |
| $\Gamma L_n(q) : \text{GL}_n(q)$ | $e$ |
| $\Gamma L_2^n(q) : \Gamma L_2^n(q)$ | 1 if $n = 2$ |
| | 2 otherwise |

1.5.4 Symplectic

Definition 1.5.7. The bilinear form $f$ is symplectic if, for all $v, w \in V$

- $(v, w)f = -(w, v)f$, that is, $f$ is skew symmetric;
- $(v, v)f = 0$.

Let $f$ be a non-degenerate symplectic form on $V$, then the symplectic group $\text{Sp}_n(q) \leq \text{GL}_n(q)$ consists of all $g \in \text{GL}_n(q)$ which preserve $f$. The dimension $n$ is always even, so we often write $\text{Sp}_{2m}(q)$. The elements of $\text{Sp}_n(q)$ all have determinant 1 by [2, 22.4], so in fact $\text{Sp}_n(q) \leq \text{SL}_n(q)$. Note that given any two non-degenerate symplectic forms, their associated symplectic groups are conjugate in $\text{GL}_n(q)$.

There is a chain of subgroups

$$\text{Sp}_n(q) \leq \text{CSp}_n(q) \leq \Gamma \text{Sp}_n(q).$$

The conformal symplectic group $\text{CSp}_n(q)$ (sometimes called $\text{GSp}_n(q)$) is the set of $g \in \text{GL}_n(q)$ which preserve $f$ up to scalar multiplication and $\text{CSp}_n(q)$ is the normaliser in $\text{GL}_n(q)$ of $\text{Sp}_n(q)$. The group $\Gamma \text{Sp}_n(q)$ is the set of $g \in \Gamma L_n(q)$ which preserve $f$ up to automorphisms of $\mathbb{F}_q$.

The order of $\text{Sp}_{2m}(q)$ is $q^{m^2} \prod_{i=1}^{m}(q^{2i} - 1)$. Let $e$ be the integer such that $q = p^e$ for prime $p$. By [32, Section 2.4], the indices of the symplectic-type groups in relation to each other are given in Table 1.2.
Table 1.2: Indices of the symplectic-type groups

<table>
<thead>
<tr>
<th>CSp_{2m}(q) : Sp_{2m}(q)</th>
<th>q - 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>ΓSp_{2m}(q) : CSp_{2m}(q)</td>
<td>e</td>
</tr>
</tbody>
</table>

1.5.5 Unitary

The field \( \mathbb{F}_q \) has an extension field \( \mathbb{F}_{q^2} \) of degree 2, which is unique up to isomorphism. Let \( \sigma \in \text{Aut}(\mathbb{F}_{q^2}) \) such that \( \sigma : \lambda \mapsto \lambda^q \). Then \( \sigma \) has order 2.

**Definition 1.5.8.** Let \( \sigma \) be defined as above. The sesquilinear form \( f : V \times V \rightarrow \mathbb{F}_{q^2} \) is unitary if, for all \( v, w \in V \)

\[
(v, w)f = ((w, v)f)\sigma.
\]

Let \( f \) be a non-degenerate unitary form on \( V \), then the general unitary group \( \text{GU}_n(q) \) is the set of \( g \in \text{GL}_n(q^2) \) which preserve \( f \). (Note that some authors write this group as \( \text{GU}_n(q^2) \).) Again, given two non-degenerate unitary forms their associated general unitary groups are conjugate in \( \text{GL}_n(q^2) \).

There is a chain of subgroups

\[
\text{SU}_n(q) \leq \text{GU}_n(q) \leq \text{CU}_n(q) \leq \Gamma\text{U}_n(q).
\]

The special unitary group \( \text{SU}_n(q) \leq \text{SL}_n(q^2) \) contains the elements of \( \text{GU}_n(q) \) with determinant 1. The subgroup of \( \text{GU}_n(q) \) which preserves \( f \) up to scalar multiplication is the conformal unitary group \( \text{CU}_n(q) \) and this is the normaliser in \( \text{GL}_n(q^2) \) of \( \text{SU}_n(q) \). The group \( \Gamma\text{U}_n(q) \) consists of the elements of \( \Gamma\text{GL}_n(q^2) \) which preserve \( f \) up to field automorphism.

The group \( \text{GU}_n(q) \) has order \( q^{n(n-1)/2} \prod_{i=1}^{n}(q^i - (-1)^i) \). Let \( e \) be the integer such that \( q = p^e \), for prime \( p \), then Table 1.3 gives the indices of the unitary-type groups with relation to each other. Proof of this can be found in [32, Section 2.3].

Table 1.3: Indices of the unitary-type groups

<table>
<thead>
<tr>
<th>( \text{GU}_n(q) : \text{SU}_n(q) )</th>
<th>( q + 1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \text{CU}_n(q) : \text{GU}_n(q) )</td>
<td>( q - 1 )</td>
</tr>
<tr>
<td>( \Gamma\text{U}_n(q) : \text{CU}_n(q) )</td>
<td>( 2e )</td>
</tr>
</tbody>
</table>
1.5.6 Orthogonal

Let $Q$ be a quadratic form on $V$ with associated symmetric form $f_Q$. When $n$ is even there are two distinct types of non-degenerate quadratic forms. The even dimensional form types may be distinguished by the dimension $d$ of the maximal subspace $W \leq V$ such that $wQ = 0$, for all $w \in W$ (that is, $W$ is totally singular). We define the sign of a quadratic form $Q$ to be

\[ \epsilon = \begin{cases} + & \text{if } n \text{ is even and } d = n/2 \smallskip \text{−} & \text{if } n \text{ is even and } d = n/2 - 1 \end{cases} \]

In odd dimensions the sign $\circ$ shall be omitted when the meaning is clear.

Note that when $q$ is even, $f_Q$ is a symplectic form and hence $n$ is even.

Let $Q$ be a non-degenerate quadratic form on $V$, then the set of $g \in \text{GL}_n(q)$ preserving $Q$ is the general orthogonal group $\text{GO}_n(q)$, where $\epsilon \in \{\circ, +, −\}$, according to the sign of the form. There is a chain of subgroups

\[ \Omega_n(q) \leq \text{SO}_n(q) \leq \text{GO}_n(q) \leq \text{CO}_n(q) \leq \Gamma_{\text{GO}}(q). \]

The special orthogonal group is the subgroup $\text{SO}_n(q) \leq \text{GO}_n(q)$ consisting of elements with determinant 1. There is a unique subgroup $\Omega_n(q)$ of $\text{SO}_n(q)$ of index 2, except when $(n, q, \epsilon) = (4, 2, +)$. In the excepted case, $\Omega_n^+(2)$ is one of three subgroups of $\text{SO}_n^+(2)$ of index 2 (see [32, Proposition 2.5.9] for details). The conformal orthogonal group $\text{CO}_n(q)$ preserves $Q$ up to scalar multiplication and is the normaliser in $\text{GL}_n(q)$ of $\Omega_n(q)$. The group $\Gamma_{\text{GO}}(q)$ preserves $Q$ up to scalars and field automorphisms.

**Odd dimension**

\[ |\text{GO}_{2m+1}(q)| = 2q^{m^2} \prod_{i=1}^{m} (q^{2i} - 1). \]

Let $e$ be the integer such that $q = p^e$, for prime $p$, then Table 1.4 gives the indices of the orthogonal-type groups in odd dimension, in relation to each other, as proved in [32, Section 2.6].

**Even dimension**

\[ |\text{GO}_{2m}^\pm(q)| = 2q^{m(m-1)}(q^m \mp 1) \prod_{i=1}^{m-1} (q^{2i} - 1). \]

Let $e$ be the integer such that $q = p^e$, for prime $p$, then Table 1.5 gives the indices of the orthogonal-type groups in even dimension, in relation to each other. See [32, Sections 2.7 and 2.8] for proof.
Table 1.4: Indices of the orthogonal-type groups in odd dimension

| SO_{2m+1}(q) : \Omega_{2m+1}(q) | 1 if \( m = 0 \) 
| \hspace{1em} \| \hspace{1em} 2 otherwise |
| GO_{2m+1}(q) : SO_{2m+1}(q) | 2 |
| CO_{2m+1}^\epsilon(q) : GO_{2m+1}(q) | \frac{1}{2}(q - 1) |
| \Gamma O_{2m+1}(q) : CO_{2m+1}^\epsilon(q) | e |

Table 1.5: Indices of the orthogonal-type groups in even dimension

| SO_{\pm 2m}(q) : \Omega_{\pm 2m}(q) | 2 |
| GO_{\pm 2m}(q) : SO_{\pm 2m}(q) | (2, q - 1) |
| CO_{\pm 2m}(q) : GO_{\pm 2m}(q) | q - 1 |
| \Gamma O_{\pm 2m}(q) : CO_{\pm 2m}(q) | e |

1.5.7 The simple classical groups

The family of simple classical groups introduced in Theorem 1.3.1 consists of the simple projective classical groups. We now describe the projective classical groups and explain which of them are not simple. Let \( Z := Z(\text{GL}_n(q)) \) and recall that \( Z \cong \mathbb{F}_q^* \). A group \( G \) is quasisimple if it is perfect and \( G/Z(G) \) is non-abelian simple. The quasisimple classical groups consist of \( \text{SL}_n(q), \text{Sp}_n(q), \text{SU}_n(q), \Omega_n^\epsilon(q) \) and \( \Omega_n^{\pm}(q) \), with the exception of certain small values of \( n \) and \( q \), given in Theorem 1.5.11.

**Definition 1.5.9.** For any group \( G \leq \text{GL}_n(q) \) we write \( PG := G/(G \cap Z) \) for the projective group associated with \( G \). Equivalently, \( PG \) represents the group \( G \) reduced modulo scalars.

The projective general linear group is denoted \( \text{PGL}_n(q) := \text{GL}_n(q)/Z \) and the projective special linear group is \( \text{PSL}_n(q) := \text{SL}_n(q)/(\text{SL}_n(q) \cap Z) \). This is usually denoted simply \( L_n(q) \) and the projective versions of \( \text{Sp}_n(q), \text{SU}_n(q) \) and \( \Omega_n^\epsilon(q) \) for \( \epsilon \in \{\circ, +, -\} \) are respectively denoted \( S_n(q), U_n(q) \) and \( \Omega_n^\epsilon(q) \).

The centres of the quasisimple classical groups given here for reference. For proof, see [15]. Note that \( x - \epsilon = x - 1 \) or \( x + 1 \), accordingly as \( \epsilon = + \) or \( - \).

**Lemma 1.5.10.** Let \( G \leq \text{GL}_n(q) \) be a quasisimple classical group, then the centre of \( G \) is given in the following table.
The following theorem is well-known. See, for example [32, Proposition 2.9.1].

\textbf{Theorem 1.5.11.} The following classical groups are not simple: 
\( L_2(q) \) for \( q \leq 3 \), \( \Omega_5^+(q) \), \( \Omega_4^+(q) \), \( U_3(2) \). With the exception of these and (possibly isomorphic) groups given below, all groups \( \text{L}_n(q) \), \( \text{S}_n(q) \), \( \text{U}_n(q) \) and \( \Omega_n^\epsilon(q) \) (where \( \epsilon \in \{+, -, \circ\} \)) are simple. Furthermore, the list below includes all isomorphisms between pairs of classical or alternating groups.

\[ \begin{array}{ll}
L_2(4) & \cong L_2(5) \\
L_2(9) & \cong S_4(2) \\
U_2(q) & \cong S_2(q) = L_2(q) \\
\Omega_{2m+1}^0(2^e) & \cong S_{2m}(2^e), e \geq 1 \\
\Omega_5(q) & \cong S_4(q), q \text{ odd} \\
\Omega_6^\epsilon(q) & \cong L_4(q) \\
\Omega_6^\epsilon(q) & \cong L_2(q^2) \\
\end{array} \]

We usually treat the above groups as the right hand side of the isomorphism. The following theorem is another standard fact.

\textbf{Theorem 1.5.12.} Let \( G \) be one of \( \{ \text{L}_n(q), \text{S}_n(q), \text{U}_n(q), \Omega_n^\epsilon(q) \} \) and let \( n \) and \( q \) be such that \( G \) is simple. Then the full automorphism group of \( G \) is \( \{ \text{PGL}_n(q), \text{PSp}_n(q), \text{PGL}_n(q), \text{PO}_n^\epsilon(q) \} \), respectively, except when \( G = S_4(q) \), with \( q \) even, and when \( G = \Omega_8^\epsilon(q) \).

The excepted groups each admit an extra automorphism such that

\[ |\text{Aut}(S_4(q)) : \text{PSp}_4(q)| = 2 \]

and

\[ |\text{Aut}(\Omega_8^\epsilon(q)) : \text{PO}_8^\epsilon(q)| = 3. \]

We now give the outer automorphism groups \( \text{Out}(G) := \text{Aut}(G) / \text{Inn}(G) \) of the simple classical groups \( G \), for future reference.

\textbf{Theorem 1.5.13.} Let \( G \) be a simple classical group and let \( q = p^f \) for some prime \( p \). Then the structure of \( \text{Out}(G) \) is given in Table 1.6.
Table 1.6: Outer automorphism groups of classical groups $G$

<table>
<thead>
<tr>
<th>$G$</th>
<th>$\text{Out}(G)$</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$L_n(q)$</td>
<td>$\mathbb{Z}_{(n,q-1)} : \mathbb{Z}_f : \mathbb{Z}_2$</td>
<td>$n \geq 3$</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}_{(2,q-1)} \times \mathbb{Z}_f$</td>
<td>$n = 2$</td>
</tr>
<tr>
<td>$S_{2m}(q)$</td>
<td>$\mathbb{Z}_f$</td>
<td>$q$ even</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_f$</td>
<td>$q$ odd</td>
</tr>
<tr>
<td>$U_n(q)$</td>
<td>$\mathbb{Z}_{(n,q+1)} : \mathbb{Z}_2f$</td>
<td></td>
</tr>
<tr>
<td>$\text{PΩ}_{2m+1}(q)$</td>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_f$</td>
<td>$q$ odd, $m \geq 1$</td>
</tr>
<tr>
<td>$\text{PΩ}_{2m}^+(q)$</td>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_f$</td>
<td>$q$ even</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_f$</td>
<td>$q$ odd, $m(q-1)/2$ odd</td>
</tr>
<tr>
<td></td>
<td>$D_8 \times \mathbb{Z}_f$</td>
<td>$q$ odd, $m(q-1)/2$ even</td>
</tr>
<tr>
<td>$\text{PΩ}_{2m}^-(q)$</td>
<td>$\mathbb{Z}_2f$</td>
<td>$q$ even</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_2f$</td>
<td>$q$ odd, $m(q-1)/2$ even</td>
</tr>
<tr>
<td></td>
<td>$D_8 \times \mathbb{Z}_f$</td>
<td>$q$ odd, $m(q-1)/2$ odd</td>
</tr>
</tbody>
</table>

Proof. See [32, Sections 2.2–2.8].

In Part II of this work it will be useful to know precisely which quasisimple classical groups are soluble. The following result is taken from [32, Proposition 2.9.2]

Lemma 1.5.14. Let $G$ be one of $\text{SL}_n(q)$, $\text{Sp}_n(q)$, $\text{SU}_n(q)$ or $\text{Ω}_n(q)$. Then $G$ is soluble if and only if either $n = 1$ or $G$ is one of $\text{SL}_2(2)$, $\text{SL}_2(3)$, $\text{Sp}_2(2)$, $\text{Sp}_2(3)$, $\text{SU}_2(2)$, $\text{SU}_2(3)$, $\text{Ω}_2^+(q)$, $\text{SU}_3(2)$, $\text{Ω}_3(3)$, $\text{Ω}_3^+(2)$ or $\text{Ω}_3^+(3)$.

This concludes our introduction to the classical groups and their properties. This section will be referred to numerous times in the following chapters.
1.6 Aschbacher’s theorem

Let $G$ be a classical group, then Aschbacher’s theorem [1] states that a maximal subgroup of $G$ lies in at least one of nine classes. This theorem is an important tool for the Matrix Group Recognition Project, as it enables us to break down a matrix group problem into cases. Here we restrict our interest to groups $G \leq \text{GL}_n(q)$ and state a version of Aschbacher’s theorem which classifies all subgroups of $G$, including those which are non-maximal. We give a brief description of the nine Aschbacher classes, though more details of class $C_i$ where $i \in \{1, 2, 3, 5, 8\}$ can be found in Part II. Throughout, let $n$ be a positive integer, let $q$ be a prime power and let $V$ be the vector space $F_q^n$.

**Theorem 1.6.1** (Aschbacher’s theorem). A subgroup $G \leq \text{GL}_n(q)$ belongs to at least one of the classes $C_1$ to $C_9$, which are defined below.

We now give a brief description of each Aschbacher class $C_i$. For $1 \leq i \leq 8$ there is a geometric structure associated with $C_i$, and we present the full stabiliser in $\text{GL}_n(q)$ of this structure.

1.6.1 $C_1$: Reducible

Aschbacher class $C_1$ consists of reducible groups. Recall that a group $G$ acts reducibly on $V$ if there exists a proper non-trivial subspace $W$ of $V$ such that $Wg = W$ for all $g \in G$.

Let $M$ be the full stabiliser in $\text{GL}_n(q)$ of some subspace $W$ and let

$$\{e_1, e_2, \ldots, e_n\} := \{(1,0,\ldots,0), (0,1,0,\ldots,0), \ldots, (0,0,\ldots,0,1)\}$$

be the standard basis for $V$. Fix $1 \leq k < n$ and let $W = \langle e_1, \ldots, e_k \rangle$, then there exists some $c \in \text{GL}_n(q)$ such that $M^c$ consists of matrices of the form

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

where $A \in \text{GL}_k(q)$, $B \in \text{GL}_{n-k}(q)$ and $X$ is an arbitrary $(n-k) \times k$ matrix with entries in $F_q$. The group $M^c$ has the structure

$$F_q^{k(n-k)} : (\text{GL}_k(q) \times \text{GL}_{n-k}(q)).$$

If a group is not in $C_1$, then it is irreducible.

1.6.2 $C_2$: Imprimitive

Aschbacher class $C_2$ consists of irreducible groups which act imprimitively on $V$. A group $G$ is imprimitive if there exists a direct sum decomposition of $V$ into subspaces of equal dimension:
\[ V = W_1 \oplus W_2 \oplus \cdots \oplus W_t, \]

such that for all \( g \in G \), and all \( 1 \leq i \leq t \), there exists some \( 1 \leq j \leq t \) satisfying \( W_i g = W_j \). We call the set \( \{ W_1, \ldots, W_t \} \) a system of blocks for \( G \).

Let \( \dim(W_i) = k \), then the full stabiliser in \( \text{GL}_n(q) \) of the vector space decomposition is isomorphic to \( \text{GL}_k(q) \wr \text{S}_t \), where \( \text{S}_t \) acts on \( \text{GL}_k(q) \) by permuting the blocks.

1.6.3 \( C_3 \): Semilinear

Recall from Definition 1.2.3 that group of all semilinear automorphisms of the vector space \( \mathbb{F}_q^n \) is denoted by \( \Gamma \text{L}_n(q) \). Let \( s > 1 \) be a proper divisor of \( n \), then we can realise \( V \) as a \( n/s \)-dimensional vector space over \( \mathbb{F}_q^s \) by choosing an \( \mathbb{F}_q \)-basis of the field extension \( \mathbb{F}_q^s \). If the elements of \( G \) act on \( V \) as semilinear automorphisms of this \( n/s \)-dimensional space, then \( G \) is isomorphic to a subgroup of \( \Gamma \text{L}_{n/s}(q^s) \).

Aschbacher class \( C_3 \) consists of irreducible groups which act as semilinear automorphisms on \( V = \mathbb{F}_q^{n/s} \). The full stabiliser in \( \text{GL}_n(q) \) of \( \mathbb{F}_q^{n/s} \) is isomorphic to \( \Gamma \text{L}_{n/s}(q^s) \).

The remaining Aschbacher classes contain only absolutely irreducible groups.

1.6.4 \( C_4 \): Tensor Product

We give only a brief description of this class as it does not feature heavily in our work. An absolutely irreducible group \( G \) lies in \( C_4 \) if it preserves a tensor decomposition \( V := V_1 \otimes V_2 \). The spaces \( V_1, V_2 \) have dimensions \( n_1, n_2 > 1 \), respectively, where \( n_1 n_2 = n \) and \( n_1 \neq n_2 \) (recall the definition of the Kronecker product from Section 1.2).

A \( C_4 \)-group \( G \) is a central product (see Section 1.2) of absolutely irreducible groups \( H \leq \text{GL}(V_1) \) and \( K \leq \text{GL}(V_2) \), which can be constructed as a Kronecker product. The full stabiliser in \( \text{GL}_n(q) \) of the tensor decomposition is \( \text{GL}(V_1) \circ \text{GL}(V_2) \).

1.6.5 \( C_5 \): Subfield

Let \( G \) be an absolutely irreducible group, then \( G \) belongs to \( C_5 \) if there exists a proper subfield \( \mathbb{F}_{q_0} \subset \mathbb{F}_q \), where \( q = q_0^r \) for some prime \( r \), such that \( G \) is conjugate to a subgroup of \( \text{GL}_n(q_0)\mathbb{F}_q^* \). In other words, there exists some \( t \in \text{GL}_n(q) \) and some elements \( (\beta_g)_{g \in G} \) of \( \mathbb{F}_q^* \) such that \( \beta_g t^{-1} g t \in \text{GL}_n(q_0) \) for all \( g \in G \). The full stabiliser in \( \text{GL}_n(q) \) of \( \mathbb{F}_q^* \) is \( \text{GL}_n(q_0)\mathbb{F}_q^* \).
1.6.6 \( C_6 \): Extraspecial Normaliser

Let \( \Phi(G) \) denote the Frattini subgroup of \( G \).

**Definition 1.6.2.** A \( p \)-group \( G \), for prime \( p \), is **extraspecial** if \( Z(G) = \Phi(G) = G' \) and the group \( Z(G) \) has order \( p \).

More details about the extraspecial groups, including the following facts, can be found in [59, Section 5.3]. An extraspecial \( p \)-group \( G \) is a central product of \( m \) non-abelian subgroups of order \( p^3 \), and has order \( p^{2m+1} \). Conversely, a finite central product of non-abelian groups of order \( p^3 \) is an extraspecial group. For any prime \( p \) and \( m \geq 1 \) there are two isomorphism types of extraspecial \( p \)-groups of order \( p^{1+2m} \). When \( p \) is odd they have exponents \( p \) and \( p^2 \). When \( p = 2 \) they consist of either a central product of \( m \) copies of the dihedral group \( D_8 \), denoted by \( 2^{1+2m} \), or \( m - 1 \) copies of \( D_8 \) and one copy of the quaternion group \( Q_8 \), denoted by \( 2^{1+2m} \).

**Definition 1.6.3.** An absolutely irreducible group \( G \) lies in Aschbacher class \( C_6 \) if \( E \unlhd G \leq N_{GL_n(q)}(E) \), for some extraspecial \( p \)-group \( E \).

Let \( E \) be an extraspecial group, then the full stabiliser in \( GL_n(q) \) of \( E \) is \( N_{GL_n(q)}(E) \). We now describe the normalisers of the extraspecial groups.

**Lemma 1.6.4.** Let \( G \leq GL_n(q) \) be a \( p \)-group in \( C_6 \), then one of the following is true:

- \( p \) is odd, \( q \equiv 1 \mod p \) and \( G \) normalises an extraspecial \( p \)-group of order \( p^{1+2m} \).
  \[ p^{1+2m} \leq G \leq p^{1+2m}.Sp_{2m}(p).\mathbb{F}_q^*. \]

- \( p = 2 \), \( q \equiv 1 \mod 4 \) and \( G \) normalises a 2-group of symplectic type.
  \[ 2^{1+2m} \leq G \leq \mathbb{F}_q^* \circ (4 \circ 2^{1+2m}).Sp_{2m}(2), \text{ where } \epsilon \in \{+,-\}. \]

- \( n = 2 \), \( q \equiv 3 \mod 4 \) and \( G = 2^{1+2}.O_2^-(2).\mathbb{F}_q^* \).

We will occasionally refer to extraspecial groups using the notation given here.

1.6.7 \( C_7 \): Tensor Induced

Let \( G \) be an absolutely irreducible group, then \( G \) is in \( C_7 \) if it preserves a decomposition of \( V \) as a symmetric tensor product \( V_1 \otimes \cdots \otimes V_t \) with \( t > 1 \), \( n = m^t \) and \( \dim(V_i) = m \) for all \( i \). The action of \( G \) permutes the components of the product transitively and \( G/Z(G) \leq PGL_t(q)/S_t \). The full stabiliser in \( GL_n(q) \) of this decomposition has the form

\[ (GL_m(q) \otimes \cdots \otimes GL_m(q)): S_t. \]
1.6.8 $C_8$: Classical

The simple classical groups are given in Theorem 1.5.11. An absolutely irreducible group $G$ lies in class $C_8$ if there is a quasisimple classical group $C$ in its natural representation such that

$$C \leq G \leq N_{\text{GL}_n(q)}(C).$$

The stabiliser in $\text{GL}_n(q)$ of $C$ is $N_{\text{GL}_n(q)}(C)$, the form of which can be found in Section 1.5.

Note that some authors define $C_8$ to consist of all groups preserving a non-degenerate form, up to scalar multiplication, and also all groups containing $\text{SL}_n(q)$. In Chapter 13 we also consider a class $C'_8$ which is related to $C_8$ and consists of all absolutely irreducible groups which preserve a non-degenerate, non-trivial classical form.

1.6.9 $C_9$: Almost Simple

Aschbacher class $C_9$ consists of groups $G$ satisfying the following conditions. There exists a non-abelian simple group $T$ such that $T \leq G/Z \leq \text{Aut}(T)$ and the normal subgroup $Z.T$ is absolutely irreducible, preserves no non-degenerate classical form, is not in $C_5$ and does not contain $\text{SL}_n(q)$.

1.6.10 Common variants on the theorem

Aschbacher's theorem is widely used as a tool in computational group theory and especially in the Matrix Group Recognition Project, since the analysis of a group is helped by knowledge of the Aschbacher classes containing it. Many variants of this theorem exist, to suit different authors' needs. For example, Aschbacher's original theorem classifies only the maximal subgroups of a classical group, while we have altered the class definitions to include all subgroups.

For algorithmic tasks, certain Aschbacher classes may have particularly efficient methods associated with them, such as $C_8$, so we introduce the related class $C'_8$ to include as many groups as possible. Conversely, some classes are difficult to handle computationally and we would like the number of groups falling into this category to be small, such as the classes we do not examine in Part II: $\{C_4, C_6, C_7, C_9\}$. We have also tried to reduce the overlap between the classes as those stated in the original theorem are far from disjoint. For example we have insisted that all reducible groups lie in $C_1$ and all irreducible but not absolutely irreducible groups lie in $C_3$.

More detailed descriptions of $C_i$, for $i \in \{1, 2, 3, 5, 8\}$ are given in Part II. This concludes our description of the Aschbacher classes and also our general introduction. We now move on to the first part of the work, classifying primitive permutation groups.
Part I

The primitive permutation groups of degree less than 4096
Chapter 2

Introduction to primitive permutation groups

We extend the classification of the primitive permutation groups to degree less than 4096. We shall begin by defining primitive groups and motivating their study before presenting some background to the area. In this part of the thesis all groups are finite.

2.0.11 Primitive groups

Let the group $G$ act on the set $\Omega$ and let $\alpha^g$ denote the action of a group element $g$ on $\alpha \in \Omega$. A subset $\Delta$ of $\Omega$ is a block for $G$ if for all $g \in G$ either

$$\Delta^g = \Delta$$

or

$$\Delta^g \cap \Delta = \emptyset. \quad (1)$$

The action of $G$ is primitive if it is transitive and all blocks are trivial, that is either $|\Delta| = 1$ or $\Delta = \Omega$. We refer to a group itself as primitive when there is no ambiguity about the associated action. An intransitive group $G$ with an orbit of size $k$ is isomorphic to a subgroup of $S_k \times S_{n-k}$. A transitive group which is not primitive is imprimitive. If $G$ preserves a block of size $k$, with $1 < k < n$, then all blocks have size $k$, and $G$ is isomorphic to a subgroup of $S_k \wr S_{n/k}$, with the imprimitive action.

To motivate our study, note that a permutation group is either transitive or is a subdirect product of transitive groups, while a transitive group is either primitive or is a subgroup of an iterated wreath product of primitive groups. Hence primitive groups can be viewed as the building blocks of all permutations groups and their classification helps us to better understand the structure of permutation groups in general.

2.1 History

The earliest reference to primitive groups is in the work of Ruffini in 1799, where he divided non-cyclic permutation groups into intransitive, imprim-
itive and primitive cases while trying (unsuccessfully) to prove the insolv-
ibility of the general quintic equation. In 1871 Jordan [30] made one of the
first attempts at classifying the primitive groups up to degree 17, one of his
many significant achievements relating to primitive groups. Some of Jor-
dan’s enumerations were later corrected by Cole [14] and Miller [44, 45, 46,
47, 49, 48, 50] in the last years of the 19th century. The work of Martin [43]
in 1901 and Bennett [4] in 1912 completed the classification up to degree 20.

At this stage, the lists of groups were getting too big to work with by
hand without a high chance of error and little significant progress was made
until the birth of symbolic computation in the 1960s. Sims [66] classified all
the primitive groups up to degree 50 as well as correcting the existing classifi-
cations. The full lists were never published, but were available to the math-
ematical community and eventually formed one of the earliest databases
in computational group theory. Further important developments were made
following the announcement of the Classification of the Finite Simple Groups
(CFSG) (given here as Theorem 1.3.1). In 1988 Dixon and Mortimer [18]
used the O’Nan–Scott Theorem to classify all non-affine primitive permuta-
tion groups of degree less than 1000: the numbers of affine groups of these
degrees are too large to be handled without computers. These groups were
made into a database in GAP by Theißen [70] together with the soluble affine
type groups of degree less than 255, which were classified by Short [65].

More recently Eick and Höfling [20] classified all soluble affine groups
of degree less than 6561 and Roney-Dougal and Unger [62] classified all
affine groups of degree less than 1000. In 2005 Roney-Dougal [61] classified
all primitive permutation groups of degree less than 2500, simultaneously
checking and correcting the existing results. As a consequence we shall only
consider primitive permutation groups of degree greater than 2499: however,
Thomas Breuer has recently found a missing cohort of groups in [61], see
Section 7.1 for more details.

This work extends the classification of the primitive permutation groups
up to degree 4095, using the framework of the O’Nan–Scott Theorem and
with Aschbacher’s theorem and CFSG as important tools. A reduced version
of this part of the thesis forms a paper [16]. Section 2.2 sets out some
definitions and results that will be needed throughout the investigation and
subsequent sections treat each O’Nan–Scott class in turn, explaining in detail
how the primitive groups are found, and presenting tables of data. For some
of the classes it is possible to automate almost all of the process, while for
others it is necessary to perform some theoretical calculations. Chapter 7
discusses the missing cohort in [61], the methods used to ensure accuracy
in computation and presentation, and gives suggestions for further work in
the area. The groups will be added to the primitive group databases of GAP
[23] and Magma [5].
2.2 Preliminary results

We now state a few results which will be needed for the classification. A useful reference for more details is [19].

2.2.1 The O’Nan–Scott Theorem

The socle of a group $G$ is the subgroup generated by the minimal normal subgroups of $G$ and is denoted by $\text{Soc}(G)$. By [19, Corollary 4.3B], the socle of a finite primitive group is isomorphic to the direct product of one or more copies of a simple group $T$. The following theorem classifies the primitive permutation groups according to the structure of their socles.

**Theorem 2.2.1** (O’Nan–Scott Theorem). Let $G$ be a primitive permutation group of degree $d$, and let $H := \text{Soc}(G) \cong T^m$ with $m \geq 1$. Then one of the following holds.

1. $H$ is regular and
   
   (a) **Affine type:** $T$ is cyclic of order $p$, so $|H| = p^m$. Then $d = p^m$ and $G$ is permutation isomorphic to a subgroup of the affine general linear group $\text{AGL}_m(p)$. We call $G$ an “affine type” group.
   
   (b) **Twisted wreath product type:** $m \geq 6$, the group $T$ is non-abelian and $G$ is a group of “twisted wreath product type”, with $d = |T|^m$.

2. $H$ is non-regular and non-abelian and

   (a) **Almost simple:** $m = 1$ and $T \leq G \leq \text{Aut}(T)$.
   
   (b) **Product action:** $m \geq 2$ and $G$ is permutation isomorphic to a subgroup of the product action wreath product $P \wr S_{m/l}$ of degree $d = n^{m/l}$. The group $P$ is primitive of type 2.(a) or 2.(c), $P$ has degree $n$ and $\text{Soc}(P) \cong T^l$, where $l \geq 1$ divides $m$.
   
   (c) **Diagonal type:** $m \geq 2$ and $T^m \leq G \leq T^m \cdot (\text{Out}(T) \times S_m)$, with the diagonal action. The degree $d = |T|^{m-1}$.

We can see immediately that there are no twisted wreath product type groups of degree less than $60^6$ and so we do not consider this class further. The other cases are described in detail in Chapters 3, 4, 5 and 6, following the order above.

Note that our definition of product action groups is more restrictive than that given by some authors. This is in order to make the O’Nan–Scott classes disjoint, as will be shown in Lemma 7.2.1.
2.2.2 Maximal subgroups and point stabilisers

We will frequently make use of the following lemma.

**Lemma 2.2.2.** Let $G$ be a faithful transitive subgroup of $\text{Sym}(\Omega)$.

1. If $G$ is primitive then a point stabiliser $G_\alpha$, for $\alpha \in \Omega$, is maximal.

2. Let $M$ be a maximal subgroup of $G$, then the action of $G$ on the cosets of $M$ is primitive.

**Proof.**

1. Let $G$ act primitively on $\Omega$ and let $\alpha \in \Omega$. Suppose there is a subgroup $H$ such that $G_\alpha < H < G$ and consider the set $\Delta = \{\alpha^h : h \in H\}$. The group $H$ is not transitive, as $|\Delta| = |H:H_\alpha| = |H:G_\alpha| < |G:G_\alpha|$, and hence $|\Delta| < |\Omega|$. The set $|\Delta| > 1$, since there are elements of $H$ which do not stabilise $\alpha$.

Consider $\Delta^g$, for some $g \in G$. Then either $g \in H$ and $\Delta^g = \Delta$, or else $\alpha^{hg} \notin \Delta$, for all $h \in H$ (for, if $\alpha^{hg} = \alpha^k$, for some $h, k \in H$ then $hkg^{-1} \in G_\alpha \leq H$, and therefore $g \in h^{-1}Hk = H$). Hence $\Delta$ is a non-trivial block of imprimitivity, causing a contradiction. So there is no such $H$ and $G_\alpha$ is maximal.

2. Let $M$ be a maximal subgroup of $G$, let $\Gamma := \{Mg : g \in G\}$ and consider the action of $G$ on $\Gamma$. Suppose $\Delta \subset \Gamma$ is a block of imprimitivity for this action, and let $H := \{g \in G : Mg = \Delta\}$. Then $M \leq H \leq G$ and the maximality of $M$ is violated unless either $H = M$, in which case $|\Delta| = 1$, or else $H = G$ and $|\Delta| = |\Gamma|$. Hence $\Delta$ is a trivial block and the action of $G$ on $\Gamma$ is primitive.

The above lemma tells us that maximal subgroups of permutation groups correspond to point stabilisers of primitive representations. We would like to classify only the faithful primitive actions and the following facts help us to identify when a group acts faithfully.

**Definition 2.2.3.** Let $G$ be a group and let $H \leq G$. The (normal) core of $H$ in $G$ is the largest normal subgroup of $G$ which is contained in $H$. The subgroup $H$ is core-free if its core is trivial.

**Lemma 2.2.4.** Let $G$ act faithfully and transitively on the set $\Omega$. Then $G_\alpha$ is core-free.
Proof. Let $\alpha \in \Omega$ and let $K$ be the normal core of a point stabiliser $G_\alpha$. Let $g \in G$, then for all $k \in K$ there exists $k_1 \in K$ such that $k = g^{-1}k_1g$, and

$$
(a^g)^k = a^{g(g^{-1}k_1g)} = a^{k_1g} = a^g.
$$

So $K$ acts as the identity on the whole orbit of $\alpha$. The orbit of $\alpha$ under the transitive action of $G$ is the whole of $\Omega$, and the kernel of a faithful action is trivial, so $K = \text{id}_G$.

Any pair of point stabilisers of a transitive group $G \leq \text{Sym}(\Omega)$ is conjugate in $G$, so by the above lemmas all faithful, primitive actions of $G$ correspond to conjugacy classes of core-free maximal subgroups of $G$.

**Lemma 2.2.5.** Let $G$ be a faithful and transitive group, then $\text{Soc}(G)$ is not contained in any point stabiliser of $G$.

**Proof.** Let $G_\alpha$ be a point stabiliser of $G$, then by Lemma 2.2.4 $G_\alpha$ is core-free. Hence $G_\alpha$ contains no normal subgroups, and in particular $\text{Soc}(G) \notin G_\alpha$.

### 2.2.3 Permutation isomorphism

If two permutation groups $G$ and $H$ can be obtained from each other by relabelling the points they act on, then we don’t want to count them twice in our tables. We use permutation isomorphism to determine whether two permutation groups are truly “different”.

**Definition 2.2.6.** Two permutation groups $G \leq \text{Sym}(\Omega)$ and $H \leq \text{Sym}(\Gamma)$ are **permutation isomorphic** if there exists an bijection $\sigma : \Omega \to \Gamma$ and an isomorphism $\phi : G \to H$ such that for all $\omega \in \Omega$ and $g \in G$

$$(\omega^g)\sigma = (\omega\sigma)^g.$$

We classify groups only up to permutation isomorphism, making use of the following fact.

**Lemma 2.2.7.** Two groups $G, H \leq \text{Sym}(\Omega)$ are permutation isomorphic if and only if they are conjugate in $\text{Sym}(\Omega)$.

**Proof.** ($\Rightarrow$) $G$ and $H$ are permutation isomorphic so there exists $\sigma \in \text{Sym}(\Omega)$ and an isomorphism $\phi : G \to H$ such that for any $\alpha \in \Omega$

$$(\alpha^g)\sigma = (\alpha\sigma)^g.$$
Let \( \alpha \) be arbitrary and put \( \beta := \alpha \sigma^{-1} \), then

\[
(\beta^g)\sigma = (\beta\sigma)^{g\phi} \\
((\alpha\sigma^{-1})^g)\sigma = (\alpha\sigma^{-1}\sigma)^{g\phi} \\
\alpha^{\sigma^{-1}g\sigma} = \alpha^{g\phi}.
\]

This shows that \( g\phi : \alpha \mapsto \alpha^{\sigma^{-1}g\sigma} \), for all \( \alpha \in \Omega \) and \( g \in G \). Hence \( G\phi = \sigma^{-1}G\sigma = H \) and \( G \) and \( H \) are conjugate in \( \text{Sym}(\Omega) \).

\((\Leftarrow)\) Suppose \( G \) and \( H \) are conjugate in \( \text{Sym}(\Omega) \). Let \( \sigma \in \text{Sym}(\Omega) \) such that \( H = \sigma^{-1}G\sigma \), and define \( \phi : G \rightarrow H \) such that \( \phi : g \mapsto \sigma^{-1}g\sigma \). Then \( \phi \) is an isomorphism and for any \( \alpha \in \Omega \) and any \( g \in G \)

\[
(\alpha^g)\sigma = (\alpha\sigma\sigma^{-1})^g\sigma \\
= (\alpha\sigma)^{\sigma^{-1}g\sigma} \\
= (\alpha\sigma)^{g\phi}
\]

Hence \( G \) and \( H \) are permutation isomorphic.

\[\square\]

**Lemma 2.2.8.** Let \( G, H \leq \text{Sym}(\Omega) \) be transitive groups with point stabilisers \( G_\alpha, H_\beta \), respectively. Then \( G \) and \( H \) are permutation isomorphic if and only if there is an isomorphism \( \phi : G \rightarrow H \) mapping \( G_\alpha \) to \( H_\beta \).

**Proof.** \((\Rightarrow)\) By Lemma 2.2.7 the group \( G = \sigma H \sigma^{-1} \), for some \( \sigma \in \text{Sym}(\Omega) \). The subgroup \( \sigma^{-1}G_\alpha \sigma \leq H \) is the point stabiliser in \( H \) of \( \alpha \sigma \) and hence is conjugate in \( \text{Sym}(\Omega) \) to \( H_\beta \), say \( \alpha^{\sigma\rho} = \beta \), where \( \rho \in \text{Sym}(\Omega) \). Let \( \phi : G \rightarrow H \) be the isomorphism given by \( G\phi = (\sigma\rho)^{-1}G(\sigma\rho) \), then \( G_\alpha\phi = H_\beta \).

\((\Leftarrow)\) Suppose there is an isomorphism \( \phi : G \rightarrow H \) such that \( G_\alpha\phi = H_\beta \). Then for all \( g \in G \) and \( \alpha \in \Omega \)

\[
(\alpha^g)^{\phi} = (\alpha^\sigma)^{\sigma^{-1}g\sigma} \\
= (\alpha^{\sigma\sigma^{-1}})^{g\sigma} \\
= (\alpha^\sigma)^{\sigma}.
\]

Hence \( G \) and \( H \) are permutation isomorphic. \[\square\]

### 2.2.4 Cohorts

It is useful to collect our primitive groups into families relating to their socles. We partition the primitive groups into cohorts, where two groups are in the same cohort if their socles are permutation isomorphic. The following is proved in [18, Lemma 3].
Lemma 2.2.9. Let $G$ be a primitive subgroup of $\text{Sym}(\Omega)$ with $H := \text{Soc}(G)$, and let $N := \text{NSym}(\Omega)(H)$. Let $H$ be either abelian or else non-regular, then every primitive group $K$ with $H \leq K \leq N$ has $\text{Soc}(K) = H$.

From the comment following Theorem 2.2.1, the socle of a primitive group of degree $d$, where $2500 \leq d < 4096$, is either abelian or else non-regular. Hence if $G$ is a primitive group with degree in this range then every primitive group between $H := \text{Soc}(G)$ and $N := \text{NSym}(\Omega)(H)$ lies in the same cohort.

The following lemma will be useful in our classification.

Lemma 2.2.10. Let $G \leq \text{Sym}(\Omega)$ be a primitive group of almost simple type, with socle $H$. Then $\text{NSym}(\Omega)(H)$ embeds in $\text{Aut}(H)$.

Proof. Let $N := \text{NSym}(\Omega)(H)$, then the action of $N$ on $H$ induces a homomorphism $\psi : N \to \text{Aut}(H)$, the kernel of which is the centraliser $C := C_{\text{Sym}(\Omega)}(H)$. If $C$ is trivial then $\psi$ is an embedding. The group $C \leq N$ and so $C$ contains some minimal normal subgroup $M$ of $N$. By Lemma 2.2.9 the socle $\text{Soc}(N) = H$ and so $M \leq H \cap C = Z(H) = 1$. Therefore $C$ is trivial and hence $N$ embeds into $\text{Aut}(H)$.

Under this embedding the socle $H$ maps to $\text{Inn}(H)$. The following is proved in [18, Lemma 2].

Lemma 2.2.11. Let $H$ be the non-regular socle of a primitive subgroup of $\text{Sym}(\Omega)$ and let $N := \text{NSym}(\Omega)(H)$. Then an automorphism $\sigma$ of $H$ is induced by conjugation by an element of $N$ if and only if $\sigma$ permutes the point stabilisers $H_\alpha$, for $\alpha \in \Omega$, amongst themselves.

Rank

Recall that the number of orbits of a point stabiliser is the rank of the group. The lists of primitive permutation groups of degree less than 2500 in [18] and [61] include the rank of $\text{NSd}(G)$, for each non-affine primitive permutation group $G$ of degree $d < 2500$. This value is easily computed, and for the sake of completeness our lists also include the rank of the normaliser for each cohort.

This concludes the preliminary results and definitions required for our classification. In the following chapters we treat each O'Nan–Scott class in turn and compute the primitive permutation groups in that class of degree $d$, where $2500 \leq d < 4096$. 

31
Chapter 3

Affine type groups

3.1 Introduction

In this chapter we classify the primitive permutation groups of affine type of degree $d$, where $2500 \leq d < 4096$. In this chapter, maps are written on the left and $V := \mathbb{F}_p^k$.

**Definition 3.1.1.** The affine general linear group $AGL_k(p)$ consists of all maps $f : V \to V$ given by $f(v) = va + u$, where $u \in V$ and $a \in GL_k(p)$. If $a = 1$ then $f$ is a translation and these maps generate the translation subgroup $T \leq AGL_k(p)$.

The action of $T$ on $V$ is regular and $T$ is permutation isomorphic to $V^+$, the additive group of the vector space.

**Lemma 3.1.2.** Let $G \leq \text{Sym}(\Omega)$ and let $\alpha \in \Omega$. If $R$ is a regular normal subgroup of $G$ then $G = R : G_\alpha$.

**Proof.** By Lemma 1.2.2 the group $G = R : G_\alpha$ if $G = RG_\alpha$ and $G_\alpha \cap R = \text{id}_G$. Consider the action of $G$ on $\alpha \in \Omega$ and note that $R$ acts transitively on $\Omega$. If $g \in G$ then there exists $y \in R$ such that $\alpha^y = \alpha^g$, by the transitivity of $R$. Then $x = gy^{-1}$ is in $G_\alpha$ and $g = xy$, so $g \in G_\alpha R$. The group $R$ is normal in $G$, so $G_\alpha R = RG_\alpha$ and since $RG_\alpha \subset G$ we deduce that $G = RG_\alpha$. The intersection $G_\alpha \cap R = R_\alpha = \text{id}_G$, since $R$ is regular, and thus $G = R : G_\alpha$. □

The stabiliser in $AGL_k(p)$ of $0_V$ is $GL_k(p)$, so $AGL_k(p) = T : GL_k(p)$ by Lemma 3.1.2.

**Definition 3.1.3.** A primitive group $G$ is of affine type if $G$ is permutation isomorphic to a subgroup of $AGL_k(p)$ in its natural action on $V := \mathbb{F}_p^k$, for some prime $p$ and integer $k \geq 1$, and also $\text{Soc}(G) \cong T$.

Note that for all primitive groups $G$ of affine type, the socle $T$ is normal in $G$ and hence $G \cong T : K$, for some $K \leq GL_n(q)$.
We now present some results which will be used to describe the connection between primitive and affine groups. A group $G$ is characteristically simple if the only characteristic subgroups of $G$ are the trivial group and $G$ itself.

**Lemma 3.1.4.** Let $H$ be a non-trivial, abelian, characteristically simple group, then $H$ is elementary abelian.

*Proof.* Let $p$ be a prime divisor of $|H|$ and let $B := \{h \in H : h^p = \text{id}_H\}$. Then $B$ is a subgroup of $H$, since $H$ is abelian, and in fact $B$ is elementary abelian. We prove that $B = H$. Let $b \in B$, then for any $\alpha \in \text{Aut}(H)$

$$\alpha(b)^p = \alpha(b^p) = \text{id}_H,$$

so $\alpha(b) \in B$ and $B$ is characteristic in $H$. Let $x \in H$ be a non-identity element of order $n > p$. Then by Cauchy’s theorem $x^{n/p}$ is a non-identity element of order $p$, so $B$ is non-trivial. Since $H$ is characteristically simple, the group $B = H$, and hence $H$ is elementary abelian.

The following lemmas are well-known and needed for future proofs.

**Lemma 3.1.5.** Let $G \leq \text{Sym}(\Omega)$ be an abelian group, acting transitively on $\Omega$. Then $G$ acts regularly on $\Omega$.

*Proof.* A transitive group $G$ acts regularly on $\Omega$ if $G_\alpha = \text{id}_G$, for all $\alpha \in \Omega$. Let $g \in G_\alpha$, then $g^\alpha = \alpha$. If $h$ is any other element of $G$ then $\alpha^{gh} = \alpha^{gh} = \alpha^h$, and hence $g$ fixes all elements of $\Omega$, by the transitivity of $G$. Therefore $g = \text{id}_G$.

**Lemma 3.1.6.** Let $G$ be a primitive subgroup of $\text{Sym}(\Omega)$ and let $H \leq G$ be abelian and transitive on $\Omega$. Then $H = C_G(H)$.

*Proof.* Since $H$ is abelian, the group $C := C_G(H)$ contains $H$, and so $C$ is transitive. Let $\alpha \in \Omega$ and suppose $\alpha^c = \alpha$, for some $c \in C$. Then $\alpha^{hc} = \alpha^{ch} = \alpha^h$, for all $h \in H$. Since $H$ is transitive, the element $c$ fixes all elements of $\Omega$ and so $c = \text{id}_C$, hence $C$ is regular. The group $H$ is regular by Lemma 3.1.5, and so $|C| = |H|$. Since $H \leq C$, we deduce that $H = C$.

**Lemma 3.1.7.** Let $G$ be a primitive permutation group with an abelian minimal normal subgroup $H$, then $H = \text{Soc}(G)$.

*Proof.* Recall that the socle of $G$ is generated by all minimal normal subgroups of $G$. Let $C := C_G(H)$. The group $H$ is transitive, as it is a normal subgroup of a primitive group. Hence $H = C$, by Lemma 3.1.6.

Let $K$ be a minimal normal subgroup of $G$ distinct from $H$, then $K \cap H$ is normal in $G$ and hence is trivial, so $K$ commutes with $H$. Hence $K \leq C$, that
is $K \leq H$, which implies that $K = H$, by the minimality of $H$. Therefore $H = \text{Soc}(G)$. \qed

The next theorem characterises the primitive permutation groups of affine type.

**Theorem 3.1.8.** Let $G \leq \text{Sym}(\Omega)$ be a primitive permutation group with an abelian minimal normal subgroup $H$. Then there exists a prime $p$ and an integer $k \geq 1$ such that

1. $H$ is permutation isomorphic to the translation subgroup $T \leq \text{AGL}_k(p)$;
2. the degree of $G$ is $p^k$;
3. $G = H : G_\alpha$, and $G$ is permutation isomorphic to a subgroup of $\text{AGL}_k(p)$; and
4. $G_\alpha$ is permutation isomorphic to an irreducible subgroup of $\text{GL}_k(p)$, acting on non-zero vectors.

**Proof.**

1. For all $\omega \in \text{Sym}(\Omega)$ the stabiliser $H_\omega \unlhd H$, since $H$ is abelian, and so $H$ is regular. The group $H$ is characteristically simple and hence is elementary abelian, by Lemma 3.1.4. So $|H| = p^k$, for some prime $p$ and $k \geq 1$, and $H \cong T$, the translation subgroup of $\text{AGL}_k(p)$. Let $V := \mathbb{F}_p^k$, then $T \cong V^+$ and we identify $H$ with $V^+$.

2. $H$ is regular, so the degree of $G$ is $|H|$. Fix $\alpha \in \Omega$ and let $\omega \in \Omega$ be arbitrary. Since $H$ is regular there is a unique $h \in H$ such that $\alpha^h = \omega$. Let $V := \mathbb{F}_p^k$, as above. We define a map $\delta : \Omega \to V$ given by $\delta(\omega) = \delta(\alpha^h) = h$ and note that $\delta$ is well-defined and invertible. Let $G$ act on $V$ by $\delta(\omega)^g = \delta(\omega^g)$.

3. The group $H$ is regular, so $G = H : G_\alpha$, by Lemma 3.1.2 and $G_\alpha$ is isomorphic to a subgroup of $\text{Aut}(H) \cong \text{Aut}(V^+) \cong \text{GL}_k(p)$. We demonstrate the action of $G_\alpha$ on $H$. Let $s \in G_\alpha$, then

$$h^s = \delta(\alpha^h)^s$$

$$= \delta(\alpha^{hs})$$

$$= \delta(\alpha^{ss^{-1}hs})$$

$$= \delta(\alpha^{s^{-1}hs})$$

$$= s^{-1}hs.$$
$s^{-1}Ks = K$ for all $s \in G_\alpha$, and hence $K$ is normal in $G$. This contradicts the minimality of $H$, and hence $G_\alpha$ acts irreducibly on $V$.

We use the following lemma to classify the primitive permutation groups of affine type.

**Lemma 3.1.9.** Let $G := T:K \leq \text{GL}_k(q)$ and $R := T_1:L \leq \text{GL}_k(q)$ be two primitive subgroups of affine type, with socles $T$ and $T_1$, respectively. Then $G$ and $R$ are permutation isomorphic if and only if $K$ and $L$ are conjugate in $\text{GL}_k(p)$.

**Proof.** The groups $G$ and $R$ are permutation isomorphic if and only if they are conjugate in $S_{p^k}$, by Lemma 2.2.7. Hence $T$ and $T_1$ are conjugate in $S_{p^k}$ and without loss of generality, we set $T = T_1$.

The group $T$ is abelian and transitive, so $C_{S_{p^k}}(T) = T$, by Lemma 3.1.6, and hence $N_{S_{p^k}}(T) \cong T : \text{Aut}(T) = \text{AGL}_k(p)$. Therefore $G$ and $R$ are permutation isomorphic if and only if they are conjugate in $\text{AGL}_k(p)$.

$(\Rightarrow)$ Fix a copy of $\text{GL}_k(p)$ in $\text{AGL}_k(p)$ by taking the stabiliser of $0_V$. Let $t_1h \in \text{AGL}_k(p)$ and let $tg \in G$. Then

\[
(tg)^{t_1h} = h^{-1}t_1^{-1}tgt_1h = h^{-1}(t_1^{-1}t)h \cdot h^{-1}tgt_1h = (t_1^{-1}t)^{h^{-1}g}t_1(h^{-1}g)^{-1}(h^{-1}g)h = (t_1^{-1}t)^{h^{-1}g}t_1(h^{-1}g)^{-1} g
\]

and $(t_1^{-1}t)^{h^{-1}g}t_1(h^{-1}g)^{-1} \in T$, so the image of $g \in \text{GL}_k(p)$ is only determined by the conjugating element of $\text{GL}_k(p)$. Hence $K$ and $L$ are conjugate in $\text{GL}_k(p)$.

$(\Leftarrow)$ Now suppose that $K$ and $L$ are conjugate in $\text{GL}_k(p)$. Then the actions of $K$ on $T$ and of $L$ on $T$ are permutation isomorphic. This implies that the associated external semidirect products are permutation isomorphic, as are their natural actions, since the action is derived from $T$ acting on itself. 

Hence, classifying the primitive permutation groups of affine type of degree $d$, where $2500 \leq d < 4096$, corresponds to classifying the irreducible subgroups of $\text{GL}_k(p)$ with $2500 \leq p^k = d < 4096$.

### 3.2 Method

For all prime powers $q = p^k$ in the range $2500 \leq q < 4096$, the group $\text{GL}_k(p)$ has computable subgroups in Magma. For $k = 2$ the Magma command
IrreducibleSubgroups(G) returns a representative of each conjugacy class of irreducible subgroups of G (it is not available for dimensions other than 2). We now consider in turn the cases where $k = 1$ and $k > 1$.

**Case $k = 1$.** The group $\text{AGL}_1(p)$ consists of all maps from $\mathbb{F}_p$ to itself given by $f(x) = xa + b$, where $a, b \in \mathbb{F}_p$ and $a$ is non-zero. This is equivalent to $T: \mathbb{F}_p^*$, where $T = \{ t : t(x) = x + b \}$, and $\text{AGL}_1(p) \cong p:(p-1)$. All subgroups of $\mathbb{F}_p^* = \text{GL}_1(p)$ are irreducible and there is one conjugacy class of affine type groups for each divisor of $p-1$. We store only two generators, $g_1$ and $g_2$, where $g_1$ is a $p$-cycle and $g_2$ generates the group $(p-1)$. Then any primitive subgroup $G$ of $\text{AGL}_1(p)$ is generated by $\langle g_1, g_2^s \rangle$, for some $s$.

**Case $k > 1$.** The values for $(p,k)$ such that $2500 \leq p^k < 4096$ are $\{(53,2), (59,2), (61,2), (5,5)\}$. For $(p,k) \in \{(53,2), (59,2), (61,2)\}$ we use Magma to compute representatives for each conjugacy class of the irreducible subgroups of $\text{GL}_2(p)$. The corresponding subgroups of $\text{AGL}_2(p)$ may be constructed by taking semidirect products of the irreducible subgroups with their natural modules. This is achieved using the command $\text{Semidir(G,Getvecs(G))}$, where $G$ is one of the irreducible matrix groups.

The group $\text{GL}_5(5)$ is somewhat larger and it is not convenient to directly compute its subgroups in Magma. We deal with this group as follows: first calculate its irreducible maximal subgroups which contain $\text{SL}_5(5)$; in $\text{GL}_5(5)$ there is a unique proper subgroup $M := \text{SL}_5(5):2$ containing $\text{SL}_5(5)$ as a proper subgroup. Let $L$ be the union of the class representatives of the irreducible maximal subgroups of $\text{GL}_5(5)$, $M$ and $\text{SL}_5(5)$ which do not contain $\text{SL}_5(5)$. See Table 3.1 for more details.

We then let $L_1$ be the union of the class representatives of the irreducible subgroups of each member of $L$. Finally, we check members of $L_1 \cup \{\text{GL}_5(5), M, \text{SL}_5(5)\}$ for conjugacy under $\text{GL}_5(5)$, and discard any duplicates. This method avoids a large enough part of the subgroup lattice to make the computation manageable, since the index of $\text{Sp}_4(5)$ in $\text{GL}_5(5)$ is huge.

The following theorem summarises the results of this chapter.

**Theorem 3.2.1.** Let $G$ be a primitive permutation group of affine type of degree $d$, where $2500 \leq d < 4096$. If $d$ is prime then $G \cong d:r$ where $r$ divides $d-1$. Otherwise $d = p^k$ for $(p,k) \in \{(53,2), (59,2), (61,2), (5,5)\}$, and $G \cong T:K$, where $T \cong \mathbb{F}_p^k$ and $K$ is an irreducible subgroup of $\text{GL}_k(p)$.

The numbers of primitive soluble and insoluble affine groups of non-prime degree $d$, where $2500 \leq d < 4096$, are given in Table 3.2.
Table 3.1: Groups contained in \( L \)

<table>
<thead>
<tr>
<th>( G )</th>
<th>Subgroups of ( G ) in ( L )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( GL_5(5) )</td>
<td>2.2.5.11.71</td>
</tr>
<tr>
<td></td>
<td>( L_2(11).2 )</td>
</tr>
<tr>
<td></td>
<td>( 2.A_5.2.2^4.2^4 )</td>
</tr>
<tr>
<td></td>
<td>( 2.S_4(5).2 )</td>
</tr>
<tr>
<td>( M )</td>
<td>2.5.11.71</td>
</tr>
<tr>
<td></td>
<td>( L_2(11).2 )</td>
</tr>
<tr>
<td></td>
<td>( 2.A_5.2^4.2^4 )</td>
</tr>
<tr>
<td></td>
<td>( 2.S_4(5).2 )</td>
</tr>
<tr>
<td>( SL_5(5) )</td>
<td>5.11.71</td>
</tr>
<tr>
<td></td>
<td>( L_2(11) )</td>
</tr>
<tr>
<td></td>
<td>( 2.A_5.2^4.2^4 )</td>
</tr>
<tr>
<td></td>
<td>( 2.S_4(5) )</td>
</tr>
</tbody>
</table>

Table 3.2: Primitive groups of affine type

<table>
<thead>
<tr>
<th>( p^k )</th>
<th>Soluble</th>
<th>Insoluble</th>
</tr>
</thead>
<tbody>
<tr>
<td>53^2</td>
<td>100</td>
<td>6</td>
</tr>
<tr>
<td>59^2</td>
<td>82</td>
<td>6</td>
</tr>
<tr>
<td>61^2</td>
<td>212</td>
<td>20</td>
</tr>
<tr>
<td>5^5</td>
<td>48</td>
<td>46</td>
</tr>
</tbody>
</table>
Accuracy checks

The soluble irreducible subgroups of $\text{GL}_k(p)$, for $p^k < 2^{16}$, are in the IRREDSOL package of GAP, and these were checked against MAGMA, finding no discrepancy. Our numbers of soluble groups also agree with those in [20].

This concludes our classification of the primitive permutation groups of affine type of degree $d$, where $2500 \leq d < 4096$. In the following chapters, we consider the O’Nan–Scott classes of groups with non-regular socles.
Chapter 4

Almost simple groups

4.1 Introduction

In this chapter we classify the primitive almost simple groups of degree $d$, for $2500 \leq d < 4096$. We consider each family of simple groups in turn, as described in Theorem 1.3.1 (CFSG). The groups with alternating socle are considered first, followed by the groups with classical, exceptional and finally sporadic socle. Note that in this chapter all maps are written on the right. We begin with some definitions and basic results.

If an almost simple group $G$ with socle $T$ has a maximal subgroup $M$, for which $M \cap T$ is a proper, non-maximal subgroup of $T$, then $M$ is a novelty. If $T \leq M$ then $M$ is a triviality and corresponds to a non-faithful action of $G$. Otherwise, $M$ is an ordinary maximal subgroup.

Lemma 4.1.1. Let $N$ be a novelty of $G$, then $|G:N|$ is a proper multiple of $|T:M|$, for some maximal subgroup $M$ of $T$.

Proof. Let $T := \text{Soc}(G)$. Since $N$ is a novelty $N \cap T < M$, for some maximal subgroup $M$ of $T$, and hence $|T:N \cap T| > |T:M|$. Note that for any subgroup $H < G$

$$|G:H||H:H \cap T| = |G:H \cap T| = |G:T||T:H \cap T|. \quad (4.1)$$

Now, the quotient $N/(N \cap T) \cong NT/T$, by the second isomorphism theorem, and $NT = G$ since $T \not\leq N$. Substituting $N$ for $H$ in (4.1), we see that $|G:N| = |T:N \cap T|$. Hence $|G:N| > |T:M|$.

Let $M$ be a core-free maximal subgroup of $G$. Then by Lemma 2.2.2 there exists a faithful, primitive action of $G$ for which $M$ is a point stabiliser. Conversely, the point stabiliser of a primitive action of $G$ is a maximal subgroup of $G$. Hence we can classify the almost simple primitive permutation groups
of degree \(d\), where \(2500 \leq d < 4096\), by finding the maximal subgroups of almost simple groups \(G\) of index in that range.

Let \(P(G)\) denote the smallest \(d\) such that \(G\) has a faithful primitive permutation action of degree \(d\). The following lemma and its proof are found in [61].

**Lemma 4.1.2.** Let \(G\) be an almost simple group with socle \(T\), and let \(T \leq G \leq \text{Aut}(T)\). Then \(P(G) \geq P(T)\).

**Proof.** Let \(G_\alpha\) be a point stabiliser of \(G\) in a primitive faithful action of degree \(P(G)\), then \(T \not\trianglelefteq G_\alpha\), by Lemma 2.2.5. By the second isomorphism theorem \(G_\alpha/(G_\alpha \cap T) \cong G_\alpha T/T\), and since \(G_\alpha T = G\) and \(G_\alpha \cap T = T_\alpha\), the index \(|T:T_\alpha| = |G:G_\alpha|\), which is the degree of the action. If \(T_\alpha \leq \text{max} T\), then \(T\) is primitive and \(P(G) \geq P(T)\). Otherwise \(T_\alpha\) is contained in a maximal subgroup \(M\), and \(M\) is the point stabiliser of an action of degree \(P(T)\), which is smaller than \(P(G)\).

By Theorem 1.3.1 (CFSG), a non-abelian simple group is either an alternating, classical, exceptional or sporadic group. We now address each of these families in turn, finding the almost simple groups with maximal subgroups of index \(d\), where \(2500 \leq d < 4096\). For each such almost simple group \(G\), we construct the actions of \(G\) on the cosets of these maximal subgroups and the resulting primitive groups are given in Subsection 4.6.

### 4.2 Alternating and symmetric groups

Recall from Section 2 that two permutation groups lie in the same cohort precisely when they have the same degree and their socles are permutation isomorphic. For \(d > 4\), the groups \(A_d\) and \(S_d\) in their natural action are primitive almost simple groups and form a single cohort. We refer to these groups as improper primitive groups and do not consider them further.

The following is proved in [28, Kapitel II: Satz 4.6]

**Theorem 4.2.1** (Bochert’s theorem). Let \(G\) be a primitive group acting on the set \(\Omega\), let \(|\Omega| = n\) and \(A_n \not\trianglelefteq G\). Then

\[
|S_n : G| \geq \left\lfloor \frac{(n + 1)}{2} \right\rfloor !.
\]

We now find the values of \(n\), for which an almost simple group with socle \(A_n\) is primitive and of degree \(d\), where \(2500 \leq d < 4096\).

**Proposition 4.2.2.** Let \(G\) be \(A_n\) or \(S_n\). If \(G\) has a faithful primitive action of degree \(d\), where \(2500 \leq d < 4096\), other than the natural action, then \(n \leq 91\). If a point stabiliser \(H\) of this action is transitive on \(\{1, \ldots, n\}\) then \(H\) is primitive and \(10 \leq n \leq 12\).
Proof. Since $6! < 2500$ we may assume that $n \geq 7$. If $G = A_n$ then let $X$ be a point stabiliser of a faithful primitive action of $G$ and let $X \neq A_{n-1}$ to exclude the improper action. If $G = S_n$ then let $X = Y \cap A_n$, where $Y$ is a point stabiliser of a faithful primitive action of $G$, and note that in this case $X$ may not be maximal in $A_n$.

Case 1: Suppose that $X$ is primitive in its action on $\{1, \ldots, n\}$. We require $|A_n : X| < 4096$ and hence $|S_n : X| < 8192$, so $n < 15$ by Theorem 4.2.1. For $7 \leq n \leq 14$ the groups $A_n$ and $S_n$ have computable subgroups in MAGMA. We find that only $A_{10}$, $A_{11}$, $A_{12}$ and $S_{10}$ have primitive maximal subgroups of index $d$, for $2500 \leq d < 4096$. Each has one conjugacy class of such subgroups, of index 2520, and these are described in Theorem 4.2.3.

Note that the point stabiliser in this action of $S_{10}$ has primitive intersection with $A_{10}$ (in the natural action), as this fact will be used later.

Case 2: Suppose that $X$ acts imprimitively on $\{1, \ldots, n\}$. Let $k$ be the size of some non-trivial block for $X$, so that $1 < k < n$, and set $m := n/k$; then $X \leq S_k \wr S_m$. We have seen in Case 1 that there is no maximal primitive group $Y \leq S_n$ of index $d$, for $2500 \leq d < 4096$, such that $X = Y \cap A_n$ is imprimitive, and hence $Y = S_k \wr S_m$ in this case. Therefore, $X$ is an index 2 subgroup of $S_k \wr S_m$. This implies that $|X| = (k!)^m(m!)^2$, and so

$$|A_n : X| = |S_n : Y| = (mk)!/(k!)^m m! = (m, k)f.$$ 

The function $(m, k)f$ increases monotonically in both variables and the reader may check that for $(m, k) \in \{(2, 7), (3, 3), (4, 2), (5, 2)\}$ the value of $(m, k)f$ is less than 2500, whilst for $(m, k) \in \{(2, 8), (3, 4), (4, 3), (5, 3), (6, 2)\}$ the value of $(m, k)f$ is greater than 4095. Hence there is no $n$ such that $G$ has an imprimitive maximal subgroup, of index in the required range.

Case 3: Finally, suppose that $X$ acts intransitively on $\{1, \ldots, n\}$. Suppose that $X$ has an orbit of length 1, then $X$ is conjugate to a subgroup of $A_{n-1}$. If $X$ is maximal in $A_n$, then $X \cong A_{n-1}$, a contradiction, so $X = Y \cap A_n$, for some $Y \leq S_n$. Since $|Y : X| = 2$, the group $Y$ has an orbit of length $\leq 2$. The group $Y$ has at most one orbit of length 1, for if $i, j \in \{1, \ldots, n\}$ both have orbits of length 1 under the action of $Y$, then

$$Y < \langle Y, (i j) \rangle < S_n$$

and $Y$ is not maximal in $S_n$. If $Y$ has a single orbit of length 1 then $Y \cong S_{n-1}$ and $G$ is improper. Hence $Y$ has no orbits of length 1 and $Y \cong S_2 \times S_{n-2}$. However $(S_2 \times S_{n-2}) \cap A_n$ contains either the permutation $(1 2)(3 \ldots n)$ or else $(1 2)(3 \ldots (n-1))$ and $(n-2)(n-1)n$ and hence $X$ has no fixed points, a contradiction. We deduce that $X$ has no orbits of length 1.
Let $\Gamma$ be the smallest orbit of $X$ and set $k := |\Gamma| \leq n/2$. Then $X \leq (S_k \times S_{n-k}) \cap A_n$, so

$$|X| \leq k!(n-k)!/2$$

and

$$|A_n : X| = |S_n : Y| \geq n!/k!(n-k)! = \binom{n}{k} \geq \frac{n}{2}.$$ 

The upper bound $|A_n : X| < 4096$ implies that $n \leq 91$. $\square$

For $n = 10, 11, 12$ we find all primitive and all intransitive maximal subgroups of $A_n$ and $S_n$ of index $d$, for $2500 \leq d < 4096$. For $12 < n < 92$ we determine all intransitive maximal subgroups of $A_n$ and $S_n$ of index in that range. Note that MAGMA has a database of maximal subgroups of $S_n$ for each of these values of $n$. We then use MAGMA to construct the actions on the cosets of these maximal subgroups and store the primitive groups.

**Primitive point stabiliser**

We now identify the primitive maximal subgroups of $A_n$ and $S_n$ of index $d$, where $2500 \leq d < 4096$.

**Theorem 4.2.3.** Let $G$ be either $A_n$ or $S_n$ and suppose $G$ has a proper, faithful primitive action of degree $d$, where $2500 \leq d < 4096$. If the point stabiliser $X$ acts primitively on the set $\{1, \ldots, n\}$, then $G$, $X$ and $\text{Soc}(X)$ appear in the following table.

<table>
<thead>
<tr>
<th>$G$</th>
<th>$X$</th>
<th>$\text{Soc}(X)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_{10}$</td>
<td>$M_{10}$</td>
<td>$A_6$</td>
</tr>
<tr>
<td>$S_{10}$</td>
<td>$\text{Aut}(A_6)$</td>
<td>$A_6$</td>
</tr>
<tr>
<td>$A_{11}$</td>
<td>$M_{11}$</td>
<td>$M_{11}$</td>
</tr>
<tr>
<td>$A_{12}$</td>
<td>$M_{12}$</td>
<td>$M_{12}$</td>
</tr>
</tbody>
</table>

**Proof.** By Proposition 4.2.2 and Lemma 4.2.3, we know that $n \in \{10, 11, 12\}$. For each $n$ we use MAGMA to find the maximal subgroups of $G$, up to conjugacy. The maximal subgroups which are primitive and of index $d$, where $2500 \leq d < 4096$, are recorded in the table, together with their socles. $\square$

**Intransitive point stabiliser**

Let $G$ be $A_n$ or $S_n$. A maximal subgroup $X$ of $G$, acting intransitively on the set $\{1, \ldots, n\}$, is isomorphic to $(S_k \times S_{n-k}) \cap G$, where $k$ is the length of the smallest orbit of $X$. 

42
Theorem 4.2.4. Let $G$ be $A_n$ or $S_n$ and suppose $G$ has a proper, faithful primitive action of degree $d$, where $2500 \leq d < 4096$. Let $X$ be a point stabiliser of $G$ which acts intransitively on $\{1, \ldots, n\}$, and whose smallest orbit has size $k$. Then $(n, k)$ is one of the following:

- $(14, 7), (14, 6), (15, 5), (18, 4), (19, 4)$;
- $(n, 3)$, with $26 \leq n \leq 30$;
- $(n, 2)$, with $72 \leq n \leq 91$.

Proof. The point stabiliser $X \cong (S_k \times S_{n-k}) \cap G$. Let $d$ be the degree of the coset action of $G$ on $X$. Then $d = \binom{n}{k}$, since

$$|A_n : X| = \frac{n!/2}{(k!(n-k))/2} = \frac{n!}{k!(n-k)!} = |S_n : X|.$$ 

The values of $n$ and $k$ for which $2500 \leq \binom{n}{k} < 4096$ are given above. □

We conclude:

Theorem 4.2.5. Let $G$ be a primitive almost simple group of degree $d$, where $2500 \leq d < 4096$, with socle $A_n$. Then $G$ appears in Table 4.7 at the end of the chapter.

Proof. We discount the natural action. Let $X$ be the point stabiliser of a faithful primitive action of $G$ of degree $d$, where $2500 \leq d < 4096$, then by Proposition 4.2.2 the group $X$ is either primitive or intransitive. If $X$ is primitive then $n \in \{10, 11, 12\}$ and $X$ is given in Theorem 4.2.3. If $X$ is intransitive then $X \cong (S_k \times S_{n-k}) \cap G$, where $n$ and $k$ are given in Theorem 4.2.4. We use Magma to compute the primitive action of $G$ on the cosets of $X$, as well as the degree of the action and the rank of $\text{NS}_d(A_n)$. □

This completes our treatment of the almost simple primitive groups with alternating socle.

4.3 Classical groups

Recall from Chapter 1.5, that a simple classical group takes one of the following forms: linear, $L_n(q)$; symplectic, $S_{2m}(q)$; unitary, $U_n(q)$; orthogonal in odd dimension, $P\Omega_{2m+1}(q) = P\Omega^\epsilon_{2m+1}(q)$ and orthogonal in even dimension, $P\Omega^\epsilon_{2m}(q)$ with $\epsilon \in \{+,-\}$. In this section, heavy use will be made of Theorem 1.5.11, which describes which classical groups are not simple and presents the isomorphisms between the classical groups. Recall from page 3 that a group is $\mathcal{CS}$ if it has computable subgroups in Magma V2.14–12 and
\( P(G) \) is the minimal degree of a faithful primitive permutation representation of \( G \).

Table 4.1: Socles of almost simple classical groups \( G \) with \( P(\text{Soc}(G)) < 4096 \)

<table>
<thead>
<tr>
<th>Soc(G)</th>
<th>( n )</th>
<th>( q )</th>
<th>Non-CS</th>
</tr>
</thead>
<tbody>
<tr>
<td>( L_n(q) )</td>
<td>( n = 2 )</td>
<td>( q \leq 4093 )</td>
<td></td>
</tr>
<tr>
<td></td>
<td>( n = 3 )</td>
<td>( q \leq 61 )</td>
<td></td>
</tr>
<tr>
<td></td>
<td>( n = 4 )</td>
<td>( q \leq 13 )</td>
<td></td>
</tr>
<tr>
<td></td>
<td>( n = 5 )</td>
<td>( q \leq 7 )</td>
<td></td>
</tr>
<tr>
<td></td>
<td>( n = 6 )</td>
<td>( q \leq 5 )</td>
<td>( L_6(4) ), ( L_6(5) )</td>
</tr>
<tr>
<td></td>
<td>( n = 7 )</td>
<td>( q \leq 3 )</td>
<td></td>
</tr>
<tr>
<td></td>
<td>( n = 8 )</td>
<td>( q \leq 3 )</td>
<td>( L_8(3) )</td>
</tr>
<tr>
<td></td>
<td>( 9 \leq n \leq 12 )</td>
<td>( q = 2 )</td>
<td></td>
</tr>
<tr>
<td>( S_{2m}(q) )</td>
<td>( m = 2 )</td>
<td>( q \leq 13 )</td>
<td></td>
</tr>
<tr>
<td></td>
<td>( m = 3 )</td>
<td>( q \leq 5 )</td>
<td>( S_6(4) ), ( S_6(5) )</td>
</tr>
<tr>
<td></td>
<td>( m = 4 )</td>
<td>( q \leq 3 )</td>
<td>( S_8(3) )</td>
</tr>
<tr>
<td></td>
<td>( 5 \leq m \leq 6 )</td>
<td>( q = 2 )</td>
<td>( S_{12}(2) )</td>
</tr>
<tr>
<td>( U_n(q) )</td>
<td>( n = 3 )</td>
<td>( q \leq 13 )</td>
<td></td>
</tr>
<tr>
<td></td>
<td>( n = 4 )</td>
<td>( q \leq 7 )</td>
<td></td>
</tr>
<tr>
<td></td>
<td>( n = 5 )</td>
<td>( q \leq 3 )</td>
<td>( U_5(3) )</td>
</tr>
<tr>
<td></td>
<td>( 6 \leq n \leq 7 )</td>
<td>( q = 2 )</td>
<td>( U_7(2) )</td>
</tr>
<tr>
<td>( \text{P}\Omega_{2m+1}(q) )</td>
<td>( m = 3 )</td>
<td>( q \leq 5 ) and odd</td>
<td>( \text{P}\Omega_7(5) )</td>
</tr>
<tr>
<td></td>
<td>( m = 4 )</td>
<td>( q = 3 )</td>
<td>( \text{P}\Omega_9(3) )</td>
</tr>
<tr>
<td>( \text{P}\Omega_{2m}^{+}(q) )</td>
<td>( m = 4 )</td>
<td>( q \leq 3 )</td>
<td>( \text{P}\Omega_7^{+}(3) )</td>
</tr>
<tr>
<td></td>
<td>( 5 \leq m \leq 6 )</td>
<td>( q = 2 )</td>
<td>( \text{P}\Omega_{12}^{+}(2) )</td>
</tr>
<tr>
<td>( \text{P}\Omega_{2m}^{-}(q) )</td>
<td>( m = 4 )</td>
<td>( q \leq 3 )</td>
<td></td>
</tr>
<tr>
<td></td>
<td>( 5 \leq m \leq 6 )</td>
<td>( q = 2 )</td>
<td>( \text{P}\Omega_{12}^{-}(2) )</td>
</tr>
</tbody>
</table>

**Lemma 4.3.1.** Let \( G \) be an almost simple classical group with \( P(G) < 4096 \). Then the socle \( T \) of \( G \) appears in Table 4.1.

**Proof.** By Lemma 4.1.2, if the maximal subgroups of a simple classical group \( T \) all have indices greater than 4095, then no group with socle \( T \) has a primitive permutation representation on fewer than 4095 points. Hence it suffices to consider the simple classical groups. The formulae for \( P(T) \) are given in [32, Theorem 5.2.2], corrected in [6], and are all monotonically increasing in each variable. We consider each classical type in turn, determining the maximum values of \( n \) (or \( m \)) and \( q \) such that \( P(T) < 4096 \).

**Linear** A group \( L_2(q) \), with \( q \leq 5 \), is either soluble or else is isomorphic to an alternating group, by Theorem 1.5.11, and so its primitive representations
of degree \( d \), for \( 2500 \leq d < 4096 \), are given in Theorem 4.2.5. If \((n, q) \not\in \{(2, q) : q \text{ odd}, 7 \leq q \leq 11\} \cup \{(4, 2)\} \) then the minimal degree of a non-trivial permutation representation of \( L_n(q) \) is \((q^n - 1)/(q - 1)\). Each of the excluded groups \( G \) satisfy \( P(G) < 4096 \), since either \(|G| < 4096\) or \( G = L_4(2) \cong A_8 \) and \( P(G) = 8 \). Hence the largest values of \( n \) and \( q \) for which \( P(L_n(q)) < 4096 \) are as given in Table 4.1.

**Symplectic** We may assume without loss of generality that \( m > 1 \) and \((m, q) \not\in \{(3, 2), (4, 2)\} \), by Theorem 1.5.11. The minimal degree of a non-trivial permutation representation of \( S_{2m}(2) \) is \( 2^{m-1}(2^m - 1) \) for \( m \geq 3 \). With the exception of \( P(S_4(3)) = 27 \), if \( m \geq 2 \) and \( q \geq 3 \) then \( P(S_{2m}(q)) = (q^{2m} - 1)/(q - 1) \).

**Unitary** We may assume without loss of generality that \( n > 2 \) and \((n, q) \not\in \{(3, 2), (4, 2)\} \), by Theorem 1.5.11. If \( q \neq 2 \), 5 then \( P(U_3(q)) = q^3 + 1 \), whilst \( P(U_3(5)) = 50 \). If \( q \neq 2 \) then \( P(U_4(q)) = q^4 + q^3 + q + 1 \). Now let \( n \geq 5 \). When \( n \) is even \( P(U_n(2)) = 2^{n-1}(2^n - 1)/3 \). Otherwise
\[
P(U_n(q)) = (q^n - (-1)^n)(q^{n-1} - (-1)^{n-1})/(q^2 - 1).
\]

**Orthogonal, odd dimension** We may assume that \( m \geq 3 \) and \( q \) is odd, by Theorem 1.5.11. Then \( P(P\Omega_{2m+1}(3)) = 3^m(3^m - 1)/2 \) and for \( q \geq 5 \) the minimal degree is \( P(P\Omega_{2m+1}(q)) = (q^{2m} - 1)/(q - 1) \).

**Orthogonal, plus and minus types** We may assume without loss of generality that \( m \geq 4 \), by Theorem 1.5.11. Then \( P(P\Omega^\pm_{2m}(2)) = 2^{m-1}(2^m - 1) \) and \( P(P\Omega^\pm_{2m}(3)) = 3^{m-1}(3^m - 1)/2 \). For \( \epsilon = + \) and \( q \geq 4 \), or for \( \epsilon = - \) and all \( q \),
\[
P(P\Omega^\epsilon_{2m}(q)) = (q^m - \epsilon)(q^{m-1} + \epsilon)/(q - 1).
\]

Hence the largest values of \( n \) (or \( m \)) and field size, \( q \), of a primitive almost simple classical group \( G \), of degree less than 4096, are as given in Table 4.1.

In general, the primitive almost simple groups with CS socles can be created computationally, by constructing the maximal subgroups of their natural representations and making the action on their cosets. The group \( L_{12}(2) \) is CS, but is too large to deal with in a straightforward manner on a standard machine. This group is treated as a non-CS group in Lemma 4.3.16.

### 4.3.1 Groups with CS socles

We deal with these groups computationally, making use of the following results.
Lemma 4.3.2. Let $G$ be an almost simple group and let $H, K \leq G$. The action of $G$ on the cosets of $H$ is permutation isomorphic to the action of $G$ on the cosets of $K$ if and only if there exists $\alpha \in \text{Aut}(G)$ such that $H^\alpha = K$.

Proof. ($\Leftarrow$) Suppose $H^\alpha = K$ for some $\alpha \in \text{Aut}(G)$ and let $\sigma : \{Hg : g \in G\} \rightarrow \{Kg : g \in G\}$ be given by

$$(Hg)\sigma = (Hg)\alpha$$
$$= (H\alpha)(g\alpha)$$
$$= K(g\alpha).$$

The map $\sigma$ is a bijection, since $\alpha$ is an automorphism. It is easy to check that $\sigma$ is well-defined. Hence, for all $g_1, g_2 \in G$

$$(Hg_1)\sigma(g_2\alpha) = K(g_1g_2)\alpha$$
$$= (Hg_1g_2)\sigma,$$

and the action of $G$ on the cosets of $H$ is permutation isomorphic to the action of $G$ on the cosets of $K$.

($\Rightarrow$) Now suppose the action of $G$ on the cosets of $H$ is permutation isomorphic to the action of $G$ on the cosets of $K$. Then there exists a bijection $\sigma : \{Hg : g \in G\} \rightarrow \{Kg : g \in G\}$ and an automorphism $\alpha$ of $G$ such that, for all $g_1, g_2 \in G$

$$(Hg_1g_2)\sigma = (Hg_1)\sigma(g_2\alpha).$$

Now suppose that $g_1, g_2 \in H$, then

$$(Hg_1g_2)\sigma = H\sigma$$
$$(Hg_1)\sigma(g_2\alpha) = (H\sigma)(g_2\alpha)$$
$$\Rightarrow g_2\alpha \in H\sigma$$
$$\Rightarrow H\alpha \subseteq H\sigma$$
$$\Rightarrow H\alpha = H\sigma,$$

which implies that $H\alpha = K$, since $\alpha$ is an automorphism. \qed

Lemma 4.3.3. Let $G$ be an almost simple group and let $H, K \leq G$. Then $H$ and $K$ are conjugate in $\text{Aut}(G)$ if and only if $H^\alpha = K$ for some $\alpha \in \text{Aut}(G)$.

Proof. Let $\phi : G \rightarrow \text{Inn}(G)$ be the isomorphism given by $\phi : x \mapsto \phi_x$, where $g\phi_x = x^{-1}gx$. Then $H\phi$ is a subgroup of $\text{Inn}(G)$. 

46
Suppose \( H\alpha = K \), for some \( \alpha \in \text{Aut}(G) \). Let \( h \in H \) be arbitrary and let \( k := h\alpha \), then for all \( g \in G \)

\[
g(\alpha^{-1}(h\phi)\alpha) = (h^{-1}(g\alpha^{-1})h)\alpha
= (h\alpha)^{-1}g(h\alpha)
= g((h\alpha)\phi)
= g(k\phi).
\]

Therefore \( \alpha^{-1}(H\phi)\alpha = K\phi \) and hence \( H \) and \( K \) are conjugate in \( \text{Aut}(G) \).

(\( \Rightarrow \)) Now suppose \( \sigma^{-1}(H\phi)\sigma = K\phi \) for some \( \sigma \in \text{Aut}(G) \). Let \( k \in K \) and \( h \in H \), such that \( k\phi = \sigma h\phi\sigma \), then for all \( g \in G \)

\[
g(k\phi) = g(\sigma^{-1}(h\phi)\sigma)
= (h^{-1}(g\sigma^{-1})h)\sigma
= (h\sigma)^{-1}g(h\sigma)
= g(h\sigma)\phi
\]

so \( (H\sigma)\phi = K\phi \) and hence \( H\sigma = K \).

Now Lemma 4.3.2 can be restated as follows.

**Corollary 4.3.4.** Let \( G \) be an almost simple group and let \( H, K \leq G \). The action of \( G \) on the cosets of \( H \) is permutation isomorphic to the action of \( G \) on the cosets of \( K \) if and only if \( H \) and \( K \) are conjugate subgroups of \( \text{Aut}(G) \).

Although the groups are CS, it is impractical to construct all permutation representations of every almost simple group and then check them all for permutation isomorphism. We describe a function \text{ASClassical} which takes as input a simple classical group \( T \) and returns a list \text{groups} of the almost simple classical groups with socle \( T \) and a list of lists \text{maximals}. The latter consists of lists of the maximal subgroups of each group in \text{groups}, where no pair of maximal subgroups is conjugate in \( A := \text{Aut}(T) \). Recall from Lemma 2.2.9 that all primitive groups with socle \( T \) are subgroups of \( \text{Aut}(T) \).

**Algorithm:** \text{ASClassical}

\[
A := \text{Aut}(T);
\]

construct a homomorphism \( \phi : A \to A/T \);

let \text{groups} be the list of preimages under \( \phi \) of groups in \text{Subgroups}(\text{Im}(\phi))

(\text{these are the almost simple groups with socle} \ T, \ \text{up to} \ A\text{-conjugacy});

for \( G \) in \text{groups} do

\[
M := [ ];
\]
maxsG := \{\text{MaximalSubgroups}(G) : T \not\leq M\};
ind := \{[G:M] : M \text{ in maxsG}\};
for i in ind do
  if \(G = A\) then Append\((M, \text{maxsG})\);
  else if \([m \text{ in maxsG} : [G:M] = i]\) has length 1 then
    \(K := \text{maxsG}[1]\);
    Append\((M,K)\);
    delete \(K\) from maxsG;
  else partition the elements of maxsG of index \(i\) by their chief factors;
    for all classes \(C\) of size > 1 in this partition do
      IsConjugate\((A,K_1,K_2)\) for all pairs \([K_1,K_2]\) in \(C\),
      (i.e. check for conjugacy in \(A\));
      append one \(K_i\) per conjugacy class to \(M\);
    end for;
  end if;
end for;
Append\((\text{maximals}, M)\);
end for;

Note that in practice, the number of groups for which we check conjugacy
by hand is small.

We use the following lemma to prove that the maximal subgroups returned
by the above algorithm stabilise different primitive actions, up to
permutation isomorphism.

\textbf{Lemma 4.3.5.} Let \(G\) be an almost simple group with socle \(T\). Then the
group \(\text{Aut}(G) \leq \text{Aut}(T)\).

\textit{Proof.} The group \(T\) is characteristic in \(G\), so every automorphism of \(G\)
induces an automorphism of \(T\). Let \(\rho : \text{Aut}(G) \rightarrow \text{Aut}(T)\) be the homo-
morphism mapping elements of \(\text{Aut}(G)\) to the induced automorphism of \(T\),
and identify \(G\) with \(\text{Inn}(G)\). If \(\ker(\rho)\) were non-trivial then \(T \leq \ker(\rho)\),
as \(T\) is the unique minimal normal subgroup of \(G \leq \text{Aut}(G)\). However,
\(T\) induces \(\text{Inn}(T)\) on \(T\), so \(\rho(T) \cong T\). Hence \(\rho\) is injective and therefore
\(\text{Aut}(G) \leq \text{Aut}(T)\). \(\square\)

By Corollary 4.3.4, two maximal subgroups, \(K_1\) and \(K_2\), of \(G\) are point
stabilisers of permutation isomorphic primitive actions if and only if they are
conjugate in \(\text{Aut}(G)\). Lemma 4.3.5 tells us that if \(K_1\) and \(K_2\) are conjugate
in \(\text{Aut}(G)\), then they are conjugate in \(\text{Aut}(T)\). We now show that the
maximal subgroups returned by the above algorithm are not conjugate in Aut(G).

**Lemma 4.3.6.** Let $G$ be an almost simple group with $T := \text{Soc}(G)$. Then the maximal subgroups of $G$ computed by ASClassical$(T)$ correspond to point stabilisers of faithful primitive actions of $G$, and no pair of these actions is permutation isomorphic.

**Proof.** Recall that the faithful primitive actions of $G$ correspond to conjugacy classes of core-free maximal subgroups of $G$. The function ASClassical returns only the maximal subgroups of $G$ which do not contain $T$, and since $T$ is the unique minimal normal subgroup of $G$, these maximal subgroups are core-free. Hence all of the corresponding actions are faithful.

By Corollary 4.3.4 and Lemma 4.3.5, two maximal subgroups of $G$ are conjugate in Aut($T$) if the actions of $G$ on their cosets are permutation isomorphic. Let $\text{maxs}G$ be the set of maximal subgroups of $G$ up to conjugacy in $G$, and let $\text{maxs}A$ be the set of maximal subgroups of $A := \text{Aut}(T)$ up to conjugacy in $A$. Let $K_1, K_2, \ldots, K_r$ be the groups in $\text{maxs}G$ of index $i$. If $G$ has only one maximal subgroup, $K_1$, of index $i$, then $K_1$ stabilises a unique primitive action, so we store $K_1$. If $G = A$, and no two groups in $\text{maxs}G$ are conjugate in $A$, then no two groups in $\text{maxs}G$ are conjugate in Aut($T$), by Lemma 4.3.5, so we store all of the $K_i$. Otherwise we check for conjugacy by hand, storing one $K_i$ for each conjugacy class.

Thus the subgroups returned by ASClassical$(T)$ are precisely the stabilisers of non-permutation isomorphic, faithful primitive actions of $G$. 

We conclude:

**Theorem 4.3.7.** Let $G \leq \text{GL}_n(q)$ be an almost simple primitive permutation group of degree $d$, where 2500 ≤ $d < 4096$, and with CS socle. Then $G$ appears in Table 4.8 if $G$ is linear and $n = 2$, and 4.9 if $n > 2$.

**Proof.** By Lemma 4.3.1, if $G$ is an almost simple primitive permutation group of degree less than 4096, then $T := \text{Soc}(G)$ is given in Table 4.1. For each CS group $T$ in this table, we compute ASClassical$(T)$ to obtain a list groups of almost simple groups with socle $T$ and a list of lists maximals, where each sublist maximals[i] contains the maximal subgroups of groups[i] of index $d$, where 2500 ≤ $d < 4096$, up to conjugacy in Aut($T$).

We construct the action of each group in groups on the cosets of its maximal subgroups, giving a primitive permutation group of degree $d$, where 2500 ≤ $d < 4096$.

**4.3.2 Groups with non-CS socles : reduction of actions**

For certain of the non-CS classical groups $G$, all maximal subgroups of $G$ of index < 4096 are reducible. Then we can use the algorithms of [6] and [27]
to construct the maximal reducible subgroups of $G$. We make use of the following theorem which combines parts of [37, Theorems 5.1–5.6].

**Theorem 4.3.8.** Let $G$ be a simple classical group and let $X$ be a proper irreducible subgroup of $G$, of largest possible order.

1. Let $G = L_n(q)$ with $n \geq 6$ and $n$ even, then $\text{Soc}(X) = S_n(q)$.

2. Let $G = S_{2m}(q)$, then
   
   (a) if $m = 3$ and $q$ is odd and non-square, then
   $$X = (\text{SL}_2(q) \wr S_3) / \text{Z(} \text{Sp}_6(q)\text{));}$$
   (b) if $m \geq 4$, $m$ is even and $q$ is odd, then $X = S_m(q^2).2$.

3. Let $G = U_n(q)$, then
   
   (a) if $n$ is odd and $q$ is odd, then $\text{Soc}(X) = \Omega_n(q)$;
   (b) if $n$ is odd and $q$ is even, then one of the following holds:
      i. $X = ((\text{GU}_a(q) \wr S_b) \cap \text{SU}_n(q)) / \text{Z(} \text{SU}_n(q)\text{)}$ where $ab = n$ and $a \neq n$;
      ii. $\text{Soc}(X) = U_n(q_0^c)$, where $q_0^c = q$ and $c$ is an odd prime;
      iii. $|X| < q^{2n+4}$.

4. Let $G = \Omega_{2m+1}(q) \cong \text{P} \Omega_{2m+1}(q)$ then $q$ is odd. If $m \geq 3$ then one of the following holds:
   
   (a) $X = (\text{GO}_a(q) \wr S_b) \cap G$, where $ab = 2m + 1$ and $a \notin \{1, 2m + 1\}$;
   (b) $\text{Soc}(X) = \Omega_{2m+1}(q_0)$, where $q_0^c = q$ and $c$ is prime;
   (c) $\text{Soc}(X)$ is isomorphic to $A_{2m+2}$ or $A_{2m+3}$;
   (d) $|X| < q^{3m+6}$.

5. Let $G = \text{PSO}_{2m}^{\pm}(q)$ with $m \geq 6$ and $m$ even, then
   $$X = \text{GU}_m(q).2 / \text{Z(} \text{SO}_{2m}^{\pm}(q)\text{)}.$$ 

6. Let $G = \text{P} \Omega_{12}^{\pm}(2)$, then $G \cong \Omega_{12}^{\pm}(2)$ and $\text{Soc}(X) = A_{14}$.

We now use this theorem to prove the following.

**Proposition 4.3.9.** Let $T$ be one of the following simple classical groups:

$L_6(4), L_6(5), L_8(3), S_6(3), U_8(3), U_7(2), P \Omega_9(3), P \Omega_{12}^{\pm}(2), P \Omega_{12}^{-}(2).$

Then all faithful primitive actions of $T$ of degree less than 4096 are on the cosets of reducible subgroups.

**Proof.** Throughout, let $X$ be a proper irreducible subgroup of $T$, of largest possible order. For each $T$, we find $X$ or an upper bound on the order of $X$, and hence show that $|T:X| > 4095$. We consider the classical types in turn.
Linear  Let $T := \text{L}_n(q)$ with $(n, q) \in \{(6, 4), (6, 5), (8, 3)\}$. For each group, $n$ is even and at least 6, so $\text{Soc}(X) = \text{S}_n(q)$, by Case 1 of Theorem 4.3.8. This implies that $X = N_T(S_n(q)) \leq N_{\text{PGL}_n(q)}(S_n(q)) = \text{PCSp}_n(q)$ (see Subsection 1.5.4 for details of $\text{CSp}_n(q)$). For $(n, q) \in \{(6, 4), (6, 5), (8, 3)\}$

$$|T: X| \geq |T|/|\text{PCSp}_n(q)| > 4095,$$

so in each case the index of the largest order irreducible subgroup is greater than 4095. Hence all subgroups of $T$ of index below 4096 are reducible. The details are given below.

| $T$       | $|T|/|\text{PCSp}_n(q)|$ |
|-----------|--------------------------|
| $L_6(4)$  | $\approx 9 \times 10^7$  |
| $L_6(5)$  | $\approx 3 \times 10^9$  |
| $L_8(3)$  | $\approx 4 \times 10^{12}$ |

Symplectic  Let $T := \text{S}_6(5)$ or $\text{S}_8(3)$. Then by Case 2 of Theorem 4.3.8, the group $X$ is of shape $(\text{SL}_2(5) \wr \text{S}_3)/2$ (since $Z(\text{Sp}_6(5)) = 2$) or $\text{S}_4(9).2$, respectively. In both cases $|T: X| > 4095$, and hence the index of any irreducible subgroup of $T$ is outside our range. The details are given in the table below.

| $T$       | $X$                      | $|T|/|X|$   |
|-----------|--------------------------|------------|
| $\text{S}_6(5)$ | $(\text{SL}_2(5) \wr \text{S}_3)/2$ | $\approx 4 \times 10^7$ |
| $\text{S}_8(3)$ | $\text{S}_4(9).2$         | $\approx 2 \times 10^7$ |

Unitary  Let $T := \text{U}_5(3) \cong \text{SU}_5(3)$, then by Case 3(a) of Theorem 4.3.8, the group $X = N_T(\Omega_5(3)) \leq N_{\text{GL}_5(3)}(\Omega_5(3)) = \text{CO}_5(3)$, (see Subsection 1.5.6 for details of $\text{CO}_n(q)$). Therefore $|T: X| > 4095$. Let $T := \text{U}_7(2) \cong \text{SU}_7(2)$, then one of the cases in Theorem 4.3.8 3.(b) occurs.

i. $a = 1, b = 7$ and $Z(\text{SU}_7(2)) = 1$, so

$$X = (\text{GU}_1(2) \wr \text{S}_7) \cap \text{SU}_7(2)$$

and $|T|/|X| > 4095$;

ii. since $q$ is prime this does not occur;

iii. $|X| < 2^{18}$, so $|T|/|X| > 4095$.

Hence all maximal subgroups of $T$ of index below 4096 are reducible. The details are given below.
Orthogonal, odd dimension  Let $T := PΩ_9(3) ≅ Ω_9(3)$. We are in case 4 of Theorem 4.3.8, and $q$ is prime, so one of the following holds:

(a) $X = (GO_3(3) \rtimes S_3) \cap Ω_9(3)$;
(b) $\text{Soc}(X) \cong A_{10}$ or $A_{11}$;
(d) $|X| < 3^{22} < 4 \times 10^{10}$.

In cases (a) and (d) the index $|T:X| > 4095$. For case (c), the order $|A_{11}|$ does not divide $|T|$, so this is not a subgroup. Let $\text{Soc}(X) = A_{10}$, then by Lemma 2.2.10, the group $X$ embeds in $\text{Aut}(A_{10}) = S_{10}$ and so the index $|T:X| > 4095$. Hence the only maximal subgroups of $T$ of index less than 4096 are reducible. The details are given below.

Orthogonal, even dimension  By Case 5 of Theorem 4.3.8, the proper irreducible subgroup of $T_0 := \text{PSO}_{12}^+(2)$ of largest possible order is $X_0 := GU_6(2)$.2 (since $Z(SO_{12}^+(2)) = 1$). Let $T := \text{Soc}(T_0) = PΩ_{12}^+(2)$, then $X \leq X_0$ and hence $|T:X| \geq |T|/|X_0| \approx 3 \times 10^8$.

Now let $T := Ω_{12}^+(2)$, then by Case 6 of Theorem 4.3.8 the group $\text{Soc}(X) = A_{13}$. By Lemma 2.2.10 the group $X$ embeds in $S_{13}$ and hence $|T:X| \approx 8 \times 10^{10}$. For both groups $T = PΩ_{12}^+(2)$, the index of the largest irreducible maximal subgroup of $T$ is greater than 4095.

Let $T$ be one of the simple groups listed in Proposition 4.3.9. For each almost simple group $G$ with $\text{Soc}(G) = T$, we use the formulae in [32, Section 4.1], corrected in [27], to calculate the orders of the maximal reducible subgroups of $G$. In the next section, we describe the different types of reducible subgroups of a classical group. For each $G$, we determine conjugacy class representatives of reducible subgroups of $G$ which are maximal in $G$ and whose index is $d$, where $2500 \leq d < 4096$. Then we use the algorithms of [6] and [27] to construct generators of each subgroup.
4.3.3 Actions on reducible subgroups

We begin by describing the reducible maximal subgroups of an almost simple classical group. Let $G$ be a matrix group acting on a vector space $V$, and recall that a reducible subgroup of $G$ stabilises some proper, non-trivial subspace of $V$. We describe the different types of maximal subspace stabilisers for each type of classical group and display them in Table 4.2. Recall that a maximal subgroup $M$ of an almost simple group $G$ is a novelty if $M \cap \text{Soc}(G)$ is a proper, non-maximal subgroup of $\text{Soc}(G)$.

Let $V$ be a vector space over $\mathbb{F}_q$ and recall from Definition 1.5.1 that a sesquilinear form $f$ is a map $f : V \times V \rightarrow \mathbb{F}_q$. A vector $v \in V$ is isotropic with respect to $f$ if $f(v,v) = 0$. Let $Q$ be a quadratic form with associated bilinear form $f_Q$, then $v$ is isotropic with respect to $Q$ when it is isotropic with respect to $f_Q$. A vector which is not isotropic is non-isotropic and a subspace all of whose vectors are isotropic is totally isotropic.

Let $Q$ be a quadratic form, then $v$ is singular with respect to $Q$ if $Q(v) = 0$. For sesquilinear forms we do not differentiate between the terms singular and isotropic. A vector which is not singular is non-singular and a subspace $W$ of $V$ is totally singular if all of its vectors are singular. Note that if $f$ is a linear or symplectic form, then $f(v,v) = 0$ for all $v \in V$, hence all vectors are isotropic.

Recall the following definition from Section 1.5.

**Definition 4.3.10.** A sesquilinear form $f$ is non-degenerate if

- for each non-zero $v \in V$, there exists $w \in V$ such that $f(v,w) \neq 0$, and
- for each non-zero $w \in V$, there exists $v \in V$ such that $f(v,w) \neq 0$.

A quadratic form is non-degenerate if its associated symmetric form is non-degenerate. A subspace $W$ is non-degenerate, with respect to the form $f$, precisely when $f|_{W \times W}$ (the restriction of $f$ to $W \times W$) is non-degenerate.

Let $G$ be a linear group and recall from Subsection 1.5.3 that when $n \geq 3$ the group $\text{Aut}(G)$ contains an additional duality automorphism $\iota$, called the inverse transpose automorphism.

The maximal reducible subgroups of an almost simple classical group take one of the forms we are about to describe, by [32, Section 4.1]. Note that the converse is not true, as not all of the reducible groups given correspond to a maximal subgroup for every almost simple group in a cohort.

**Parabolic subgroups** A maximal parabolic subgroup $P_k$ is the stabiliser of a totally singular $k$-space. If $G$ is linear, then the inverse transpose automorphism $\iota$ interchanges the stabilisers in $G$ of the subspaces of $V$ of size $k$ and $n-k$. The subgroups $P_k$ and $P_{n-k}$ are conjugate in $\text{Aut}(G)$, hence
the primitive groups arising from $P_k$ and $P_{n-k}$ are permutation isomorphic, so in this case we let $k \leq n/2$. Let $G$ be a symplectic, unitary or orthogonal group, then all maximal totally singular subspaces of $V$ have dimension at most $n/2$, by [32, Corollary 2.1.7].

Reducible novelties of linear groups Let $G$ be a linear group. We describe two types of reducible subgroups of $G$ which are maximal in $G$ only when $G$ contains $\iota$. A reducible novelty of $G$ occurs as the stabiliser of both a subspace $W \leq V$ of dimension $k$ and a subspace $X \leq V$ of dimension $n - k$, such that $W \cap X = 0$, that is, $X$ is a complement of $W$. This type of novelty has the structure $\text{GL}_k(q) \oplus \text{GL}_{n-k}(q)$.

The group $G$ has another novelty which stabilises both a $k$-dimensional subspace $X$ and a $(n-k)$-dimensional subspace $W$ with $W < X$. This type of novelty is represented in Column 2 of Table 4.2 by $P_{k,n-k}$.

Other reducible maximal subgroups of non-linear classical groups
Let $G$ be an almost simple orthogonal group of even dimension and let $q$ be even. If $W$ is a non-singular 1-dimensional subspace of $V$, then the group $T := \text{Stab}_G(W)$ is potentially maximal in $G$, and $T \cap \text{Soc}(G)$ has shape $\text{Sp}_{n-2}(q)$.

For the remaining maximal subgroups, let $G$ be a symplectic group, a unitary group or an orthogonal group. Then the stabiliser in $G$ of a non-degenerate subspace of $V$ of dimension $k$ is a potential maximal subgroup of $G$.

The details of Table 4.2 are found in [32, Tables 3.5.A-F]. Column 3 of the table gives information about the $k$-dimensional subspace $W \leq V$ to be stabilised, where t.s., n.d. and n.s. denote totally singular, non-degenerate and non-singular, respectively. Column 2 gives an indication of the type of the subgroup $T$ stabilising $W$, as described above. When $T$ is not parabolic, this indication demonstrates the shape of $T$, however the structure of a maximal parabolic subgroup is too complicated to represent in a concise and enlightening way. The notation introduced here will be used again later in the section.

Reducible maximal subgroups of index $d$, where $2500 \leq d < 4096$
For each $T$ given in Proposition 4.3.9, we create a list of almost simple groups $G$, such that $T \leq G \leq \text{Aut}(T)$. For each $G$ we use the algorithms of [6] and [27] to construct generators of a conjugacy class representative for the subgroups described above. For each potentially maximal subgroup $M$, of index $d$ in the range $2500 \leq d < 4096$, we construct the group actions of
Table 4.2: Potentially maximal reducible subgroups

<table>
<thead>
<tr>
<th>Type</th>
<th>Type of maximal</th>
<th>Description</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>L, S, U, PΩ^+</td>
<td>P_k</td>
<td>W t.s.</td>
<td>1 ≤ k ≤ n/2</td>
</tr>
<tr>
<td>PΩ^-</td>
<td>P_k</td>
<td>W t.s.</td>
<td>1 ≤ k &lt; n/2</td>
</tr>
<tr>
<td>L</td>
<td>P_{k,n-k}</td>
<td>W &lt; X</td>
<td>1 ≤ k &lt; n/2</td>
</tr>
<tr>
<td>L</td>
<td>GL_k(q) ⊕ GL_{n-k}(q) W ∩ X = 0</td>
<td>1 ≤ k &lt; n/2</td>
<td></td>
</tr>
<tr>
<td>S</td>
<td>Sp_k(q) ⊥ Sp_{n-k}(q)</td>
<td>W n.d.</td>
<td>k even, 2 ≤ k &lt; n/2</td>
</tr>
<tr>
<td>U</td>
<td>GU_k(q) ⊥ GU_{n-k}(q)</td>
<td>W n.d.</td>
<td>1 ≤ k &lt; n/2</td>
</tr>
<tr>
<td>PΩ_+</td>
<td>GO_k(q) ⊥ GO_{n-k}(q)</td>
<td>W n.d.</td>
<td>ϵ = ±, k odd, 1 ≤ k &lt; n/2</td>
</tr>
<tr>
<td>PΩ^-</td>
<td>GO'<em>k(q) ⊥ GO'</em>{n-k}(q)</td>
<td>W n.d.</td>
<td>ϵ ∈ {+, −, ◦}, k odd ⇒ q odd, 1 ≤ k &lt; n/2</td>
</tr>
<tr>
<td>PΩ±</td>
<td>Sp_{n-2}(q)</td>
<td>W n.s. 1-space</td>
<td>q even</td>
</tr>
</tbody>
</table>

an almost simple group G with socle T on the cosets of M and check to see if the action is primitive. The corresponding primitive groups are given in Table 4.9.

**Linear** Let T := L_n(q) with (n, q) ∈ { (6, 4), (6, 5), (8, 3) }. Recall from Theorem 1.5.13 that for n ≥ 3 the outer automorphism group Out(T) is of shape

\[(n, q - 1):f:2,\]

where q = p^f with p prime. The formulae for |P_k|, where 1 ≤ k ≤ n/2, and for |GL_k(q) ⊕ GL_{n-k}(q)| and |P_{k,n-k}|, where 1 ≤ k < n/2 are found in [32, Propositions 4.1.17, 4.1.4, 4.1.22] and corrected in [27]. The indices are given in the table below. The only reducible subgroups of appropriate index are P_1 ≤ L_6(5) and P_1 ≤ L_8(3), of index 3906 and 3280 respectively. Both of these are maximal and since we require the natural action on the cosets of P_1, we may construct them using Stabilizer(G,1), for each almost simple group T ≤ G ≤ Aut(T).
Symplectic  Let $T := S_n(q)$ with $(n, q) \in \{(6, 5), (8, 3)\}$. Recall from Theorem 1.5.13 that $\text{Out}(T) = 2$ when $q$ is prime. The reducible maximal subgroups of $T$ are $P_k$, where $1 \leq k \leq n/2$, and $\text{Sp}_k(q) \bot \text{Sp}_{n-k}(q)$, where $2 \leq k < n/2$ and $k$ is even. The group orders are calculated using [32, Propositions 4.1.19, 4.1.3] (and [27]) and the indices given in the table below. The subgroups $P_1 \leq S_6(5)$ and $P_1 \leq S_8(3)$ are of index 3906 and 3280, respectively, and both of these are maximal. Since we require the natural actions on the cosets of each $P_1$, we may construct them using $\text{Stabilizer}(G, 1)$ for each almost simple group $T \leq G \leq \text{Aut}(T)$. All other stabilisers have index greater than 4095.
Unitary  Let $T := U_n(q)$ with $(n, q) \in \{(5, 3), (7, 2)\}$. Recall from Theorem 1.5.13 that $\text{Out}(T)$ is of shape $(n, q + 1):2$, when $q$ is prime. The reducible maximal subgroups of $T$ are $P_k$, where $1 \leq k \leq n/2$, and the group of shape $\text{GU}_k(q) \perp \text{GU}_{n-k}(q)$, where $1 \leq k < n/2$. By [32, Propositions 4.1.18, 4.1.4] and [27], the only subgroups of appropriate index are $P_1$ and $\text{GU}_1(2) \perp \text{GU}_6(2)$ in $U_7(2)$, of index 2709 and 2752, respectively: see the table below for details. Both of these are maximal, so we construct the corresponding subgroups in $T$ and $\text{Aut}(T)$, using the algorithms of [6] and [27].

<table>
<thead>
<tr>
<th>$G$</th>
<th>Out($G$)</th>
<th>Subgroup type</th>
<th>Index in $G$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_6(5)$</td>
<td>2</td>
<td>$P_1$</td>
<td>3906</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$P_2$</td>
<td>101556</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$P_3$</td>
<td>19656</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{Sp}_2(5) \perp \text{Sp}_4(5)$</td>
<td>406875</td>
</tr>
<tr>
<td>$S_8(3)$</td>
<td>2</td>
<td>$P_1$</td>
<td>3280</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$P_2$</td>
<td>298480</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$P_3$</td>
<td>918400</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$P_4$</td>
<td>91840</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{Sp}_2(3) \perp \text{Sp}_6(3)$</td>
<td>597780</td>
</tr>
</tbody>
</table>

Orthogonal, odd dimension  Let $T := P\Omega_9(3)$. Recall from Theorem 1.5.13 that $\text{Out}(T) = 2$ when $q$ is prime. The potentially maximal reducible subgroups of $T$ are $P_k$, where $1 \leq k \leq 4$, and $\text{GO}_k(3) \perp \text{GO}_{9-k}(3)$, where $\epsilon \in \{+, -\}$, $1 \leq k < 9$ and $k$ is odd. The group orders are found in [32, Propositions 4.1.20, 4.1.6], corrected in [27], and the indices given in the table below. The subgroups of appropriate index are $P_1$, $\text{GO}_1(3) \perp \text{GO}_8(3)$ and $\text{GO}_1(3) \perp \text{GO}_8(3)$, of index 3280, 3321 and 3240, respectively. All of these are maximal so we construct the corresponding subgroups in $T$ and $\text{Aut}(T)$ using the algorithms of [6] and [27].
<table>
<thead>
<tr>
<th>Subgroup type</th>
<th>Index in $\text{P}\Omega_9(3)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_1$</td>
<td>3280</td>
</tr>
<tr>
<td>$P_2$</td>
<td>$\approx 3 \times 10^5$</td>
</tr>
<tr>
<td>$P_3$</td>
<td>$\approx 9 \times 10^5$</td>
</tr>
<tr>
<td>$P_4$</td>
<td>91840</td>
</tr>
<tr>
<td>$\text{GO}_1(3) \perp \text{GO}_8^+(3)$</td>
<td>3321</td>
</tr>
<tr>
<td>$\text{GO}_3(3) \perp \text{GO}_8^-(3)$</td>
<td>$\approx 2 \times 10^8$</td>
</tr>
<tr>
<td>$\text{GO}_5(3) \perp \text{GO}_8^+(3)$</td>
<td>$\approx 2 \times 10^9$</td>
</tr>
<tr>
<td>$\text{GO}_7(3) \perp \text{GO}_8^+(3)$</td>
<td>$\approx 4 \times 10^6$</td>
</tr>
<tr>
<td>$\text{GO}_1(3) \perp \text{GO}_6^-(3)$</td>
<td>3240</td>
</tr>
<tr>
<td>$\text{GO}_3(3) \perp \text{GO}_6^+(3)$</td>
<td>$\approx 2 \times 10^8$</td>
</tr>
<tr>
<td>$\text{GO}_5(3) \perp \text{GO}_6^-(3)$</td>
<td>$\approx 2 \times 10^9$</td>
</tr>
<tr>
<td>$\text{GO}_7(3) \perp \text{GO}_6^-(3)$</td>
<td>$\approx 2 \times 10^6$</td>
</tr>
</tbody>
</table>

**Orthogonal, even dimension**  Let $T := \text{P}\Omega^{+}_{12}(2)$, then $\text{Out}(T) = 2$ by Theorem 1.5.13. The potentially maximal reducible subgroups of $T$ are: $P_k$, where $1 \leq k \leq 6$; $\text{GO}_k^\epsilon(2) \perp \text{GO}_{12-k}^\epsilon(2)$, where $\epsilon \in \{+, -\}$, $1 \leq k \leq 5$ and $k$ is even; and $\text{Sp}_{10}(2)$. By [32, Propositions 4.1.20, 4.1.6, 4.1.7] and [27], none of these has index in the required range. See the table below for details.

Let $T := \text{P}\Omega^{-}_{12}(2)$, then $\text{Out}(T) = 2$ by Theorem 1.5.13. The potentially maximal reducible subgroups of $T$ are: $P_k$, where $1 \leq k \leq 5$; $\text{GO}_k^\epsilon(2) \perp \text{GO}_{12-k}^{-\epsilon}(2)$, where $\epsilon \in \{+, -\}$, $1 \leq k \leq 6$ and $k$ is even; and $\text{Sp}_{10}(2)$. By [32, Propositions 4.1.20, 4.1.6, 4.1.7] and [27], none of these has index in the required range. See the table below for details.
Table 4.9

<table>
<thead>
<tr>
<th>$G$</th>
<th>Out($G$)</th>
<th>Subgroup type</th>
<th>Index in $G$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Omega_{12}^+(2)$</td>
<td>2</td>
<td>$P_1$</td>
<td>2079</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$P_2$</td>
<td>$\approx 4 \times 10^5$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$P_3$</td>
<td>$\approx 7 \times 10^6$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$P_4$</td>
<td>$\approx 2 \times 10^7$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$P_5$</td>
<td>$\approx 5 \times 10^6$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$P_6$</td>
<td>75735</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$GO_4^+(2) \perp GO_{10}^+(2)$</td>
<td>$\approx 10^6$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$GO_4^+(2) \perp GO_8^+(2)$</td>
<td>$\approx 4 \times 10^9$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$GO_4^+(2) \perp GO_6^+(2)$</td>
<td>$\approx 3 \times 10^5$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$GO_4^+(2) \perp GO_8^+(2)$</td>
<td>$\approx 2 \times 10^9$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$Sp_{10}(2)$</td>
<td>2016</td>
</tr>
</tbody>
</table>

| $\Omega_{12}^-(2)$ | 2        | $P_1$         | 2015         |
|              |          | $P_2$         | $\approx 3 \times 10^5$ |
|              |          | $P_3$         | $\approx 6 \times 10^6$ |
|              |          | $P_4$         | $\approx 10^7$ |
|              |          | $P_5$         | $\approx 2 \times 10^6$ |
|              |          | $GO_2^+(2) \perp GO_{10}^-(2)$ | $\approx 10^6$ |
|              |          | $GO_4^+(2) \perp GO_8^-(2)$ | $\approx 4 \times 10^9$ |
|              |          | $GO_6^+(2) \perp GO_6^+(2)$ | $\approx 5 \times 10^{10}$ |
|              |          | $GO_4^+(2) \perp GO_8^+(2)$ | $\approx 4 \times 10^5$ |
|              |          | $GO_4^-(2) \perp GO_8^-(2)$ | $\approx 2 \times 10^9$ |
|              |          | $Sp_{10}(2)$  | 2080         |

We conclude:

**Theorem 4.3.11.** Let $G$ be a primitive permutation group of degree $d$, for $2500 \leq d < 4096$, and let $\text{Soc}(G)$ be one of the groups

$L_6(4), L_6(5), L_8(3), S_6(5), S_8(3), U_5(3), U_7(2), P\Omega_9(3), P\Omega_{12}^+(2), P\Omega_{12}^-(2)$.

Then $G$ appears in Table 4.9.

**Proof.** By Lemma 2.2.2, Proposition 4.3.9 and Lemma 4.1.2, all faithful primitive actions of $G$ of degree less than 4096 are on the cosets of reducible maximal subgroups. The preceding paragraphs give details of the reducible maximal subgroups of $G$ of index $d$, where $2500 \leq d < 4096$, and for each of these maximal subgroups $M$, we construct the action of $G$ on the cosets of $M$.

4.3.4 Actions on irreducible subgroups

The groups which remain to be analysed are $S_6(4), S_{12}(2), P\Omega_7(5), P\Omega_7^+(3)$ and $L_{12}(2)$. We use Aschbacher’s theorem [1] (see Section 1.6) to classify the primitive permutation representations of degree $d$, where $2500 \leq d < 4096$, 59
for the set of groups containing each of these groups as its socle, except for
the subgroups of the almost simple groups $G$ with socle $\Omega^+_8(3)$, which are
analysed using [31].

Recall that a subgroup of a classical group must fall into at least one of
nine Aschbacher classes $C_i$, with $1 \leq i \leq 9$. Each of the first eight of these
classes has associated to it a geometric structure. The main theorem of [32,
Chapter 3] states that the full stabilisers of these structures in the almost
simple classical groups $G$ are given in [32, Tables 3.5.A-F], apart from those
$G$ inducing a triality automorphism, when $\text{Soc}(G) = \Omega^+_8(q)$, and those $G$
inducing a graph automorphism, when $\text{Soc}(G) = \text{Sp}_4(2^f)$.

We find the maximal subgroups of a group $G$ with socle in
$\{S_6(4), S_{12}(2), P\Omega_7(5), L_{12}(2)\}$ as follows. For each Aschbacher class $C_i$, calculate the
index in $\text{Soc}(G)$ of the stabiliser $M$ in $\text{Soc}(G)$ associated with $C_i$, using the
formulae of [32, Section 4]. If $2500 \leq |\text{Soc}(G):M| < 4096$, then we construct
the subgroup of $G$ corresponding to $M$, determine whether it is maximal and
create the action of $G$ on the cosets of $M$.

We deal with the subgroups of an almost simple group lying in class $C_9$ as
follows. For a group $G$ of Lie type, the absolutely irreducible representations
of $G$ in its defining characteristic within certain bonds are given in [40].
The absolutely irreducible representations of all simple groups that are not
groups of Lie type in defining characteristic are given in [24]. Since all of
the groups we are considering lie within the required bounds, we use these
sources to find all potentially maximal subgroups of $G$ lying in class $C_9$.

The following theorem is adapted from [37, Theorem 4.1].

**Theorem 4.3.12.** Let $T \leq \text{GL}_n(q)$ be a simple classical group and let $G$
be a group such that $T \leq G \leq \text{Aut}(T)$. Let $H$ be a $C_9$ maximal subgroup of $G$
such that $G = HT$. Then one of the following holds:

(i) $H$ is $A_c$ or $S_c$, embedded in $G$, and $c$ is $n + 1$ or $n + 2$.

(ii) $|H| < q^{3n}$.

We use this theorem to prove that $C_9$ contains no maximal subgroup of index
less than 4096, for some of the groups.

**Lemma 4.3.13.** Let $G$ be an almost simple group with socle $T := S_6(4)$. If
$M$ is a maximal subgroup of $G$, of index less than 4096, then $M$ has index
less than 2500.

**Proof.** Note that $\text{Out}(T) = 2$, by Theorem 1.5.13, and $Z(\text{Sp}_6(4)) = 1$. By
[32, Table 3.5.C] Aschbacher classes $C_4, C_6$ and $C_7$ are empty for $S_6(4)$. All
vectors are isotropic.

60
\(C_1: \) By [32, Prop 4.1.19] the subgroups \(P_k\) of \(T\), for \(k \in \{1, 2\}\) have shape
\[
[4^a].3.(\text{PGL}_k(4) \times S_{6-2k}(4)),
\]
where \(a = \frac{1}{2}k(13 - 3k)\). The index \(|T:P_1| = 1365\) and \(|T:P_2| = 23205\). By [27] the group \(P_3\) has shape
\[
[4^6].3.\text{PGL}_3(4),
\]
which has index 5525 in \(T\). By [32, Prop 4.1.3], the stabiliser of a non-degenerate 2-space has shape \(S_2(4) \times S_4(4)\) and index 69888 in \(T\).

\(C_2: \) There is one imprimitive maximal subgroup of \(T\) which has shape \(S_2(4).S_3\), by [32, Prop 4.2.10], and has index \(\approx 3 \times 10^6\).

\(C_3: \) The only maximal subgroup in this class has shape \(S_2(4^3).3\), by [32, Prop 4.3.10], and has index \(\approx 5 \times 10^6\).

\(C_5: \) The stabiliser of a subfield of \(\mathbb{F}_4\) of index 2 has shape \(S_6(2)\), by [32, Prop 4.5.4], and has index \(\approx 3 \times 10^6\).

\(C_8: \) By [32, Prop 4.8.6] the groups in this class are \(\text{PGO}_6^+(4)\) and \(\text{PGO}_6^-(4)\), of index 2080 and 2016, respectively. Both are maximal.

\(C_9: \) From [24] the socle of a potential \(C_9\)-maximal subgroup \(M\), not in defining characteristic, is one of \(\{U_3(3), 2.J_2, 2.L_2(13), 2.L_2(5), 2.L_2(7)\}\). By Lemma 2.2.10 a projectively simple group \(H\) embeds in \(\text{Aut}(\text{Soc}(H))\), so \(|T|/|\text{Aut}(M)|\) gives a lower bound for the index of a maximal \(C_9\) group with socle \(M\). For each group \(M\) in this list \(|T|/|\text{Aut}(M)| > 4095\). From the tables in [40], the groups given in the following table are potential \(C_9\)-maximals in defining characteristic. For each potential maximal subgroup \(M\) we give \(|T|/|\text{Aut}(M)|\). A dash means the quotient \(|T|/|M|\) is not an integer, and hence \(M\) is not a subgroup.

| \(M\)    | \(e\) | \(|T|/|\text{Aut}(M)|\) |
|----------|-------|---------------------|
| \(L_4(2^e)\) | 1     | \(\approx 10^8\) |
|          | 2     | 1040                |
| \(L_6(2^e)\) |       |                      |
| \(U_4(2^e)\) | 1     | \(\approx 8 \times 10^7\) |
|          | 2     | 1008                |
| \(U_6(2^e)\) |       |                      |
| \(S_6(2^e)\) | 1     | \(\approx 3 \times 10^6\) |
| \(G_2(2^e)\) | 2     | 8160                |
Of these groups, only $Aut(U_4(4))$ and $Aut(L_4(4))$ are of index less than 4096. The groups $U_4(4)$ and $L_4(4)$ are of index 2016 and 2080, respectively, so they lie outside our range. □

**Lemma 4.3.14.** Let $G := S_{12}(2)$. If $M$ is a maximal subgroup of $G$ of index $d$, where $2500 \leq d < 4096$, then $M$ is the stabiliser of a totally isotropic 1-space, of index 4095.

**Proof.** Note that $Out(G) = 1$, by Theorem 1.5.13, and $Z(Sp_{12}(2)) = 1$. By [32, Table 3.5.C], there are no groups in Aschbacher classes $C_i$, with $4 \leq i \leq 7$, for $S_{12}(2)$. All vectors are isotropic.

**$C_1$:** The group $P_k$, for $k \in \{1, \ldots, 5\}$, has shape

$$[2^a].(PGL_k(2) \times S_{12-2k}(2)),$$

where $a = \frac{1}{2}k(25 - 3k)$, by [32, Prop 4.1.19]. The group $P_6$ has shape

$$M = [2^{21}].PGL_6(2),$$

by [27]. The indices of these subgroups are given in the following table.

| $k$ | $|G:P_k|$      |
|-----|---------------|
| 1   | 4095          |
| 2   | $\approx 10^6$|
| 3   | $\approx 5 \times 10^7$ |
| 4   | $\approx 2 \times 10^8$ |
| 5   | $\approx 10^8$  |
| 6   | $\approx 5 \times 10^6$ |

By [32, Prop 4.1.3] the stabiliser of a non-degenerate $k$-space has shape $S_k(2) \times S_{12-k}(2)$, where $k$ is even and $2 \leq k < 6$. For $k = 2$ the index of this group is $\approx 10^6$ and for $k = 4$ the index is $\approx 6 \times 10^9$.

**$C_2$:** By [32, Prop 4.2.10] the maximal imprimitive subgroups of $G$ have shape $M = S_k(2) \wr S_{12/k}$, where $k$ is even and $2 \leq k \leq 6$. The indices of these subgroups are given in the following table. None have index less than 4096.

| $k$ | $|G:M|$         |
|-----|----------------|
| 2   | $\approx 6 \times 10^{15}$ |
| 4   | $\approx 9 \times 10^{13}$ |
| 6   | $\approx 5 \times 10^{10}$ |
$C_3$: By [32, Prop 4.3.10] there are two classes of maximal semilinear sub-
groups in $G$. The group $S_6(4).2$ has index $\approx 3 \times 10^{10}$ and $S_4(8).3$ has index $\approx 7 \times 10^{13}$.

$C_8$: By [32, Prop 4.8.6] the maximal classical subgroups of $G$ are $\text{PGO}^+_12(2)$, of index 2080 and $\text{PGO}^-_{12}(2)$, of index 2016.

$C_9$: By Theorem 4.3.12 a maximal $C_9$-subgroup of $G$ either has socle iso-
morphic to one of $A_{13}$, $A_{14}$, $S_{13}$, $S_{14}$ or has order less than $2^{36}$; hence the smallest possible index of such a subgroup is $|S_{12}(2)|/14! > 4095$.

Lemma 4.3.15. Let $M$ be a maximal subgroup of an almost simple group $G$ with socle $T := P\Omega_7(5)$, and suppose $M$ has index less than 4096. Then $M$ stabilises a totally singular 1-space, $|G:M| = 3906$, and $N_S(M \cap T)$ is maximal in all almost simple groups $S$ with socle $T$.

Proof. Note that $\text{Out}(T) = 2$, by Theorem 1.5.13, and $Z(\text{SO}_7(5)) = 1$. By [32, Table 3.5.D] there are no groups in Aschbacher classes $C_i$, with $3 \leq i \leq 8$, for a group with socle $P\Omega_7(5)$.

$C_1$: Let $a := \frac{1}{2}k(13 - 3k)$ and let $\frac{1}{m}H$ denote a subgroup of the group $H$ of index $m$. By [32, Prop 4.1.20] the group $P_k$, for $k \in \{1, 2, 3\}$, has shape

$$M = [5^a].\left(\frac{1}{2}\text{GL}_k(5) \times \Omega_{7-2k}(5)\right).2$$

and $P_3$ has shape $M = [5^6].\frac{1}{2}\text{GL}_3(5)$.

By [32, Prop 4.1.6] a non-degenerate 1-space is stabilised by a group of shape $M = \Omega^{+}_6(5).2$ and the stabiliser of a non-degenerate $k$-space, for $k \in \{3, 5\}$, has shape

$$M = (\Omega_k(5) \times \Omega^{+}_{7-k}(5)).[4].$$

The indices in $T$ of all of the $C_1$ subgroups $M$ are given in the following table.

| $k$ | $M$ | $|T:M|$ |
|-----|-----|--------|
| 1   | $[5^5].(2 \times \Omega_5(5)).2$ | 3906   |
|     | $\Omega^+_5(5).2$               | 7875   |
|     | $\Omega^-_6(5).2$               | 7750   |
| 2   | $[5^7].\left(\frac{1}{2}\text{GL}_2(5) \times \Omega_3(5)\right).2$ | $\approx 10^5$ |
| 3   | $[5^6].\frac{1}{2}\text{GL}_3(5)$ | 19656  |
|     | $(\Omega_3(5) \times \Omega^+_4(5)).[4]$ | $\approx 10^8$ |
|     | $(\Omega_3(5) \times \Omega^-_4(5)).[4]$ | $\approx 10^8$ |
| 5   | $(\Omega_5(5) \times \Omega^+_5(5)).[4]$ | $\approx 6 \times 10^6$ |
|     | $(\Omega_5(5) \times \Omega^-_5(5)).[4]$ | $\approx 4 \times 10^6$ |
$C_2$: By [32, Prop 4.2.15] the maximal imprimitive groups in this class have shape $2^6.A_7$ and index $\approx 10^9$.

$C_9$: By [24] a maximal subgroup in this class, not in defining characteristic, has socle in $\{A_6, S_6(2), L_2(7), L_2(8), U_3(3)\}$. For each group $M$ in this list $|\Omega_2(5)|/|\text{Aut}(M)| > 4095$. The only potential maximal subgroup from [40] is $G_2(5)$, which is isomorphic to its own automorphism group, and has index greater than 4095. 

Lemma 4.3.16. Let $G$ be an almost simple group with socle $T := L_{12}(2)$. If $M$ is a maximal subgroup of $G$ of index $d$, for $2500 \leq d < 4096$, then $M$ is the stabiliser in $G$ of a $1$-space and has index $4095$.

Proof. Note that $\text{Out}(T) = 2$, by Theorem 1.5.13, and $Z(L_{12}(2)) = 1$. Aschbacher classes $C_i$, with $5 \leq i \leq 7$, are empty for groups with socle $L_{12}(2)$, by [32, Table 3.5.A].

$C_1$: The group $P_k$, where $1 \leq k \leq 6$, has shape

$$M_1 = [2^{k(12-k)}].(L_k(2) \times L_{12-k}(2)),$$

by [32, Prop 4.1.17]. The group $\text{GL}_k(2) \oplus \text{GL}_{n-k}(2)$, where $1 \leq k < 6$, has shape

$$(L_k(2) \times L_{12-k}(2)),$$

by [32, Prop 4.1.4]. The group $P_{k,n-k}$, where $1 \leq k < 6$, has shape

$$[2^{2k-3k^2}].(L_k(2)^2 \times L_{12-2k}(2)),$$

by [32, Prop 4.1.22].

The indices of these subgroups are given in the following table.

| $k$ | $|T:P_k|$ | $|T:(\text{GL}_k(2) \oplus \text{GL}_{n-k}(2))|$ | $|T:P_{k,n-k}|$ |
|-----|-----------|-----------------|----------------|
| 1   | 4095      | $\approx 8 \times 10^6$ | $\approx 8 \times 10^6$ |
| 2   | $\approx 3 \times 10^6$ | $\approx 3 \times 10^{12}$ | $\approx 5 \times 10^{11}$ |
| 3   | $\approx 4 \times 10^8$ | $\approx 5 \times 10^{16}$ | $\approx 3 \times 10^{14}$ |
| 4   | $\approx 10^{10}$ | $\approx 6 \times 10^{19}$ | $\approx 3 \times 10^{15}$ |
| 5   | $\approx 10^{11}$ | $\approx 4 \times 10^{21}$ | $\approx 3 \times 10^{14}$ |
| 6   | $\approx 2 \times 10^{11}$ | - | - |

The only maximal reducible subgroup of index $d$, where $2500 \leq d < 4096$, is $P_1$. This group has index 4095 and shape $2^{11}.L_{11}(2)$. 

64
$C_2$: By [32, Prop 4.2.9] the potentially maximal imprimitive subgroups of $T$ have shape $L_k(2)^{12/k}.S_{12/k}$, where $1 \leq k \leq 6$. The indices of these subgroups are all greater than 4095, as the following table shows.

\[
\begin{array}{c|c}
  k & |T:(L_k(2)^{12/k}.S_{12/k})| \\
  \hline
  1 & \approx 10^{34} \\
  2 & \approx 2 \times 10^{35} \\
  3 & \approx 3 \times 10^{32} \\
  4 & \approx 10^{29} \\
  6 & \approx 8 \times 10^{21} \\
\end{array}
\]

$C_3$: By [32, Prop 4.3.6] the potentially maximal $C_3$-subgroups of $T$ are $7.L_4(8).3$, of index $\approx 9 \times 10^{27}$ and $3.L_6(4).3.2$, of index $\approx 10^{21}$.

$C_4$: By [32, Prop 4.4.10] the potentially maximal $C_4$-subgroups of $T$ are $(L_2(2) \times L_6(2))$ and $(L_3(2) \times L_4(2))$. These groups have indices $5 \times 10^{31}$ and $2 \times 10^{36}$, respectively.

$C_8$: By [32, Prop 4.8.3] the potentially maximal $C_8$-subgroup of $T$ is $S_{12}(2)$, which has index $\approx 3 \times 10^{19}$.

$C_9$: By Theorem 4.3.12 a maximal $C_9$-subgroup of $G$ either has socle isomorphic to one of $A_{13}$, $A_{14}$, $S_{13}$, $S_{14}$ or has order less than $2^{36}$; hence the smallest possible index of such a subgroup is $|L_{12}(2)|/14! > 4095$.

\[\square\]

Lemma 4.3.17. If $G$ is a group with socle $\Omega_8^+(3)$, then $G$ has no primitive permutation representation of degree $d$, for $2500 \leq d < 4096$.

Proof. We use the lists of maximal subgroups of $G$ in [31] and [15] to create Table 4.3. Let $T := \Omega_8^+(3)$, then Table 4.3 gives all groups $M \cap T$, such that $M$ is maximal in an almost simple group $G$ with socle $T$, together with the index of $M$ in $G$. This list of groups has been compared to the list of maximal subgroups in [15] (which is not claimed to be complete), and no discrepancy was found. The groups are presented in the structures given by [31]. The group $H$ represents the image of $H \leq \Omega_8^+(3)$ in the group $\Omega_8^+(3)$ and $\frac{1}{m}H$ is a subgroup of $H$, of index $m$.

It is clear from Table 4.3 that no almost simple group with socle $\Omega_8^+(3)$ has a maximal subgroup of index $d$, where $2500 \leq d < 4096$.

\[\square\]

We conclude:

Theorem 4.3.18. The primitive almost simple classical groups of degree $d$, for $2500 \leq d < 4096$, are given in Tables 4.8 and 4.9.
Table 4.3: Maximal subgroups $M$ of groups $G$ with socle $T := PΩ_9^+(3)$

| Subgroups        | $M \cap T$               | $|G:M|$ |
|------------------|---------------------------|--------|
| Ordinary         | $Ω_7(3)$                  | 1080   |
| maximal          | $^3[6] : \left( \frac{1}{2}GL_4(3) \right)$ | 1120   |
| subgroups        | $Ω_8^+(2)$                | 28431  |
|                  | $^3[3] : \left( \frac{1}{2}GL_2(3) \times Ω_4^+(3) \right) . 2$ | 36400  |
|                  | $(2 \times Ω_6^+(3)).2^2$ | 189540 |
|                  | $(L_2(3) \times S_4(3)).2$ | 7960680|
|                  | $(Ω_7^-(3) \times Ω_4^-(3)).2^2$ | 9552816|
|                  | $(Ω_7^+(3) \circ Ω_4^+(3)).2 .2^2$ | 14926275|
| Novelty          | $Ω_9^+(3).2^2$            | 408240 |
| maximal          | $G_2(3)$                  | 1166400|
| subgroups        | $^3[11] : \frac{1}{2}GL_2(3).2^2$ | 582400 |
|                  | $^3[9] : \frac{1}{2}GL_3(3).2$ | 44800  |
|                  | $2^6 : A_8$               | 3838185|
|                  | $2^4 2^2 2^3 : S_4$       | 403009425|
|                  | $[2^9] : L_3(2)$          | 57572775|
|                  | $2^2 (2 \times \frac{1}{2}GU_5(3)).2^2$ | 102351600|
|                  | $(D_{10} \times D_{10}).2^2$ | 12380449536|

Proof. By Lemma 4.3.1 the socle of an almost simple group with minimal degree less than 4096 appears in Table 4.1. Let $G$ be an almost simple group with CS socle. Then by Theorem 4.3.7 the group $G$ appears in Table 4.8, if $G$ is linear and $n = 2$, or Table 4.9, otherwise.

Now assume that $\text{Soc}(G)$ is non-CS. By Theorems 4.3.11, 4.3.13, 4.3.14, 4.3.15, 4.3.16 and 4.3.17, the socle of $G$ is one of $\{ L_6(5), L_6(3), L_{12}(2), S_6(5), S_8(3), S_{12}(2), U_7(2), PΩ_9(3) \}$. The primitive action of $G$ is on the cosets of a reducible maximal subgroup, and $G$ appears in Table 4.9.

Proof.

We now move on to another family of simple groups.

4.4 Exceptional groups

To eliminate duplication of work we restrict our attention to exceptional groups which are not isomorphic to a classical group. Recall that $P(G)$ denotes the smallest $d$ such that $G$ has a faithful primitive permutation action of degree $d$, and by Lemma 4.1.2 the minimal degree $P(\text{Soc}(G)) \leq P(G)$, for all exceptional groups $G$. The untwisted exceptional groups are

$E_6(q), E_7(q), E_8(q), F_4(q), G_2(q)$
and the twisted groups are

\[ 2\text{B}_2(2^{2m+1}) = \text{Sz}(2^{2m+1}), 3\text{D}_4(q), 2\text{E}_6(q), 2\text{F}_4(q), 2\text{G}_2(3^{2m+1}). \]

The orders of each exceptional group are found in [15] and reproduced in Table 4.4.

Let \( G := \text{Ch}(q) \) be a Chevalley group, with \( q = p^e \), and define \( l(G, p) > 1 \) to be the smallest possible degree of a non-trivial projective irreducible representation of \( G \), over a field of characteristic other than \( p \). Then [33] gives a lower bound for \( l(G, p) \). We state these values in Table 4.5, for each simple exceptional group \( G \).

Recall that \( P(G) \) denotes the smallest integer \( d \), such that \( G \) has a faithful primitive permutation representation of degree \( d \).

**Lemma 4.4.1.** Let \( G \) be a simple exceptional group, then a lower bound for \( l(G, p) \) is a lower bound for \( P(G) \).

**Proof.** Let \( d := P(G) \), then \( G \leq S_d \) and we can form a (not necessarily irreducible) permutation representation \( \rho \) of \( G \) by writing each group element as a permutation matrix over any field; so let \( \rho(G) \leq \text{GL}_d(\mathbb{F}_r) \), where \( r \) is coprime to \( |G| \). Since \( G \) is non-abelian and simple, \( \rho(G) \cap Z(\text{GL}_d(\mathbb{F}_r)) = 1 \) and hence \( G \) is isomorphic to a subgroup of \( \text{PGL}_d(\mathbb{F}_r) \). The natural module

| \( G \) | Conditions on \( q \) | \( |G| \) |
|---|---|---|
| \( \text{E}_6(q) \) | \( q^{36}(q^{12} - 1)(q^9 - 1)(q^8 - 1) \) \( (q^6 - 1)(q^3 - 1)(q^2 - 1)/(3, q - 1) \) |
| \( \text{E}_7(q) \) | \( q^{63}(q^{18} - 1)(q^{14} - 1)(q^{12} - 1)(q^{10} - 1) \) \( (q^8 - 1)(q^6 - 1)(q^2 - 1)/(2, q - 1) \) |
| \( \text{E}_8(q) \) | \( q^{120}(q^{30} - 1)(q^{24} - 1)(q^{20} - 1)(q^{18} - 1) \) \( (q^{14} - 1)(q^{12} - 1)(q^8 - 1)(q^2 - 1) \) |
| \( \text{F}_4(q) \) | \( q^{24}(q^{12} - 1)(q^8 - 1)(q^6 - 1)(q^2 - 1) \) |
| \( \text{G}_2(q) \) | \( q^6(q^6 - 1)(q^2 - 1) \) |
| \( \text{Sz}(q) \) | \( q = 2^{2m+1} \) | \( q^2(q^2 + 1)(q - 1) \) |
| \( 3\text{D}_4(q) \) | \( q^{12}(q^8 + q^4 + 1)(q^6 - 1)(q^2 - 1) \) |
| \( 2\text{E}_6(q) \) | \( q^{36}(q^{12} - 1)(q^9 + 1)(q^8 - 1)(q^6 - 1) \) \( (q^5 + 1)(q^2 - 1)/(3, q + 1) \) |
| \( 2\text{F}_4(q) \) | \( q = 2^{2m+1} \) | \( q^{12}(q^6 + 1)(q^4 - 1)(q^3 + 1)(q - 1) \) |
| \( 2\text{G}_2(q) \) | \( q = 3^{2m+1} \) | \( q^3(q^3 + 1)(q - 1) \) |
Table 4.5: $l(G, p)$, for a simple exceptional group $G$

\begin{tabular}{|c|c|}
\hline
$G$ & $l(G, p) \geq$ \multicolumn{1}{c}{Exceptions} \\
\hline
$E_6(q)$ & $q^9(q^2 - 1)$ \\
$E_7(q)$ & $q^{15}(q^2 - 1)$ \\
$E_8(q)$ & $q^{27}(q^2 - 1)$ \\
$F_4(q)$ & $q^4(q^6 - 1), q$ odd \\
 & $\frac{1}{2}q^7(q^3 - 1)(q - 1), q$ even \\
$G_2(q)$ & $q(q^2 - 1)$ \\
$Sz(2^{2m+1})$ & $2^m(2^{2m+1} - 1)$ \\
$3^2D_4(q)$ & $q^3(q^2 - 1)$ \\
$2^2E_6(q)$ & $q^8(q^4 + 1)(q^3 - 1)$ \\
$2^2F_4(2^{2m+1})$ & $2^{2m+4}(2^{2m+1} - 1)$ \\
$2^2G_2(3^{2m+1})$ & $3^{2m+1}(3^{2m+1} - 1)$ \\
\hline
\end{tabular}

Table 4.6: Largest order of a maximal subgroup $M$ of a simple exceptional group $G$

\begin{tabular}{|c|c|c|}
\hline
$G$ & Conditions & $|M| \leq$ \multicolumn{1}{c}{Exceptions} \\
\hline
$G_2(q)$ & $q > 2$ & $q^8(q^2 - 1)(q - 1)$ \\
 & & $q = 3$ and $M = G_2(2)$ \\
 & & $q = 4$ and $M = J_2$ \\
$3^2D_4(q)$ & & $q^{12}(q^6 - 1)(q - 1)$ \\
\hline
\end{tabular}

for the representation $\rho(G)$ has at least one non-trivial composition factor, corresponding to an irreducible submodule of dimension $k$, say. So $l(G, p) \leq k \leq d$.

Table 4.6 presents an upper bound on the order of a maximal subgroup $M$ of $G$, for certain exceptional groups $G$, as given in [38, Theorem 5.2].

We now use the above Lemma to produce a short-list of simple exceptional groups which may be the socle of a primitive permutation group of degree less than 4096.

**Proposition 4.4.2.** Let $G$ be an almost simple exceptional group with minimal degree $P(G) < 4096$. Then $\text{Soc}(G) \in \{E_6(2), F_4(2), G_2(2)', G_2(3), G_2(4), G_2(5), Sz(8), Sz(32), Sz(128), 3^2D_4(2), 2^2E_6(2), 2^2F_4(2)', 2^2G_2(27)\}$.

**Proof.** As before, we use the fact that $P(G) \geq P(\text{Soc}(G))$ for an almost simple group $G$. To begin with we examine the untwisted groups.
E₆(q): By Table 4.5, the minimal degree \( P(E₆(q)) > q^8(q^2 - 1) \), which is greater than 4095 for all \( q > 2 \). The values of \( l(E'http://example.com'), \( p \) and \( l(E₆(q), p) \) are greater than 4095 for all \( q \).

F₄(q): By Table 4.5, the minimal degree

\[
l(F₄(q), p) \geq \min(q^4(q^6 - 1), q^7/2(q^3 - 1)(q - 1)),
\]

which is greater than 4095 for all \( q > 2 \).

G₂(q): By Table 4.6 the largest maximal subgroup of \( G₂(q) \) has index greater than \((q^6 - 1)/(q - 1)\), where \( q > 4 \), and therefore \( P(G₂(q)) > 4095 \) for all \( q > 5 \). The group \( G₂(2) \) is not simple but has simple derived subgroup \( G₂(2)' \cong U₃(3) \). This group was covered in Section 4.3, so we do not consider it further.

Now we analyse the twisted groups.

Sz(\(2^{2m+1}\)): Table 4.5 shows that \( P(Sz(2^{2m+1})) > 4095 \), for \( m \geq 4 \).

\(3^1D₄(q)\): All maximal subgroups of \( 3^1D₄(q) \) have index at least \( q^8 + q^4 + 1 \), by Table 4.6, so for \( q > 2 \) the group \( 3^1D₄(q) \) has no maximal subgroups of index less than 4095.

\(2^2E₆(q)\): The minimal degree \( l(2^2E₆(q), p) \geq q^8(q^4 + 1)(q^3 - 1) \) by Table 4.5, which is greater than 4095 for all \( q > 2 \).

\(2^1F₄(q)\): The minimal degree \( l(2^1F₄(q), p) \geq 2^{9m+4}(2^{2m+1} - 1) \), by Table 4.5, and so \( P(2^1F₄(q)) > 4095 \) for \( m > 0 \). The group \( 2^1F₄(2) \) is not simple, but it has simple derived subgroup \( 2^1F₄(2)' \).

\(2^2G₂(3^{2m+1})\): Lastly, \( 2^2G₂(3) \cong L₂(8):3 \) and the minimal degree

\[
l(2^2G₂(3^{2m+1}), p) \geq 3^{2m+1}(3^{2m+1} - 1),
\]

for \( m > 0 \). If \( m \geq 2 \) then \( P(2^2G₂(3^{2m+1})) > 4095 \), which leaves only \( 2^2G₂(3^2) \).

For each \( G \) in the short-list of Proposition 4.4.2, we examine the maximal subgroups of \( G \) to see if any have index \( d \), where \( 2500 \leq d < 4096 \). The group \( Sz(128) \) is not in [15], so we use the following theorem, which is found in [68, Theorem 9] and classifies the subgroups of \( Sz(q) \).
Theorem 4.4.3. Let $H$ be a subgroup of $G := Sz(q)$ and let $r^2 = 2q$. Then either $H \cong Sz(q_0)$, where $q_0 = q$, or else $H$ is conjugate in $G$ to a subgroup of one of the following.

1. a Frobenius group of order $q^2(q - 1)$;
2. $D_{2(q-1)}$;
3. $N_G(q + r + 1)$, of order $4(q + r + 1)$;
4. $N_G(q - r + 1)$, of order $4(q - r + 1)$.

We now use this theorem to eliminate the group $Sz(128)$ from our investigation.

Lemma 4.4.4. Let $G := Sz(128)$, then $G$ has no subgroups of index less than 4096.

Proof. Since $q = 128$, we assign $r := 16$ and $q_0 := 2$. Let $H \leq G$, then by Theorem 4.4.3 either $H \cong Sz(2)$ and

$$|H| = q_0^2(q_0 - 1)(q_0^2 + 1) = 20,$$

or else the theorem gives an upper bound on $|H|$. These values are given in the table below, together with the resulting lower bounds on the subgroup indices.

| $|H|$ | $|G:H|$ |
|------|--------|
| 20   | $10^9$ |
| $\leq q^2(q - 1)$ | $\geq 16384$ |
| $\leq 2(q - 1)$ | $> 10^8$ |
| $\leq 4(q + r + 1)$ | $> 5 \times 10^7$ |
| $\leq 4(q - r + 1)$ | $> 7 \times 10^7$ |

Hence no subgroup of $G$ has index below 4096.

With the exception of $Sz(128)$, all of the exceptional groups in the short-list of Proposition 4.4.2 are in [15]. We conclude:

Theorem 4.4.5. Let $G$ be an exceptional almost simple group with a faithful primitive permutation representation of degree $d$, where $2500 \leq d < 4096$. Then $\text{Soc}(G) \in \{G_2(3), G_2(5), 2F_4(2)\}$ and these groups are given in Table 4.10.
Proof. By Proposition 4.4.2 and Lemma 4.4.4, the possible values for \( \text{Soc}(G) \) are \( E_6(2), F_4(2), G_2(3), G_2(4), G_2(5), Sz(8), Sz(32), D_4(2), 2E_6(2), 2F_4(2)' \) and \( 2G_2(3^3) \).

The maximal subgroups of \( F_4(2) \) all have index greater than 4096 and \( F_4(2) \) is contained in \( E_6(2) \), by [15]. Hence, neither \( F_4(2) \) nor \( E_6(2) \) has a faithful permutation representation on fewer than 4096 points, for, if \( E_6(2) \) had such a representation then so would its subgroups.

Let \( \text{Soc}(G) \in \{G_2(3), G_2(5), 2F_4(2)\}' \). Then the maximal subgroups of \( G \) are described in [15] and \( G \) has no maximal subgroups of index \( d \), where \( 2500 \leq d < 4096 \). The group \( ^2G_2(3^3) \cong R(27) \), which has no maximal subgroups of index less than 4096, by [15].

The group \( G_2(3) \) has three maximal subgroups of index \( d \), where \( 2500 \leq d < 4096 \), and \( \text{Aut}(G_2(3)) \cong G_2(3).2 \) has no new subgroups of index in that range, by [15]. The indices of the subgroups are 2808, 3159 and 3888.

The group \( G_2(5) \cong \text{Aut}(G_2(5)) \) has two maximal subgroups of index 3906, by [15], and no other maximal subgroups of index less than 4096.

The groups \( ^2F_4(2)' \) and \( \text{Aut}(^2F_4(2)') \) each have a maximal subgroup of index 2925, by [15], and no other maximal subgroups of index \( d \), for \( 2500 \leq d < 4096 \).

Let \( G \) be an almost simple group with \( \text{Soc}(G) \in \{G_2(3), G_2(5), 2F_4(2)\}' \). Then \( G \) is CS and we can compute the primitive permutation representations of \( G \) as in Subsection 4.3.1. \( \square \)

This completes our treatment of the almost simple groups with exceptional socle.

## 4.5 Sporadic Groups

The maximal subgroups of the 26 sporadic groups are described in [15], corrected in [56]. With the exception of the Monster group \( M \), the list of maximal subgroups is complete for each sporadic group.

**Theorem 4.5.1.** Let \( G \) be an almost simple group with sporadic socle. If \( G \) has a maximal subgroup \( M \) of index \( d \), for \( 2500 \leq d < 4096 \), then \( G \) is one of \( J_1, HS, M_{24}, Ru \) or \( Fi_{22} \).

**Proof.** By [15], the order \( |\text{Out}(G)| \leq 2 \) and the sporadic groups \( M_{11}, M_{12}, M_{22}, J_2, M_{23}, J_3, \text{McL}, He, \text{Suz}, O'N, \text{Co}_3, \text{Co}_2, \text{HN}, Ly, \text{Th}, \text{Fi}_{23}, \text{Co}_1, J_4, \text{Fi}'_{24} \) and \( B \) have no maximal subgroups of index \( d \), where \( 2500 \leq d < 4096 \), nor do their automorphism groups. The smallest dimension of an irreducible complex representation of the Monster group \( M \) is 196883, hence \( M \) has no faithful transitive permutation representation of degree less than 4096.
Let $G := J_1$, then $\text{Out}(G) = 1$ and $G$ has a maximal subgroup of shape $S_3 \times D_{10}$ and of index 2926. All other maximal subgroups of $G$ have index outside the required range.

Let $G := HS$, then $\text{Out}(G) = 2$. Let $M$ be a maximal subgroup of an almost simple group with socle $G$, and suppose $2500 \leq |G:M| < 4096$. Then $M \cap G$ has shape $2^4:S_6$ and index 3850.

Let $G := M_{24}$, then $\text{Out}(G) = 1$ and $G$ has a maximal subgroup of shape $2^6:(L_3(2) \times S_3)$ and index 3795. All other maximal subgroups of $G$ have index less than 2500 or greater than 4095.

Let $G := Ru$, then $\text{Out}(G) = 1$ and $G$ has a maximal subgroup of index 4060 and shape $2^{14}.S_6$. All other maximal subgroups of $G$ have index greater than 4095.

Let $G := Fi_{22}$, then $\text{Out}(G) = 2$. Let $M$ be a maximal subgroup of $G$ or $\text{Aut}(G)$, of index less than 4096. Then $M$ has index 3510 and $M \cap G$ has shape $2.U_6(2)$.

We have now considered all of the sporadic groups. All of the relevant almost simple groups $G$ with sporadic socle are in Magma’s database of almost simple groups. Hence we can compute the primitive permutation representations of $G$ as in Subsection 4.3.1. □

We conclude:

**Theorem 4.5.2.** The sporadic groups with faithful primitive permutation representations of degree $d$, for $2500 \leq d < 4096$, are given in Table 4.11.

This completes our classification of the almost simple primitive permutation groups of degree $d$, where $2500 \leq d < 4096$.

### 4.6 Tables

We present the tables of results from the preceding sections.

**Theorem 4.6.1.** Let $G$ be an almost simple primitive permutation group of degree $d$, where $2500 \leq d < 4096$. Then $G$ is contained in one of the tables of this section.

**Proof.** Let $T$ be a non-abelian simple group such that $\text{Soc}(G) \cong T \triangleleft G < \text{Aut}(T)$. Then one of the following holds:

- $T \cong A_n$ for some $n$ and $G$ is in Table 4.7.
- $T \cong L_2(q)$ and $G$ is in Table 4.8.
• $T$ is a classical group and if $T$ is linear, then $n > 2$. The group $G$ is in Table 4.9.

• $T$ is an exceptional group and $G$ is in Table 4.10.

• $T$ is a sporadic group and $G$ is in Table 4.11.

By the Classification of Finite Simple Groups, Theorem 1.3.1, this covers all the possibilities for $T$. \hfill $\blacksquare$

Column 1 of each table gives the smallest group $G$ in the cohort. We give the shape of a stabiliser in $G$ of the primitive action and the normaliser $N := N_{S_n}(T)$, written as an extension of $T := \text{Soc}(G)$. Recall that the rank of a group is the number of orbits of a point stabiliser of the group. This is easy for us to calculate in Magma, and to remain consistent with the lists of primitive groups in [18] and [61] we give the rank of $N$ in each table. The last column gives the number of groups in the cohort.

Table 4.7: Primitive almost simple groups with alternating socle

<table>
<thead>
<tr>
<th>Primitive group $G$</th>
<th>Conditions</th>
<th>Degree $n$</th>
<th>Stabiliser in $G$</th>
<th>$N$ Rank of $N$</th>
<th>Cohort size</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_n$</td>
<td>$72 \leq n \leq 91$</td>
<td>$\binom{n}{2}$</td>
<td>$S_{n-2}$</td>
<td>$T.2$</td>
<td>3</td>
</tr>
<tr>
<td>Out = 2</td>
<td>$26 \leq n \leq 30$</td>
<td>$\binom{n}{3}$</td>
<td>$(A_{n-3} \times 3):2$</td>
<td>$T.2$</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>$18 \leq n \leq 19$</td>
<td>$\binom{n}{4}$</td>
<td>$(A_{n-4} \times A_4):2$</td>
<td>$T.2$</td>
<td>5</td>
</tr>
<tr>
<td>$A_{10}$</td>
<td>2520</td>
<td>$M_{10}$</td>
<td>$T.2$</td>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>$A_{11}$</td>
<td>2520</td>
<td>$M_{11}$</td>
<td>$T$</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>$A_{12}$</td>
<td>2520</td>
<td>$M_{12}$</td>
<td>$T$</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>$A_{14}$</td>
<td>3003</td>
<td>$(A_8 \times A_6):2$</td>
<td>$T.2$</td>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>$A_{15}$</td>
<td>3003</td>
<td>$(A_{10} \times A_5):2$</td>
<td>$T.2$</td>
<td>6</td>
<td>2</td>
</tr>
</tbody>
</table>
Table 4.8: Primitive almost simple groups with socle $L_2(q)$

<table>
<thead>
<tr>
<th>Primitive group $G$</th>
<th>Conditions</th>
<th>Degree</th>
<th>Stabiliser in $G$</th>
<th>$N$</th>
<th>Rank of $N$</th>
<th>Cohort size</th>
</tr>
</thead>
<tbody>
<tr>
<td>$L_2(p)$</td>
<td>$73 \leq p \leq 89$</td>
<td>$\binom{p}{2}$</td>
<td>$D_{p+1}$</td>
<td>$T.2$</td>
<td>$\frac{p+1}{2}$</td>
<td>2</td>
</tr>
<tr>
<td>$L_2(p)$</td>
<td>$71 \leq p \leq 89$</td>
<td>$\binom{p+1}{2}$</td>
<td>$D_{p-1}$</td>
<td>$T.2$</td>
<td>$\frac{p-1}{2}$</td>
<td>2</td>
</tr>
<tr>
<td>$L_2(p)$</td>
<td>$2503 \leq p \leq 4093$</td>
<td>$p+1$</td>
<td>$p:(p-1)/2$</td>
<td>$T.2$</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$L_2(43)$</td>
<td></td>
<td>3311</td>
<td>$A_4$</td>
<td>$T.2$</td>
<td>152</td>
<td>2</td>
</tr>
<tr>
<td>$L_2(71)$</td>
<td></td>
<td>2982</td>
<td>$A_5$</td>
<td>$T$</td>
<td>61</td>
<td>1</td>
</tr>
<tr>
<td>$L_2(p^2)$</td>
<td>$53 \leq p \leq 61$</td>
<td>$p^2+1$</td>
<td>$p^2:(p^2-1)/2$</td>
<td>$T.2^2$</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>$L_2(19^2)$</td>
<td></td>
<td>3439</td>
<td>$PGL_2(19)$</td>
<td>$T.2$</td>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td>$L_2(3^4)$</td>
<td></td>
<td>3240</td>
<td>$D_{82}$</td>
<td>$T.(2 \times 4)$</td>
<td>14</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3321</td>
<td>$D_{80}$</td>
<td>$T.(2 \times 4)$</td>
<td>15</td>
<td>8</td>
</tr>
<tr>
<td>$L_2(5^5)$</td>
<td></td>
<td>$5^5+1$</td>
<td>$5^5:(5^5-1)/2$</td>
<td>$T.10$</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Primitive group $G$</td>
<td>Degree</td>
<td>Stabiliser in $G$</td>
<td>$N$</td>
<td>Rank of $N$</td>
<td>Cohort size</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>--------</td>
<td>------------------</td>
<td>-----</td>
<td>------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>$L_3(5)$</td>
<td>3100</td>
<td>$S_5$</td>
<td>$T.2$</td>
<td>32</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3875</td>
<td>$4^2:S_3$</td>
<td>$T.2$</td>
<td>35</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4000</td>
<td>$31:3$</td>
<td>$T.2$</td>
<td>35</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>$L_3(7).2$</td>
<td>2793</td>
<td>$2^2(L_2(7) \times 2) \cdot 2$</td>
<td>$T. S_3$</td>
<td>10</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>$L_3(13).2$</td>
<td>2562</td>
<td>$[13^3],[48].2$</td>
<td>$T. S_3$</td>
<td>4</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>$L_3(53)$</td>
<td>2863</td>
<td>$53^2,[52],L_2(53).2$</td>
<td>$T$</td>
<td>2</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>$L_3(59)$</td>
<td>3541</td>
<td>$59^2,[58],L_2(59).2$</td>
<td>$T$</td>
<td>2</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>$L_3(61)$</td>
<td>3783</td>
<td>$61^2,[20],L_2(61).2$</td>
<td>$T.3$</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>$L_4(7)$</td>
<td>2850</td>
<td>$[7^4],[6],L_2(7).2$</td>
<td>$T.2^2$</td>
<td>3</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>$L_5(7)$</td>
<td>2801</td>
<td>$[7^4],[6],L_4(7).2$</td>
<td>$T$</td>
<td>2</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>$L_5(5)$</td>
<td>3906</td>
<td>$[5^5]2.L_5(5)$</td>
<td>$T.2$</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>$L_7(2)$</td>
<td>2667</td>
<td>$[2^{10}],(S_3 \times L_5(2))$</td>
<td>$T$</td>
<td>3</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>$L_8(3)$</td>
<td>3280</td>
<td>$[3^7],L_7(3)$</td>
<td>$T.2$</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>$L_{12}(2)$</td>
<td>4095</td>
<td>$[2^{11}],L_{11}(2)$</td>
<td>$T$</td>
<td>2</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>$S_3(3^2)$</td>
<td>3240</td>
<td>$S_3(3^4).2$</td>
<td>$T.2^2$</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3321</td>
<td>$2,(S_3(3^2) \rtimes 2)$</td>
<td>$T.2^2$</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>$S_6(3)$</td>
<td>3640</td>
<td>$3^3 \rtimes 2,(S_4 \times A_4)$</td>
<td>$T.2$</td>
<td>5</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>$S_6(5)$</td>
<td>3906</td>
<td>$[5^5]4,S_4(5)$</td>
<td>$T.2$</td>
<td>3</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>$S_8(3)$</td>
<td>3280</td>
<td>$[3^7]2,S_6(3)$</td>
<td>$T.2$</td>
<td>3</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>$S_{12}(2)$</td>
<td>4095</td>
<td>$[2^{11}],S_{10}(2)$</td>
<td>$T$</td>
<td>3</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>$U_3(2^3)$</td>
<td>3648</td>
<td>$3 \times L_2(8)$</td>
<td>$T.(3 \times S_3)$</td>
<td>5</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>$U_4(3)$</td>
<td>2835</td>
<td>$2,(A_4 \times A_4).2$</td>
<td>$T.D_8$</td>
<td>9</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>$U_4(2^2)$</td>
<td>3264</td>
<td>$5,U_3(4)$</td>
<td>$T.4$</td>
<td>4</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>$U_4(5)$</td>
<td>3276</td>
<td>$[5^5],[12],U_2(5).2$</td>
<td>$T.2^2$</td>
<td>3</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>$U_4(7)$</td>
<td>2752</td>
<td>$[7^4],3.L_3(7^2)$</td>
<td>$T.D_8$</td>
<td>3</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>$U_5(2)$</td>
<td>3520</td>
<td>$S_3 \rtimes 3^1+2,2A_4$</td>
<td>$T.2$</td>
<td>12</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>$U_7(2)$</td>
<td>2709</td>
<td>$[2^{11}],3,U_5(2)$</td>
<td>$T.2$</td>
<td>3</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2752</td>
<td>$3.U_6(2).3$</td>
<td>$T.2$</td>
<td>3</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>$P\Omega_7(3)$</td>
<td>3159</td>
<td>$S_6(2)$</td>
<td>$T$</td>
<td>4</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3640</td>
<td>$3^1+6:,(2A_4 \times A_4).2$</td>
<td>$T.2$</td>
<td>5</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>$P\Omega_7(5)$</td>
<td>3906</td>
<td>$[5^5]2,(2 \times \Omega_5(5)).2$</td>
<td>$T.2$</td>
<td>3</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>$P\Omega_9(3)$</td>
<td>3240</td>
<td>$\Omega_9^-(3).2$</td>
<td>$T.2$</td>
<td>3</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3280</td>
<td>$[3^7],\Omega_7(3).2$</td>
<td>$T.2$</td>
<td>3</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3321</td>
<td>$\Omega_9^+(3).2$</td>
<td>$T.2$</td>
<td>3</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>
Table 4.10: Primitive almost simple groups with exceptional socle

<table>
<thead>
<tr>
<th>Primitive group $G$</th>
<th>Degree $N$</th>
<th>Stabiliser in $G$</th>
<th>Rank $T$</th>
<th>Cohort $2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G_2(3)$</td>
<td>2808</td>
<td>$L_2(8):3$</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>3159</td>
<td>$2^3.L_3(2)$</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>3888</td>
<td>$L_2(13)$</td>
<td>2</td>
<td>12</td>
</tr>
<tr>
<td>$2^{5}.L_3(2)'$</td>
<td>2925</td>
<td>$2^2.[2^8]:S_3$</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>$G_2(5)$</td>
<td>3906</td>
<td>$5^{1+4};GL_2(5)$</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>3906</td>
<td>$5^{2+3};GL_2(5)$</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 4.11: Primitive almost simple groups with sporadic socle

<table>
<thead>
<tr>
<th>Primitive group $G$</th>
<th>Degree $N$</th>
<th>Stabiliser in $G$</th>
<th>Rank $T$</th>
<th>Cohort $2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$J_1$</td>
<td>2926</td>
<td>$S_3 \times D_{10}$</td>
<td>2</td>
<td>67</td>
</tr>
<tr>
<td>$HS$</td>
<td>3850</td>
<td>$2^4.S_6$</td>
<td>2</td>
<td>12</td>
</tr>
<tr>
<td>$M_{24}$</td>
<td>3795</td>
<td>$2^5;(L_3(2) \times S_3)$</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>$Ru$</td>
<td>4060</td>
<td>$2^{5}.L_3(2)$</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>$Fi_{22}$</td>
<td>3510</td>
<td>$2.U_5(2)$</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>
Chapter 5

Product action groups

5.1 Introduction

In this section we classify the primitive product action groups of degree \( d \), where \( 2500 \leq d < 4096 \).

Let \( G \) be a group. The wreath product \( G \wr S_k \) has a natural imprimitive action, however we now define another action of this group on Cartesian products of sets, which is known as the product action.

**Definition 5.1.1.** Let \( G \) be a group acting on a set \( \Delta \), and let \( W := G \wr S_k \). Let \((g_1, \ldots, g_k) \in G^k \) and \( \sigma \in S_k \), then the product action of \((g_1, \ldots, g_k)\sigma \in W \) on \((\delta_1, \ldots, \delta_k) \in \Delta^k \) is defined as follows:

\[
(\delta_1, \ldots, \delta_k)^{(g_1, \ldots, g_k)\sigma} = (\delta_1^{g_1^{-1}}, \ldots, \delta_k^{g_k^{-1}})^{\sigma} = (\delta_1^{g_1\sigma^{-1}}, \ldots, \delta_k^{g_k\sigma^{-1}}).
\]

The O’Nan–Scott Theorem 2.2.1 introduced primitive groups of product action type. Let \( G \) be a primitive permutation group of degree \( d \), with non-regular and non-abelian socle \( H := \text{Soc}(G) \cong T^m \), where \( m \geq 2 \). The group \( G \) is of product action type if \( G \) is permutation isomorphic to a subgroup of a product action wreath product \( P \wr S_{m/l} \). The group \( P \) is primitive of almost simple or diagonal type and \( \text{Soc}(P) \cong T^l \), where \( l \) divides \( m \), and \( l > 1 \) only if \( P \) is of diagonal type. Let \( n \) be the degree of \( P \), then \( G \) has degree \( d := n^m/l \).

Some definitions of product action type groups allow \( P \) to be any primitive group. We restrict the type of \( P \) to almost simple or diagonal, in order to make the O’Nan–Scott classes disjoint. If \( P \) had a regular socle, then \( \text{Soc}(G) \) would also be regular, and hence \( G \) would be of affine or twisted product type. If \( P \) were a product action type group, then \( G \) would be a subgroup of an iterated wreath product isomorphic to a product action group \( P_1 \wr S_m \), where \( P_1 \) is an almost simple or diagonal type group. Hence our restriction does not omit any primitive groups from the classification.

Let \( W \) be the product action wreath product \( P \wr S_{m/l} \), where \( P, m \) and \( l \) are as described above. Let \( H = T^m \), where \( T \) is the non-abelian simple
group such that $\text{Soc}(P) = T^l$, and let $n$ be the degree of $P$. We construct the primitive groups of product action type by computing all groups $G$ of degree $d := n^{m/l}$, where $2500 \leq d < 4096$, such that

$$H \leq G \leq W.$$ 

Then we use Magma to check whether $G$ is primitive. Note that if $G$ is primitive then $W$ is the full normaliser in $S_d$ of $\text{Soc}(G)$, by [19, Lemma 4.5A].

The group $T$ is non-abelian and simple, so $n \geq 5$. The condition $2500 \leq n^{m/l} < 4096$ implies that $m/l \leq 5$, and so the following values can occur:

- $m/l = 2$ and $50 \leq n < 64$;
- $m/l = 3$ and $14 \leq n < 16$;
- $m/l = 5$ and $n = 5$.

The primitive groups of almost simple and diagonal type, of degree less than $64$, are in the primitive groups library of Magma [5]. Table 5.1 presents the primitive groups $P$ of degree $n^{m/l}$ which will give rise to a primitive product action type group $G$, where $m$ and $l$ are as defined above. The table gives the largest group $P$ of its cohort, the degree $n$ of $P$, the values of $m$ and $l$, and the integer $i$ for which $P = \text{PrimitiveGroup}(n, i)$ in Magma.

The only group of diagonal type in this list is $P = A_2^5.2^2$, the socle of which is isomorphic to $A_5 \times A_5$. In this case $l = 2$ and $m = 4$, while for all other groups $l = 1$.

### 5.2 Making the groups

To find the primitive groups of product action type of degree $d$, where $2500 \leq d < 4096$, we perform the following steps in Magma to return a list $\text{PrimGroups}$. Let $P$ be one of the primitive groups given in Table 5.1 and let $m$ and $l$ be as given in the table. Recall that the rank of a group $G$ is the number of orbits of a point stabiliser of $G$. As before, we compute the rank of $W = N_{S_d}(G)$, to remain consistent with the lists of [18] and [61].

**Step 1.** Let $W := \text{PrimitiveWreathProduct}(P, S_{m/l})$, the product action wreath product. Calculate the rank of $W$.

**Step 2.** Use the function $\text{SocleQuotient}(W)$ to compute the quotient group $S := W/\text{Soc}(W)$ and a homomorphism $\phi: W \rightarrow S$.

**Step 3.** Create a list $\text{subs}$ of conjugacy class representatives of subgroups of $S$, using $\text{Subgroups}(S)$. For each $K \in \text{subs}$, construct the preimage $G$ of $K$ under $\phi$. If $\text{IsPrimitive}(G)$ is true, then append $G$ to $\text{PrimGroups}$. 

78
Table 5.1: Almost simple and diagonal type primitive groups $P$ of degree less than 64

<table>
<thead>
<tr>
<th>$P$</th>
<th>$n$</th>
<th>$m$</th>
<th>$l$</th>
<th>$i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_5$</td>
<td>5</td>
<td>5</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>$\text{PGL}_2(13)$</td>
<td>14</td>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>$S_{14}$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$S_6$</td>
<td>15</td>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>$A_7$</td>
<td></td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\text{PSL}_4(2)$</td>
<td></td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$S_{15}$</td>
<td></td>
<td></td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>$\text{PGL}_2(49)$</td>
<td>50</td>
<td>2</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>$U_3(5) : 2$</td>
<td></td>
<td></td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>$S_{50}$</td>
<td></td>
<td></td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>$S_{51}$</td>
<td>51</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>$L_3(3).2$</td>
<td>52</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$S_{52}$</td>
<td></td>
<td></td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>$S_{53}$</td>
<td>53</td>
<td>2</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>$\text{PGL}_2(53)$</td>
<td>54</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>$S_{54}$</td>
<td></td>
<td></td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>$\text{PGL}_2(11)$</td>
<td>55</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>$\text{PGL}_2(11)$</td>
<td></td>
<td></td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>$M_{11}$</td>
<td></td>
<td></td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>$S_{11}$</td>
<td></td>
<td></td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>$S_{55}$</td>
<td></td>
<td></td>
<td>8</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$P$</th>
<th>$n$</th>
<th>$m$</th>
<th>$l$</th>
<th>$i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_8$</td>
<td>56</td>
<td>2</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>$L_3(4).2^2$</td>
<td></td>
<td></td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>$S_{56}$</td>
<td></td>
<td></td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>$L_2(19)$</td>
<td>57</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$L_3(7).3$</td>
<td></td>
<td></td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>$S_{57}$</td>
<td></td>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>$S_{58}$</td>
<td>58</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>$S_{59}$</td>
<td>59</td>
<td>2</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>$A_5.2^2$</td>
<td>60</td>
<td>4</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>$\text{PGL}_2(59)$</td>
<td>2</td>
<td>1</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>$S_{60}$</td>
<td></td>
<td></td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>$S_{61}$</td>
<td>61</td>
<td>2</td>
<td>1</td>
<td>14</td>
</tr>
<tr>
<td>$\text{PGL}_2(61)$</td>
<td>62</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>$S_{62}$</td>
<td></td>
<td></td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>$U_3(3).2$</td>
<td>63</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>$U_3(3).2$</td>
<td></td>
<td></td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>$S_6(2)$</td>
<td></td>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>$L_6(2)$</td>
<td></td>
<td></td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>$S_{63}$</td>
<td></td>
<td></td>
<td>8</td>
<td></td>
</tr>
</tbody>
</table>
Step 5. The size of the set $\text{PrimGroups}$ is the size of the cohort containing $W$. Return $\text{PrimGroups}$, the rank of $W$ and the size of the cohort.

Theorem 5.2.1. Let $G$ be a primitive group of product action type of degree $d$, where $2500 \leq d < 4096$. Then $\text{Soc}(G)$ appears in Table 5.2.

Table 5.2 also gives the rank of $W = \text{N}_{S_d}(G)$ and the size of the cohort to which $G$ belongs.
Table 5.2: Primitive product action groups

<table>
<thead>
<tr>
<th>Socle</th>
<th>Conditions</th>
<th>Degree</th>
<th>Rank of W</th>
<th>Cohort size</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_n^2$</td>
<td>$50 \leq n \leq 63$</td>
<td>$n^2$</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>$L_2(p)^2$</td>
<td>$53 \leq p \leq 61$</td>
<td>$(p + 1)^2$</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>$L_2(49)^2$</td>
<td></td>
<td>2500</td>
<td>3</td>
<td>24</td>
</tr>
<tr>
<td>$U_3(5)^2$</td>
<td></td>
<td>2500</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>$L_3(3)^2$</td>
<td></td>
<td>2704</td>
<td>10</td>
<td>3</td>
</tr>
<tr>
<td>$L_2(11)^2$</td>
<td></td>
<td>3025</td>
<td>21</td>
<td>4</td>
</tr>
<tr>
<td>$L_2(11)^2$</td>
<td></td>
<td>3025</td>
<td>21</td>
<td>3</td>
</tr>
<tr>
<td>$M_2^{11}$</td>
<td></td>
<td>3025</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>$A_{11}^2$</td>
<td></td>
<td>3025</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>$A_8^2$</td>
<td></td>
<td>3136</td>
<td>10</td>
<td>4</td>
</tr>
<tr>
<td>$L_3(4)^2$</td>
<td></td>
<td>3136</td>
<td>6</td>
<td>24</td>
</tr>
<tr>
<td>$L_2(19)^2$</td>
<td></td>
<td>3249</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>$L_3(7)^2$</td>
<td></td>
<td>3249</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>$U_3(3)^2$</td>
<td></td>
<td>3969</td>
<td>10</td>
<td>4</td>
</tr>
<tr>
<td>$U_3(3)^2$</td>
<td></td>
<td>3969</td>
<td>10</td>
<td>4</td>
</tr>
<tr>
<td>$S_6(2)^2$</td>
<td></td>
<td>3969</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>$L_6(2)^2$</td>
<td></td>
<td>3969</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>$(A_5^3)^2$</td>
<td></td>
<td>3600</td>
<td>10</td>
<td>24</td>
</tr>
<tr>
<td>$A_n^3$</td>
<td>$14 \leq n \leq 15$</td>
<td>$n^3$</td>
<td>4</td>
<td>10</td>
</tr>
<tr>
<td>$L_2(13)^3$</td>
<td></td>
<td>2744</td>
<td>4</td>
<td>10</td>
</tr>
<tr>
<td>$A_6^3$</td>
<td></td>
<td>3375</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>$A_7^3$</td>
<td></td>
<td>3375</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>$A_8^3$</td>
<td></td>
<td>3375</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>$A_5^5$</td>
<td></td>
<td>3125</td>
<td>6</td>
<td>26</td>
</tr>
</tbody>
</table>
Chapter 6

Diagonal type groups

6.1 Introduction and preliminary results

In this chapter we describe the primitive permutation groups of diagonal type and show how to compute those of degree \( d \), where \( 2500 \leq d < 4096 \).

Definition 6.1.1. Let \( m > 1 \) and let \( T \) be a group. The diagonal subgroup \( D \) of \( T^m \) is the group of \( m \)-tuples

\[
D := \{ (t, t, \ldots, t) : t \in T \}.
\]

Let \( D \) be the diagonal subgroup of \( T^m \) and consider the action of \( T^m \) on the cosets of \( D \). Each coset may be represented by an element of the form \( (1, x_1, x_2, \ldots, x_{m-1}) \), where \( x_i \in T \). For, if \( (t_1, t_2, \ldots, t_m) \in T^m \), then

\[
D(t_1, t_2, \ldots, t_m) = D(t_1, t_1, \ldots, t_1)(1, t_1^{-1}t_2, \ldots, t_1^{-1}t_m) = D(1, t_1^{-1}t_2, \ldots, t_1^{-1}t_m).
\]

This representation is unique, since

\[
D(1, s_1, \ldots, s_{m-1}) = D(1, t_1, \ldots, t_{m-1})
\]

\[ \Leftrightarrow (1, s_1, \ldots, s_{m-1})(1, t_1, \ldots, t_{m-1})^{-1} \in D \]

\[ \Leftrightarrow (1, s_1t_1^{-1}, \ldots, s_{m-1}t_{m-1}^{-1}) \in D \]

\[ \Leftrightarrow s_it_i^{-1} = 1 \text{ for all } 1 \leq i \leq m - 1 \]

\[ \Leftrightarrow s_i = t_i \text{ for all } 1 \leq i \leq m - 1. \]

Hence the set of cosets of \( D \) in \( T^m \) can be identified with the group \( T^{m-1} \).

Definition 6.1.2. Let \( T \) be a non-abelian simple group and let \( m > 1 \). Then the group \( T^m \) acting on the cosets of its diagonal subgroup \( D \) is the minimal diagonal group and the action is called the diagonal action.
This action has degree $|T^m: D| = |T|^{m-1}$. We write $[1, x_1, \ldots, x_{m-1}]$ for the coset of $D$ in $T^m$ containing $D(1, x_1, \ldots, x_{m-1})$ and let $\Omega$ be the set of all of these cosets.

The group $T^m$ may be extended to obtain more elements of $\text{Sym}(\Omega)$. We adjoin to $T^m$ elements of $S_m$, which act by permuting the co-ordinates, and elements of $\text{Aut}(T^m)$, which act in the obvious way. These extensions create larger diagonal groups, the largest of which is $N_{\text{Sym}(\Omega)}(T^m) \cong T^m: (\text{Out}(T) \times S_m)$, as we shall prove shortly.

Let $\tau \in \text{Inn} T$, where $\tau$ represents conjugation by $y \in T$. Then

$$[1, x_1, \ldots, x_{m-1}]\tau = [1, \tau, x_1\tau, \ldots, x_{m-1}\tau]$$

$$= [y^{-1}y, y^{-1}x_1y, \ldots, y^{-1}x_{m-1}y]$$

$$= [y, x_1y, \ldots, x_{m-1}y],$$

and hence the action of an inner automorphism on a coset is induced by right multiplication by an element of $T$. In other words the action of $T^m$ on $\Omega$ by right multiplication induces all inner automorphisms.

**Lemma 6.1.3.** Let $T$ be a non-abelian simple group and let $m > 1$ be an integer. Let $\Omega$ be as described above and let $T^m$ act on $\Omega$ with the diagonal action. Then $N_{\text{Sym}(\Omega)}(T^m)$ is isomorphic to a subgroup of $\text{Aut}(T^m)$.

**Proof.** Let $N := N_{\text{Sym}(\Omega)}(T^m)$, then by Lemma 2.2.10, the group $N$ embeds in $\text{Aut}(T^m)$. Hence it suffices to prove that $\text{Aut}(T^m) \cong \text{Aut}(T) \wr S_m$. Let $T_i$ be the subgroup of $T^m$ consisting of all elements with $1$ in all but the $i$th entry, then $T_i \cong T$, and as $T$ is simple the $T_i$ are precisely the minimal normal subgroups of $T^m$. An automorphism $\alpha \in \text{Aut}(T^m)$ permutes the $T_i$, and hence

$$(t_1, t_2, \ldots, t_m)\alpha = (t_1\tau_1, t_2\tau_2, \ldots, t_m\tau_m)\sigma,$$

for some $\tau_i \in \text{Aut}(T)$ and some $\sigma \in S_m$. Hence $\alpha = (\tau_1, \tau_2, \ldots, \tau_m)\sigma \in \text{Aut}(T) \wr S_m$. Any element of $\text{Aut}(T^m)$ can be written in this way and any element of $\text{Aut}(T) \wr S_m$ acts as an automorphism of $T^m$.

Considering $\text{Aut}(T^m)$ and $S_m$ as subgroups of $\text{Aut}(T^m)$, the intersection $\text{Aut}(T^m) \cap S_m = 1$, so it remains to prove that $\text{Aut}(T^m) \leq \text{Aut}(T^m)$. It suffices to show that $S_m$ normalises $\text{Aut}(T^m)$, so let $x := (x_1, \ldots, x_m) \in T^m$, let $\tau := (\tau_1, \ldots, \tau_m) \in \text{Aut}(T^m)$ and let $\sigma \in S_m$. Then

$$x(\sigma^{-1}\tau\sigma) = (x_1\tau_1, \ldots, x_m\tau_m)\sigma$$

$$= (x_1\tau_{1\sigma^{-1}}, \ldots, x_m\tau_{m\sigma^{-1}})$$

$$= (x_1, \ldots, x_m)(\tau_{1\sigma^{-1}}, \ldots, \tau_{m\sigma^{-1}}),$$

and $(\tau_{1\sigma^{-1}}, \ldots, \tau_{m\sigma^{-1}}) \in \text{Aut}(T^m)$. Hence $\text{Aut}(T^m) \cong \text{Aut}(T) \wr S_m$ and therefore $N$ is isomorphic to a subgroup of $\text{Aut}(T) \wr S_m$. \hfill $\Box$
We now prove our earlier claim about the structure of the normaliser of \( T^m \) in \( \text{Sym}(\Omega) \).

**Lemma 6.1.4.** Let \( T \) be a non-abelian simple group with associated diagonal group \( D \) and let \( m > 1 \). Let \( \Omega \) be the set of cosets of \( D \) in \( T^m \) and let \( T^m \) act on \( \Omega \) with the diagonal action. Then \( N_{\text{Sym}(\Omega)}(T^m) = T^m \cdot (\text{Out}(T) \times S_m) \).

**Proof.** Let \( H := T^m \) and let \( N := N_{\text{Sym}(\Omega)}(H) \). By Lemma 2.2.10, the normaliser \( N \) embeds in \( \text{Aut}(H) \). Let \( A \) be the image of this embedding, then by Lemma 2.2.11, the group \( A \) consists of the elements of \( \text{Aut}(H) \) which permute the point stabilisers \( H_\omega \), where \( \omega \in \Omega \). Let \( \alpha \in \text{Aut}(H) \), then by Lemma 6.1.3, the element \( \alpha = (\tau_1, \ldots, \tau_m)\sigma \), for some \( \tau_i \in \text{Aut}(T) \) and \( \sigma \in S_m \). Since \( \text{Stab}_H([x_1, \ldots, x_m]) = D^{(x_1, \ldots, x_m)} \), the element \( \alpha \in N \) if and only if

\[
D\alpha = D^{(x_1, \ldots, x_m)}
\]

for some \( x_i \in T \). That is, for any \( t \in T \) there exists \( u \in T \) such that

\[
(t, t, \ldots, t)\alpha = (u^{x_1}, \ldots, u^{x_m})
= (t\tau_1^{-1}, t\tau_2^{-1}, \ldots, t\tau_m^{-1}).
\]

This implies that \( t\tau_i^{-1} = u^{x_i} \), for all \( i \), and therefore \( u = t(\tau_i^{-1} \cdot \phi_{x_i}^{-1}) \), where \( \phi_{x_i}^{-1} \in \text{Inn}(T) \) represents conjugation by \( x_i^{-1} \). Hence

\[
t(\tau_i^{-1} \cdot \phi_{x_i}^{-1}) = t(\tau_j^{-1} \cdot \phi_{x_j}^{-1}),
\]

for all \( i, j \), or in other words \( \tau_i \equiv \tau_j \) (mod \( \text{Inn}(T) \)).

Let \( B \) be a transversal for the cosets of \( \text{Inn}(T) \) in \( \text{Aut}(T) \), then each element of \( B \) uniquely represents an element of \( \text{Out}(T) \) and

\[
A = \{(x_1b, \ldots, x_mb)\sigma : x_i \in T, b \in B, \sigma \in S_m\}.
\]

Hence \( N = T^m \cdot (\text{Out}(T) \times S_m) \). \( \square \)

We are now ready to state the definition of a group of diagonal type.

**Definition 6.1.5.** Let \( T \) be a non-abelian simple group and let \( m > 1 \). A group \( G \) is of **diagonal type** if \( T^m \leq G \leq T^m \cdot (\text{Out}(T) \times S_m) \) with the diagonal action described above.

Note that the degree of a group of diagonal type is equal to the degree of its socle \( d = |T|^{m-1} \). The following theorem, found in [19, Theorem 4.5A], gives conditions on the values of \( m \) for a group of diagonal type to be primitive.

**Theorem 6.1.6.** Let \( G \) be a group of diagonal type with socle \( T^m \). Then \( G \) is primitive exactly when either
1. \( m = 2 \); or

2. \( m \geq 3 \) and the conjugation action of \( G \) on the set of minimal normal subgroups of \( T^m \) is primitive.

In particular, the full normaliser of \( T^m \) is primitive for all \( m \geq 2 \).

Since we are only interested in the primitive groups of degree \( d \), where \( 2500 \leq d = |T|^{m-1} < 4096 \), the following table gives the simple groups \( T \) which may form the socle \( T^m \) of a primitive group of degree \( d \).

<table>
<thead>
<tr>
<th>( T )</th>
<th>( m )</th>
<th>( d )</th>
<th>( \text{Aut}(T) )</th>
<th>( \text{Out}(T) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( A_7 )</td>
<td>2</td>
<td>2520</td>
<td>( S_7 )</td>
<td>2</td>
</tr>
<tr>
<td>( L_2(19) )</td>
<td>2</td>
<td>3420</td>
<td>( \text{PGL}_2(19) )</td>
<td>2</td>
</tr>
<tr>
<td>( A_5 )</td>
<td>3</td>
<td>3600</td>
<td>( S_5 )</td>
<td>2</td>
</tr>
<tr>
<td>( L_2(16) )</td>
<td>2</td>
<td>4080</td>
<td>( \text{PGL}_2(16) )</td>
<td>4</td>
</tr>
</tbody>
</table>

### 6.2 Making the groups

Let \( T \in \{ A_7, L_2(19), L_2(16) \} \), then all groups \( G \) of diagonal type with \( \text{Soc}(G) = T^2 \) are primitive, by Theorem 6.1.6. For the remaining case, where \( T = A_5 \) and \( m = 3 \), let

\[ R := (A_5)^3(2 \times S_3) \]

and let \( G \leq R \) be primitive. Then the action of \( G \) by conjugation on the minimal normal subgroups of \( (A_5)^3 \) is primitive, by Theorem 6.1.6. Under the action of \( G \), the minimal normal subgroups of \( (A_5)^3 \) are fixed by \( (A_5)^3 \).2 and permuted by a subgroup of \( S_3 \). The only primitive subgroups of \( S_3 \) are itself and \( A_3 \), hence \( G \) is a primitive subgroup of \( R \) if and only if \( G/\text{Soc}(G) \) contains an element of order 3.

Let \( U := \text{Aut}(T) \wr S_m \), and let \( W := T^m, (\text{Out}(T) \times S_m) \) be a primitive group of diagonal type. Then \( W \) is isomorphic to a subgroup of \( U \), of index \( |\text{Out}(T)|^{m-1} \), and \( U \) is much easier to construct in MAGMA than \( W \). The group \( W \) has degree \( d := |T|^{m-1} \), and a point stabiliser of \( W \) has index \( d \) in \( W \). We find \( W \) by computing the subgroups of \( U \) of index \( |\text{Out}(T)|^{m-1} \) and which have a maximal subgroup of index \( d \).

We now describe a computational method to construct the primitive groups of diagonal type of degree \( d \), where \( 2500 \leq d < 4096 \).

#### Step 1.
Let \( m := 2 \) and \( T \in \{ A_7, L_2(19), L_2(16) \} \) or let \( m := 3 \) and \( T := A_5 \).

#### Step 2.
Let \( U := \text{Aut}(T) \wr S_m \).
Step 3. Let \( \Lambda := \{ K \leq U : |U : K| = |\text{Out}(T)|^{m-1} \} \) and check that there is a unique group \( W \) (up to isomorphism) in \( \Lambda \) with a maximal subgroup \( M \) of index \( |T|^{m-1} \).

Step 4. Let \( \text{maxs} \) be the set of conjugacy class representatives for maximal subgroups of \( W \), of index \( |T|^{m-1} \). Then each subgroup in \( \text{maxs} \) is a point stabiliser of the diagonal action. Calculate the rank of \( W \) by counting the number of orbits of one of the groups in \( \text{maxs} \).

Step 5. Let \( H, K \in \text{maxs} \). The actions of \( W \) on the cosets of \( H \) and \( K \) are primitive, so by Lemma 2.2.8, these actions are permutation isomorphic if and only if they are conjugate in \( \text{Aut}(W) \). Check that the groups in \( \text{maxs} \) are conjugate in \( U = \text{Aut}(T) \wr S_m \), then they are conjugate in \( \text{Aut}(W) \).

Step 6. Let \( R \) be the permutation representation of \( W \) acting on the cosets of \( M \). Let \( S := R/\text{Soc}(R) \) and let \( \phi : R \to S \) be a homomorphism.

Step 7. If \( m = 2 \), then calculate all subgroups of \( S \) and return the subgroups of \( R \) given by their preimages in \( \phi \).

Step 8. If \( m = 3 \), then return the preimages in \( \phi \) of all subgroups \( G \) of \( S \) such that \( G/\text{Soc}(G) \) contains an element of order 3.

Step 9. The number of subgroups returned for each \( T \) is the size of the cohort containing \( T^m \).

We conclude:

**Theorem 6.2.1.** Let \( G \) be a primitive permutation group of diagonal type of degree \( d \), where \( 2500 \leq d < 4096 \), then \( \text{Soc}(G) \) is given in Table 6.1.

Also given in Table 6.1 are the rank of \( W := T^m.(\text{Out}(T) \times S_m) \) and the size of the cohort containing \( G \). This concludes our classification of the primitive groups of diagonal type of degree \( d \), where \( 2500 \leq d < 4096 \).
Table 6.1: Primitive diagonal type groups

<table>
<thead>
<tr>
<th>Socle</th>
<th>Degree</th>
<th>Rank of $W$</th>
<th>Cohort size</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_2^7$</td>
<td>2520</td>
<td>8</td>
<td>5</td>
</tr>
<tr>
<td>$L_2(19)^2$</td>
<td>3420</td>
<td>11</td>
<td>5</td>
</tr>
<tr>
<td>$A_3^3$</td>
<td>3600</td>
<td>17</td>
<td>5</td>
</tr>
<tr>
<td>$L_2(16)^2$</td>
<td>4080</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>
Chapter 7

Loose ends

7.1 A group missing from previous databases

Thomas Breuer has pointed out to us that the classification in [61] omits a cohort of 2 groups of degree 1575 with socle $\text{PSU}_4(5)$, point stabiliser $\text{Sp}_4(5).2$, and rank 4. We thank him for drawing this to our attention.

7.2 Permutation isomorphism of groups

We check the primitive groups that have been computed for permutation isomorphism, to ensure there are no duplicates. The following theorem shows that we need only check for permutation isomorphic groups within an O’Nan–Scott class.

Lemma 7.2.1. A faithful primitive group $G$ belongs to exactly one O’Nan–Scott class.

Proof. The socle of $G$ is abelian if and only if $G$ is of affine type. The socle of $G$ is non-abelian and regular if and only if $G$ is a twisted wreath product. The socle of $G$ is non-abelian and simple if and only if $G$ is an almost simple group.

Thus we assume that $\text{Soc}(G) \cong T^m$, for some non-abelian simple group $T$ and $m \geq 2$, with non-trivial point stabilisers. It suffices to show that if $H \cong G$, and $H$ is primitive of the same degree as $G$, then $H$ and $G$ are not of product action and diagonal type, respectively. Assume otherwise, then

$$T^m \leq G \leq T^m:(\text{Out}(T) \times S_m)$$

and $T^m \cong R^k \leq H \leq P^k:S_k$, where $P$ is a primitive group of almost simple or diagonal type, $k > 1$ divides $m$ and $\text{Soc}(P) = R \cong T^{m/k}$. If $P$ is almost simple, then $H_{(\alpha,\ldots,\alpha)} = P_{\alpha} S_k$, whereas $G_{(\alpha,\ldots,\alpha)} \cong \text{Aut}(T) \times S_m$. The groups $H_{(\alpha,\ldots,\alpha)}$ and $G_{(\alpha,\ldots,\alpha)}$ are not isomorphic, as only one is a direct
product, so we have a contradiction. Thus $P$ is of diagonal type, the group $R \cong T^l$ for some $l = m/k > 1$, and $P$ has degree $|T|^{l-1}$. Now $\text{Soc}(G) \cong T^{kl}$ and $G$ has degree $|T|^{kl-1}$, however the degree of $H$ is $|(T|^{l-1})^k = |T|^{kl-k}$, so $G$ is not isomorphic to $H$.

For each O’Nan–Scott class, we check the groups of the same degree for permutation isomorphism using the same methods as [61]. The signature of a group $G$ is the following list of properties: the order of $G$, the largest integer $k$ such that $G$ acts $k$-transitively, the multiset of orbit lengths of the $k$-point stabiliser of $G$, the multiset of chief factors of $G$ and the orders of all groups in the derived series of $G$. Adding to the signature the multisets of isomorphism types of all abelian groups that both occur as quotients in the derived series of $G$ and are in the small groups library of MAGMA we obtain the extended signature of $G$.

Let $L$ be a list of groups of the same degree in a particular O’Nan–Scott class. We partition the groups in $L$ using their signatures and delete from $L$ any groups in a class of size 1. Next we compute the Sylow 2-subgroup $S$ of each group in $L$ and repeat the process, now using the extended signature of $S$, again discarding the groups in equivalence classes of size 1. Now the point stabiliser and derived subgroup of the remaining groups in $L$ are computed and the groups are again partitioned by their extended signature. The number of groups remaining after this step is small enough for us to check by hand that no two groups are permutation isomorphic. This test was carried out for each collection of groups of the same degree inside an O’Nan–Scott class.

7.3 Accuracy checks and assumptions

Where there are families of groups in [61] (such as $\{A_n : 5 \leq n \leq 71\}$) which can be extended to include groups of degree $d$, where $2500 \leq d < 4096$, the parameters of the smallest group of the new family were compared to those of the largest member of the existing family to ensure there are no omissions. We have made extensive use of [32], each time checking with [27] for discrepancies, and in particular have assumed the results of Chapter 4 to be accurate. The primitive permutation groups of degree less than 2500 given in [61] are assumed to be correct without rechecking, although see Section 7.1 for an error that has been found in [61]. The other main references whose accuracy has been relied upon are [37, Theorems 5.1–5.5] for bounds on the orders of maximal irreducible subgroups of classical groups, [24] and [40] for the $C_9$ subgroups of classical groups, [31] for the maximal subgroups of $\text{PGL}_d(3)$, [33] for bounds on degrees of permutation representations of the exceptional groups and [38, Theorem 5.2] for bounds on the orders of maximal subgroups of some exceptional groups. We frequently used [15] and

89
each time consulted [56] to ensure accuracy.

To avoid computational errors, we have run several versions of the code and checked that the results agree. When using [27] to construct the maximal reducible subgroups of a group, we ensured maximality by checking that the groups arising from them are primitive. The groups declared to be CS and the primitive groups database have been in use in MAGMA for a number of years. Note that we favour automated methods over hand checking to reduce the risk of human error.

This completes our classification of the primitive permutation groups of degree $d$, where $2500 \leq d < 4096$. This work is presented in [16].

7.4 Further work

Maximal subgroups of $A_n$ and $S_n$. In the process of computing the primitive permutation groups we have computed the primitive maximal subgroups of $A_n$ and $S_n$, for certain values of $n$. These groups will be added to the databases of MAGMA and GAP.

Extending the classification further. Similar methods to those used here could be employed to extend the classification of primitive permutation groups to higher degrees. In addition to the classes covered here, the primitive groups of degree $60^6$ and greater will include groups of twisted wreath product type.

The most significant hurdles are likely to arise from the non-CS almost simple groups, especially those of the form $Sp_4(2^e)$ and $P\Omega_8^+(q)$ not covered by Aschbacher’s theorem. In addition, the construction of the affine type primitive groups of degree 4096 will require the computation of the irreducible subgroups of $GL_{12}(2)$.

This concludes Part I of this thesis.
Part II

Normalisers of matrix groups
Chapter 8

Background and introduction

8.1 History and motivation

Part II of this thesis is concerned with the use of computational methods to find the normaliser in $\text{GL}_n(q)$ of a matrix group $G \leq \text{GL}_n(q)$. This work forms part of the Matrix Group Recognition Project [35], which is an international research project whose aim is to produce efficient algorithms for solving problems with matrix groups over finite fields. As we will see later, calculating normalisers is at least as computationally hard as problems like finding group centralisers, intersections of groups, and elements conjugating one subgroup to another [41], and existing methods for computing normalisers of matrix groups are rather inefficient.

We shall briefly describe some methods used in permutation group computation, before focusing on the normaliser problem and finally discussing some developments in computing with matrix groups. In this section we denote the action of a group on a set by exponential notation and we write $[a_1, \ldots, a_n]$ for a sequence, to avoid confusion with permutations. Background material for this section has been taken from [64].

8.1.1 Base and strong generating set

Computational problems in group theory often involve seeking elements of a group satisfying a given property. Since searching a list of elements is inconvenient for all but the smallest groups, it is useful to have a systematic way of representing a group. Sims first introduced the concept of a \textit{base and strong generating set} (BSGS) in [66] and [67]. Let $G$ be a permutation group acting on the set $\Omega$. A sequence of points $B := [\beta_1, \beta_2, \ldots, \beta_k]$ is a base for $G$ if the only element of $G$ whose action fixes all of the $\beta_i$ pointwise is $\text{id}_G$; for example, a base for the symmetric group $S_n$ is $[1, 2, \ldots, n − 1]$.

Each element $g \in G$ is uniquely determined by its base image

$$[\beta_1, \ldots, \beta_k]^g := [\beta_1^g, \ldots, \beta_k^g],$$
for if \( g_1, g_2 \in G \) have the same base image then the action of \( g_1 g_2^{-1} \) fixes all of the \( \beta_i \), and hence \( g_1 = g_2 \). As an example, let \( G = S_3 \) with base \([1, 2]\), then the base image \([1, 3]\) corresponds to the element \((23)\). This gives a very efficient and concise way of representing elements of a permutation group.

Define \( G^{(i)} \) to be the pointwise stabiliser in \( G \) of the set \([\beta_1, \ldots, \beta_i]\), for \( 1 \leq i \leq k \), and let \( G^{(0)} := G \). We call \( \beta_i^{G^{(i-1)}} \) a basic orbit, and it is the size of the basic orbits which determines the level of performance when computing with bases, as we will see shortly.

A strong generating set for \( G \) is a set \( S \subset G \) such that \( G^{(i)} = \langle S \cap G^{(i)} \rangle \), for each \( 0 \leq i \leq k \). Sims \([66, 67]\) presented a deterministic algorithm, now called Schreier–Sims, which uses Schreier’s lemma to construct strong generating sets for base point stabilisers. In 1980, Leon \([36]\) created the random Schreier–Sims algorithm, which finds smaller strong generating sets using random group elements rather than Schreier generators. In practice, this method is typically much faster than the original \([64, \text{Theorems 4.2.4, 4.5.5}]\).

Let \( G \) be a group with base \( B := [\beta_1, \ldots, \beta_k] \). The base images of all initial segments of \( B \) correspond to cosets of \( G \), and these cosets obey a partial order by inclusion. We use this to define a search tree \( T \) for \( G \). For \( i \in \{1, \ldots, k\} \), the \( i \)-th level is labelled by the base images \([\beta_1, \ldots, \beta_i]^g\), for \( g \in G \), where \( g = \text{id}_G \) for the leftmost node of the level. This base image is identified with the coset of \( G^{(i)} \) in \( G \) which contains \( g \), that is the coset consisting of all \( h \in G \) for which \([\beta_1, \ldots, \beta_i]^h = [\beta_1, \ldots, \beta_i]^g \). Note that when \( g = \text{id}_G \) this coset is \( G^{(i)} \) and the root of \( T \) corresponds to \( G \) itself. The leaves of the tree are the base images \([\beta_1, \ldots, \beta_k]^g\), each corresponding to a distinct element \( g \in G \).

**Example 8.1.1.** Let \( G := S_3 \) with base \([1, 2]\). A strong generating set for \( G \) is \( \{\text{id}_G, (2 3), (1 3)\} \) and a search tree for \( G \) is as follows.

```
G = S_3

[1] {id_G, (2 3)}
[2] {(1 2), (1 2 3)}
[3] {(1 3), (1 3 2)}

[1, 2] {id_G}
[1, 3] {(2 3)}
[2, 1] {(1 2)}
[2, 3] {(1 2 3)}
[3, 1] {(1 3 2)}
[3, 2] {(1 3)}
```

The sets below the base images are the cosets of \( G^{(i)} \) in \( G \) as described above.

Using this example, we can see how the efficiency of an algorithm depends
on the basic orbit size, since a group with larger basic orbits corresponds to a wider tree.

8.1.2 Backtrack search

Representing a group $G$ by a tree enables the systematic traversal of $G$ by a search algorithm. One such algorithm is backtrack search, also called depth first search, whereby each branch is explored as far as possible before backtracking. More formally: Start at the root. At each node reached, travel to the first (leftmost) child of that node which has not been visited. If there are no unvisited children then travel back up the branch to the previous parent node and look for unvisited children of this node. The algorithm terminates when it returns to the root node and this node has no unvisited children.

When searching the tree defined above by this method, the whole of $G^{(i)}$ is traversed before processing $G \setminus G^{(i)}$. Note that when searching a tree $T$ we do not need to construct and store $T$ explicitly, since we can traverse the branches while constructing and discarding nodes as necessary.

Pruning

Let $G(P)$ be the set of elements of a group $G$ which satisfy property $P$. For many problems of practical interest, the elements of $G(P)$ form a subgroup or a coset of a subgroup of $G$. For coset type problems, such as determining whether there exists an element conjugating one subgroup to another, we need only find one element of the coset, while subgroup type problems usually require all of the elements to be found. From now on we assume that the elements satisfying $P$ form a subgroup, as they do when $P$ is “normalises the subgroup $H$”.

In the course of a search, sometimes information about one element of a coset can eliminate the rest of the coset from the search, and by removing redundant branches of the tree, or pruning, we can improve computational efficiency. There are several property-independent techniques that can be used to prune the search.

Let $T$ be the search tree of a group $G$ and define a function $\phi$ from $T$ to the power set of $G$ by

$$[\gamma_1, \ldots, \gamma_m] \phi = \{ g \in G \mid \beta_i^g = \gamma_i \text{ for } 1 \leq i \leq m \}. $$

In other words, $[\gamma_1, \ldots, \gamma_m] \phi$ is the coset of $G^{(m)}$ corresponding to the sequence of base point images, as indicated by the labelling of the nodes in Example 8.1.1. The following is an example of property-independent pruning.
Lemma 8.1.2. Let $G$ be a group with search tree $T$, let $\phi$ be as described above and let $\mathcal{P}$ be a subgroup property. Suppose we are searching $T$ for elements with $\mathcal{P}$ and the backtrack search has reached the node $t := [\gamma_1, \ldots, \gamma_m]$ of $T$, for some $m \in \{1, \ldots, k\}$. Let $K$ be the subgroup of $G^{(m)}$ whose elements satisfy property $\mathcal{P}$. If any $g \in t\phi$ is found that satisfies $\mathcal{P}$, then $\langle K, g \rangle$ contains all elements of the coset $t\phi$ that satisfy $\mathcal{P}$, and the search need not examine the rest of the subtree rooted at $t$.

Proof. Let $h$ be another element of $t\phi$ satisfying $\mathcal{P}$. The coset $t\phi = G^{(m)}g = G^{(m)}h$, so $hg^{-1} \in K$ and therefore $h \in Kg$. The children of $t$ correspond to cosets within $t\phi$, so $\langle K, g \rangle$ contains all elements in $s\phi$ satisfying $\mathcal{P}$, for any $s < t$. \hfill \Box

In [64], there are described a number of other property-independent pruning techniques. The property $\mathcal{P}$ may imply restrictions on the base images of elements of $G(\mathcal{P})$, enabling the development of property-dependent pruning techniques. We will discuss pruning methods relevant to the normaliser problem shortly.

Obviously it is preferable to prune a branch as close to the root as possible and the most effective pruning arises from property restrictions which make use of the relationships between base points. Hence we can construct a more efficient search tree through a careful choice of base points. However, there is a balance to be struck between the computational expense of obtaining more efficient base points and that of unrefined searching.

8.1.3 Normalisers

In complexity theory, a reduction is a transformation of one problem into another. An algorithm is said to be in polynomial time if it is computable by a deterministic Turing machine in time bounded above by a polynomial in the size of the input, and this is a desirable property for group theoretical algorithms.

Many problems in computational group theory, such as finding group centralisers and intersections of groups, can be reduced to each other in polynomial time. There is a polynomial time reduction for the centraliser problem to the normaliser problem [41], however, the reverse has no known reduction in polynomial time. The first algorithm for dealing with normalisers of permutation groups was presented in 1983 by Butler [9] and was based on the fact that an element $g \in \text{Sym}(\Omega)$ which normalises a group $H \leq \text{Sym}(\Omega)$ must also fix certain structures determined by the action of $H$.

Lemma 8.1.3. $N_{\text{Sym}(\Omega)}(H)$ permutes the orbits of $H$.  

95
Proof. Let \( \alpha, \beta \in \Omega \) be two elements in the same \( H \)-orbit, so there exists \( h \in H \) such that \( \alpha^h = \beta \). Let \( x \in N_{\text{Sym}(\Omega)}(H) \), then \( \beta^x = \alpha^{xhx} = \alpha^{xh_1} \) where \( h_1 = x^{-1}hx \in H \). Hence \( \alpha^x \) and \( \beta^x \) are also in the same \( H \)-orbit. \( \square \)

Let \((\alpha, \beta) \in \Omega \times \Omega\) and let \( H \leq \text{Sym}(\Omega) \). Then we can define an action of \( H \) on \( \Omega \times \Omega \) by \((\alpha, \beta)^h := (\alpha^h, \beta^h)\). We associate to \( H \) a family of directed graphs, each with vertex set \( \Omega \) and edge set one of the \( H \)-orbits on the set \( \Omega \times \Omega \). These are known as the orbital graphs of \( H \).

By Lemma 8.1.3, the normaliser of \( H \) in \( \text{Sym}(\Omega) \) permutes the orbital graphs of \( H \). When testing isomorphisms of graphs we can partition the vertex set using common features which are preserved under isomorphism, such as valency or (directed) distance from a given vertex. Then various refinements can be applied to the partitions, to narrow down the number of possibilities that need to be checked computationally. Theissen [70] used the application of these techniques to orbital graphs to define a pruning method for permutation group normalisers which is effective but not too costly to compute. Further work towards developing polynomial time algorithms for computing permutation group normalisers appears in [42].

Matrix groups

We mentioned earlier that the efficiency of an algorithm involving bases is relative to the size of the basic orbits. For a permutation group \( H \leq \text{Sym}(\Omega) \), an orbit of \( H \) can be no longer than \(|\Omega|\). By comparison, computing with matrix groups is difficult in general, since the length of an orbit for a matrix group \( G \leq \text{GL}_n(q) \) acting on \( V := \mathbb{F}_q^n \) can be as large as \( q^n - 1 \).

\( \text{GL}_n(q) \) and \( \text{SL}_n(q) \) act transitively on the non-zero vectors \( V \), as does \( \text{Sp}_n(q) \), by [32, Theorem 5.2.2]. Consider the backtrack search tree for \( \text{GL}_n(q) \). The root node has \( q^n - 1 \) children, the nodes at level 1 have \( q^n - q \) children, the nodes at level 2 have \( q^n - q^2 \) children, and so on. The other classical groups have large orbits of size roughly \( (q^n-1)/(q-1) \). Conversely, ‘small’ matrix groups often act regularly, in the sense of a permutation group, so the children of the root are just the group elements. Note that although this is a simplification, it serves as a rough approximation for our purposes.

Butler [7] was the first to apply the Schreier–Sims algorithm to matrix groups over a finite field. Since a matrix group \( G \leq \text{GL}_n(q) \) acts faithfully by permuting the vectors of the vector space \( V \), we can use permutation group methods on \( G \), using the basis vectors of \( V \) as base points. However this is not very efficient, as already discussed. In [7] and [8] Butler considers the action of \( \text{GL}_n(q) \) on the projective space of \( V \), taking the 1-dimensional subspaces of \( V \) as the base points. This reduces the basic orbit size by a factor of up to \( q - 1 \) and significantly extends the range of the Schreier–Sims algorithm.

In 2002 Murray and O’Brien [51] presented methods for improving the...
Schreier–Sims algorithm for matrix groups by selecting ‘good’ base points with small orbits. However, there are many matrix groups for which there are no such base points, and the existing algorithms do not perform well. For example, the order and basic orbit sizes of $GL_n(q)$ itself are exponential in comparison with its input size.

Our plan

The existing algorithm in Magma to find the normaliser of $G$ in $GL_n(q)$ is called by $\text{Normaliser}(GL(n,q),G)$. In the following chapters we describe a new algorithm $\text{NormaliserGL}$, which computes the normaliser of a matrix group $G$ inside $GL_n(q)$. The general approach is to determine an overgroup $R < GL_n(q)$ which contains $N_{GL_n(q)}(G)$, then for large enough values of $n$ and $q$ the calculation of $N_R(G)$ should be quicker than that of $N_{GL_n(q)}(G)$. Consequently $\text{NormaliserGL}$ will be more efficient than $\text{Normaliser}$, provided that the computation of $R$ is not too slow.

Recall that Aschbacher’s theorem (see Section 1.6) gives nine (not, in general, disjoint) classes to which a subgroup of $GL_n(q)$ must belong. We use this as a framework and for each class $C_i$, with $i \in \{1, 2, 3, 5, 8\}$, we shall explain how to find an overgroup for the normaliser in $GL_n(q)$ of a group $G$ lying in $C_i$, or else characterise the groups for which we cannot find an overgroup. In the latter case, the original algorithm is used. The Magma commands to check membership of Aschbacher classes $C_1, C_2, C_3, C_5$ and $C_8$ appear in the algorithm of Section 8.4. For a group $G$ which does not belong to one of these classes, we use alternative methods described in Section 8.3.

8.2 General methods

We now describe some methods used in $\text{NormaliserGL}$ which are common to several or all of the Aschbacher classes.

8.2.1 Preserving precisely $n$ structures

Recall from Section 1.6 that each of the classes $C_1, \ldots, C_8$ of Aschbacher’s theorem has associated to it a type of geometric structure which is preserved by the groups of that class. For example, the groups in class $C_2$ preserve a system of imprimitivity in their action on $V := \mathbb{F}_q^n$. Our algorithms will make use this fact in the following way.

Let $G \in C_i$. If $G$ preserves precisely one of the structures associated with $C_i$, of some given type (for example, a block system of a given dimension), then we find an overgroup by deducing certain properties of the elements of $GL_n(q)$ which normalise $G$. In some cases $N_{GL_n(q)}(G)$ also preserves this structure and hence the full stabiliser in $GL_n(q)$ of this structure an overgroup for $N_{GL_n(q)}(G)$. See Section 1.6 for the shapes of these full stabilisers.
Sometimes we can characterise the groups in $C_i$ which preserve precisely one structure of a particular type.

For certain of the $C_i$, if we know that a group $G \in C_i$ preserves precisely two of these structures (of a given dimension etc.), then we can deduce information about normalising elements of $G$ and hence find an overgroup. Future work could include characterising the groups $G \leq \text{GL}_n(q)$ preserving two or more of a particular geometric structure, and investigating properties of the elements of $\text{GL}_n(q)$ which normalise $G$.

### 8.2.2 Recursion

For certain of the Aschbacher classes, such as the reducible class $C_1$ and the subfield class $C_5$, we apply recursion. In these cases we use $\text{NormaliserGL}$ to calculate the normaliser (or an overgroup of the normaliser) in $\text{GL}_n(q)$ of some smaller group associated with $G$, in order to find an overgroup for $N_{\text{GL}_n(q)}(G)$.

### 8.2.3 Normaliser of derived group

Let $G \leq \text{GL}_n(q)$ be absolutely irreducible. We will use the following lemma to show that $G' \leq N_{\text{GL}_n(q)}(G)$ is an overgroup for $N_{\text{GL}_n(q)}(G')$. Note that $K \text{char} G$ denotes the fact that $K$ is a characteristic subgroup of $G$.

**Lemma 8.2.1.** Let $H$ be a group, let $G$ be a subgroup of $H$, and let $K \text{char} G$. Then $N_H(G) \leq N_H(K)$.

**Proof.** The subgroup $K \leq N_H(G)$, since $K \text{char} G$ and $G \leq N_H(G)$, and hence $N_H(G) \leq N_H(K)$.  

We now use this Lemma to prove the following.

**Lemma 8.2.2.** Let $G \leq \text{GL}_n(q)$, then

$$N_{\text{GL}_n(q)}(G) \leq N_{\text{GL}_n(q)}(G').$$

**Proof.** First note that $G' \text{char} G$. For, if $\sigma \in \text{Aut}(G)$ and $x, y \in G$, then

$$(x^{-1}y^{-1}xy)\sigma = (x\sigma)^{-1}(y\sigma)^{-1}(x\sigma)(y\sigma),$$

which also lies in $G'$, so $G'\sigma = G'$.

Hence, the result $N_{\text{GL}_n(q)}(G) \leq N_{\text{GL}_n(q)}(G')$ follows from Lemma 8.2.1. □

Note that $N_{\text{GL}_n(q)}(G') = \text{GL}_n(q)$ if and only if $G' = \text{SL}_n(q)$ or $G' \leq Z(\text{GL}_n(q))$. Hence, in those cases this method does not return an overgroup for $N_{\text{GL}_n(q)}(G)$.  

98
8.2.4 Derived group scalar

The next theorem appears in [10, Theorem 3.7] and characterises the absolutely irreducible groups $G$ for which $G'$ contains only scalar matrices.

**Theorem 8.2.3.** Let $G \leq \text{GL}_n(q)$ be an absolutely irreducible group whose derived group $G'$ consists only of scalar matrices. Then either

1. $n = 2$ and $G$ is isomorphic to an extension by scalars of $Q_8$, acting semilinearly; or
2. $G$ is imprimitive.

If the second case holds then $G \in C_2$ and we can use the algorithms of Chapter 10 to find an overgroup for $N_{\text{GL}_n(q)}(G)$. Otherwise the algorithm fails and we default to the original algorithm $\text{Normaliser}(\text{GL}(n,q), G)$. Future work could include finding an overgroup for this case, however since $|\text{Aut}(Q_8)| = 24$, the order of $G$ is very small and MAGMA’s existing algorithm should be fast.

8.3 When our algorithms fail

For some of the Aschbacher classes, there are groups $G$ in that class for which $\text{NormaliserGL}(G)$ fails to find an overgroup for $N_{\text{GL}_n(q)}(G)$. When this occurs the following steps are taken:

1. Check to see if $G$ is contained in any other Aschbacher class. If so, then apply the methods associated with that class to find an overgroup for $N_{\text{GL}_n(q)}(G)$. Continue through the classes until an overgroup is found or all classes have been considered.

2. If no overgroup is found using Aschbacher classes $C_1$, $C_2$, $C_3$, $C_5$ or $C_8$, then consider $G'$. If $G$ is perfect, then use $\text{Normaliser}(\text{GL}(n,q), G)$ to find $N_{\text{GL}_n(q)}(G)$.

3. If $G$ is not perfect and $G'$ consists entirely of scalars, then Case 1 of Theorem 8.2.3 holds and we default to $\text{Normaliser}(\text{GL}(n,q), G)$ to find $N_{\text{GL}_n(q)}(G)$.

4. If $G$ is not perfect and there are non-scalar elements in $G'$, then use $\text{NormaliserGL}(G'; \text{Overgroup:=true})$ to try to compute an overgroup $R$ for $N_{\text{GL}_n(q)}(G')$. Then $R$ is also an overgroup for $N_{\text{GL}_n(q)}(G)$.

During the course of $\text{NormaliserGL}$ these steps may be repeated a number of times, but the algorithm will always terminate. This algorithm could be improved by finding overgroups for the cases where we default to the original algorithm.
8.4 The algorithm: NormaliserGL

Let $G \leq \text{GL}_n(q)$. We now present the algorithm NormaliserGL which takes as input a group $G$ as well as optional parameters Print, Overgroup and derived_subgroup.

The parameter Overgroup is used during recursion, as in some cases the normaliser $M$ of another group is used to make an overgroup for $N_{\text{GL}_n(q)}(G)$. In this situation, we always take the overgroup of $M$, rather than computing $M$ itself. If Overgroup = FALSE (which is the default value), then NormaliserGL returns $N_{\text{GL}_n(q)}(G)$. If Overgroup = TRUE then the function NormaliserGL returns some or all of the following:

- an overgroup $R \geq N_{\text{GL}_n(q)}(G)$;
- a boolean full_norm, indicating whether or not $R = N_{\text{GL}_n(q)}(G)$; and
- a group $D \leq G'$ (this is not always defined).

If Print is assigned a value greater than 0, then NormaliserGL returns information about the algorithm’s progress, including which Aschbacher classes (if any) are being used to seek an overgroup.

In the course of NormaliserGL, a group $D \leq G'$ may be calculated for use in one of the sub-functions and if so then we assign derived_subgroup := $D$. This is used in recursive steps, to avoid the potentially expensive recalculation of $D$. The default value of derived_subgroup is 0.

Note that in the algorithm description below, we occasionally stretch the meaning of ‘overgroup’ to include $\text{GL}_n(q)$, for convenience. An overview and justification for the steps of NormaliserGL is given after the algorithm.

The function NormaliserGL($G$:Overgroup, Print, derived_subgroup)

Set the initial value full_norm := FALSE.

Step 1. If $n = 1$, then assign $R := \text{GL}_n(q)$ and full_norm := TRUE. Go to Step 15.

Else go to Step 2.

Step 2. If $G \leq Z(\text{GL}_n(q))$, then assign $R := \text{GL}_n(q)$, and full_norm := TRUE. Go to Step 15.

Else go to Step 3.

Step 3. If $G$ is soluble, then go to Step 5. Otherwise go to Step 4.
Step 4. If \texttt{RecogniseClassical}(G)=\textsc{true}, then \(G\) normalises one of the groups \(\text{SL}_n(q), \text{Sp}_n(q), \text{SU}_n(q)\) or \(\Omega^\epsilon_n(q)\), where \(\epsilon \in \{\circ, +, -\}\). Determine whether \(G'\) is absolutely irreducible as follows. If \texttt{derived_subgroup} is a group then let \(D := \text{derived_subgroup}\). If not, then assign the group \(D := \text{DerivedGroupMonteCarlo}(G)\) and let \texttt{derived_subgroup} := \(D\). If \(D\) is not absolutely irreducible then go to Step 5.

Otherwise, the derived subgroup of \(G\) is absolutely irreducible. Compute \texttt{ClassicalForms}(G:Scalars:=true) and use \texttt{NormaliserClassical} to find an overgroup \(R\) (see Chapter 13). If \(R = N_{\text{GL}_n(q)}(G)\) then let \texttt{full_norm}:=\textsc{true}. Go to Step 15.

Else go to Step 5.

Step 5. If \texttt{IsIrreducible}(G)=\textsc{false}, then \(G \in C_1\). Try to find an overgroup \(R\) using \texttt{NormaliserReducible} (see Chapter 9). If this succeeds then go to Step 15, otherwise go to Step 14.

Else, \(G\) is irreducible; go to Step 6.

Step 6. If \texttt{IsAbsolutelyIrreducible}(G)=\textsc{false}, then \(G \in C_3\). If \(n = q = 2\), then let \(R := \text{GL}_n(q)\) and assign \texttt{full_norm}:=\textsc{true}. Otherwise, find an overgroup \(R\) using \texttt{NormaliserSemilinear} (see Chapter 11). Go to Step 15.

Else, \(G\) is absolutely irreducible; go to Step 7.

Step 7. If \texttt{IsOverSmallerField}(G:Scalars:=false)=\textsc{true}, then \(G\) is in \(C_5\). Use \texttt{NormaliserSubfield} to find an overgroup \(R\) (see Chapter 12) and go to Step 15.

Else go to Step 8.

Step 8. If \(G\) is a \(p\)-group of odd exponent \(p\), and \texttt{IsExtraSpecial}(G) returns \textsc{true}, then compute \texttt{ClassicalMaximals("L",n,q:classes:={6})}. If this list is empty then go to Step 9. Otherwise let \(E\) be the first group in the list. If \(E\) has precisely one normal subgroup \(H\) of the same order as \(G\) then let \(R := E^x\), where \(x \in \text{GL}_n(q)\) conjugates \(G\) to \(H\). Assign the value \texttt{full_norm}:=\textsc{true} and go to Step 15.

Else go to Step 9.

Step 9. If \texttt{IsPrimitive}(G)=\textsc{false} then \(G \in C_2\). Try to find an overgroup \(R\) using \texttt{NormaliserImprimitive} (see Chapter 10). If no overgroup is found, then go to Step 10. If an overgroup is found and \(R\) is equal to \(N_{\text{GL}_n(q)}(G)\), then assign \texttt{full_norm}:=\textsc{true}. Go to Step 15.
**Step 10.** If \( \text{IsSemiLinear}(G) = \text{true} \), then \( G \in C_3 \). Use the function \text{NormaliserSemilinear} (see Chapter 11) to try to find an overgroup \( R \), passing on the value of \text{derived subgroup} to this function. The function \text{NormaliserSemilinear} returns \( G' \), which we assign to \text{derived subgroup}. If \text{NormaliserSemilinear} succeeds in finding an overgroup, then go to Step 15.

Else go to Step 11.

**Step 11.** Use \text{ClassicalForms}(G) to see if \( G \) preserves a non-degenerate classical form absolutely. If NO then go to Step 12.

If YES, and the form is symplectic or unitary with \( n = 2 \), then go to Step 12. Otherwise use \text{NormaliserClassical} (see Chapter 13) to find an overgroup \( R \). If \( R = N_{GL_n(q)}(G) \) then assign \text{full norm} := \text{true}. Go to Step 15.

**Step 12.** If \( \text{IsPerfect}(G) = \text{true} \), then go to Step 14. Else, \( G \neq G' \). If \text{derived subgroup} is a group then let \( D := \text{derived subgroup} \). Otherwise assign \( D := \text{DerivedGroupMonteCarlo}(G) \). If \( D \) is not normal in \( G \) then recalculate \( D := \text{DerivedGroupMonteCarlo}(G) \), repeating until a normal subgroup \( D \) is found. Check to see if \( G/D \) is abelian and therefore \( D = G' \). If not, then let \( D := \text{DerivedGroupMonteCarlo}(G) \) and check again. Repeat until \( D = G' \). Go to Step 13.

**Step 13.** If \( D \leq Z(GL_n(q)) \) then go to Step 14. Otherwise, use the function \text{NormaliserGL}(D:Overgroup:= \text{true}) \) to try to compute an overgroup \( R \) for \( N_{GL_n(q)}(D) \) (i.e. return to Step 1, with \( D \) in place of \( G \)).

If this succeeds in finding an overgroup \( R \), then go to Step 15.

Else, go to Step 14.

**Step 14.** Compute the overgroup \( R := \text{Normaliser}(GL(n,q),G) \) and assign \text{full norm} := \text{true}. Go to Step 15.

**Step 15.** If the optional parameter \text{Overgroup} = \text{true} then return the overgroup \( R \) and the value of \text{full norm}.

Else, if \text{full norm} = \text{true} then return \( R \).

Otherwise, return \( N := \text{Normaliser}(R, G) \).

The order in which we proceed through the Aschbacher classes is decided by a combination of the efficiency of the MAGMA functions used and mathematical consistency. Since the Aschbacher classes are not in general
disjoint, we wish to treat the most computationally difficult cases later in
the algorithm. An exception to this is the $C_1$ case; the reducibility of a group
must be identified early on, despite this being a difficult case.

The worst case of $\text{NormaliserGL}(G)$ defaults to the original algorithm
$\text{Normaliser}(\text{GL}(n,q), G)$, and has exponential complexity. For this reason,
we do not give a detailed complexity analysis of our functions. Our aim
is rather to find tests in polynomial time to make smaller exponential type
problems.

Note that determining the Aschbacher membership of a group $G$ does
not always lead to an overgroup. For most of the functions associated with
an Aschbacher class, there are certain groups $G$ in that class for which the
function cannot find an overgroup. In those cases we try other methods to
find an overgroup, defaulting to $\text{Normaliser}(\text{GL}(n,q), G)$ if all attempts
fail. We now give an overview of $\text{NormaliserGL}$ and explain the order of the
steps.

**Overview of NormaliserGL**

Steps 1 and 2 test whether $G$ consists only of scalars. If so then $N_{\text{GL}_n(q)}(G) = \text{GL}_n(q)$. If $G$ is found to be soluble in Step 3 then we cannot find the
normaliser of $G$ using $\text{NormaliserClassical}$ so we skip Step 4.

Step 4 uses $\text{RecogniseClassical}$ to determine whether $G$ normalises
one of the groups $\text{SL}_n(q)$, $\text{Sp}_n(q)$, $\text{SU}_n(q)$ or $\Omega^n_\epsilon(q)$, where $\epsilon \in \{\circ, +, -\}$. This function has low-degree polynomial complexity ([11, 12, 13, 52, 53, 54, 55, 58]).

For $\text{ClassicalForms}$ to return an answer, we require $G'$ to be absolutely irreducible. If earlier iteration of $\text{NormaliserGL}$ has calculated a subgroup
of $G'$, then it is stored as $\text{derived subgroup}$, so let $D := \text{derived subgroup}$. If not then we calculate $G'$, or a subgroup of $G'$, as follows.

We could use the deterministic function $\text{DerivedSubgroup}$ to calculate
$G'$ directly, however this is not known to run in low-degree polynomial time.
Instead, we let $D := \text{DerivedGroupMonteCarlo}$, which is non-deterministic
but calculates $G'$, or a proper subgroup of $G'$, in polynomial time.

If the group $D$ is absolutely irreducible then the group $G'$ is also and we
can use $\text{NormaliserClassical}$ to calculate an overgroup for $G$. In this case
we can usually write down the full normaliser directly, so $\text{NormaliserGL}$ is
very efficient in this case.

Steps 5 and 6 treat the reducible ($C_1$) and non-absolutely irreducible
groups (part of $C_3$), respectively. These cases are dealt with early in the
algorithm since they are disjoint from all others. A group can be recognised
as irreducible or absolutely irreducible using MEATAXE-based techniques, in
time polynomial in $n$ and $\log q$ [26, 29]. If $G$ is a $C_3$-group and $n = q = 2$,
then $G$ is abelian and $N_{\text{GL}_n(q)}(G) = \text{GL}_n(q)$.

If $G$ is an extraspecial $p$-group of odd exponent $p$, then we can write down
its normaliser directly in Step 8. Subfield \((C_5)\), imprimitive \((C_2)\) and (absolutely irreducible) semilinear (the remainder of \(C_3\)) groups are dealt with in Steps 7, 9 and 10, respectively. The function \texttt{IsSubfield} may return “unknown”, but it terminates with low-degree polynomial complexity \([10]\). There is no proof that the complexity of \texttt{IsPrimitive} is polynomial, however in practice it runs quickly. \texttt{IsSemilinear} has low-degree polynomial complexity \([10]\), but may return “unknown” if the group is imprimitive. The ordering of these functions is chosen with respect to their efficiency, and to reduce the number of imprimitive groups which are tested for semilinearity.

In Step 11 we deal with the groups which preserve a classical form but do not contain one of \(\text{SL}_n(q)\), \(\text{Sp}_n(q)\), \(\text{SU}_n(q)\) or \(\Omega^\epsilon_n(q)\), where \(\epsilon \in \{\circ, +, -\}\) (and hence were not covered in Step 4). We call \texttt{ClassicalForms}(G) to detect whether \(G\) preserves a classical form absolutely. This runs in low-degree polynomial time \([27]\). Suppose \(G\) preserves a classical form, then if \(n = 2\) and the form is symplectic or unitary, then \texttt{NormaliserClassical} cannot find an overgroup for \(G\). With the exception of these cases, we use \texttt{NormaliserClassical}(G) to find an overgroup for \(G\).

By Lemma 8.2.2, an overgroup for \(N_{\text{GL}_n(q)}(G')\) is also an overgroup for \(N_{\text{GL}_n(q)}(G)\). If \(G = G'\), then we cannot use \texttt{NormaliserGL}(G') to find an overgroup, so in Step 12 we check whether \(G\) is perfect, and if so then default to the original algorithm.

Assume \(G\) is not perfect. If \texttt{derived subgroup} is a group then let \(D := \text{derived subgroup}\). Else, assign \(D := \text{DerivedGroupMonteCarlo}(G)\). If the quotient group \(G/D\) is abelian then \(D = G'\). (Note that this step can be time consuming). If not, then let \(D := \text{DerivedGroupMonteCarlo}(G)\) and check again. Repeat as required. Since this function uses random generation, an infinite loop could occur in theory, however the probability of this is extremely small.

The normaliser \(N_{\text{GL}_n(q)}(G') = \text{GL}_n(q)\) if and only if either \(G'\) contains \(\text{SL}_n(q)\) or \(G' \leq Z(G)\). The first of these situations was eliminated in Step 4, and the second is identified in Step 13. If \(G'\) consists only of scalar matrices then by Lemma 8.2.3, either \(G\) is imprimitive or else \(n = 2\) and \(G\) is isomorphic to an extension by scalars of \(Q_8\) acting semilinearly. If \(G\) is imprimitive then \texttt{NormaliserImprimitive} has failed already, so in either case we default to the original algorithm \texttt{NormaliserGL}(\text{GL}(n,q), G).

If \(G'\) is non-scalar, then we compute an overgroup for the normaliser in \(\text{GL}_n(q)\) of \(G'\), using \texttt{NormaliserGL}(G':\text{Overgroup}:=true).

In the following chapters we examine Aschbacher classes \(C_i\), for \(i \in \{1, 2, 3, 5, 8\}\). For each class, we describe the conditions under which we can find an overgroup \(R\) for \(N_{\text{GL}_n(q)}(G)\), where \(G \in C_i\), and we also present an algorithm to find \(R\) which forms part of \texttt{NormaliserGL}. At the end of each chapter there are tables of timings data for the performance of \texttt{NormaliserGL}, using a number of test groups in \(C_i\) and for a range of differ-
ent $n$ and $q$. We shall see that for large enough $n$ and $q$, the improvement is extremely good!

Finally, we give some suggestions for further work in this area. The attached disc contains the algorithm code and some example groups $G$, which the reader can use to compare $\text{NormaliserGL}(G)$ with Magma’s original function $\text{Normaliser(GL}(n,q),G)$. 
Chapter 9

\( \mathcal{C}_1: \) Reducible Groups

9.1 Introduction

In this section we define Aschbacher class \( \mathcal{C}_1 \) and describe an algorithm \texttt{NormaliserReducible} which computes an overgroup \( R < \text{GL}_n(q) \) such that \( N_\text{GL}_n(q)(G) \leq R \), for certain \( G \in \mathcal{C}_1 \). We begin with some notation, definitions and preliminary results.

Let \( G \leq \text{GL}_n(q) \), with underlying vector space \( V = \mathbb{F}_q^n \), and view this as a module for \( G \) in the natural way. In this chapter all maps are written on the right. Recall the definition of a reducible group from Section 1.2.

**Definition 9.1.1.** The Aschbacher class \( \mathcal{C}_1 \) consists of all reducible groups \( G \leq \text{GL}_n(q) \).

We now give some more definitions which will be used in this chapter.

**Definition 9.1.2.** Let \( A \) and \( B \) be two \( G \)-modules. A homomorphism \( \phi : A \rightarrow B \) is a \textit{G-homomorphism} if \((vg)\phi = (v\phi)g\), for all \( v \in A \) and \( g \in G \). The set of all \( G \)-homomorphisms between \( A \) and \( B \) form a vector space \( \text{Hom}_G(A,B) \) over a given field (which is assumed to be the base field of \( G \), unless otherwise specified). A \textit{G-isomorphism} is a bijective \( G \)-homomorphism.

**Definition 9.1.3.** Let \( G \) be reducible, then a \textit{composition series} for \( V \) is a series of submodules

\[
\{0_V\} = M_0 \subset \cdots \subset M_{n-1} \subset M_n = V,
\]

where each \( M_i \) is a maximal \( G \)-submodule of \( M_{i+1} \), with respect to containment. That is, the \textit{composition factor} \( M_i/M_{i-1} \) is irreducible.

The \textit{constituents} of \( V \) are representatives for the isomorphism classes of the composition factors of \( V \). Note that the constituents of \( V \) are not necessarily submodules. The \textit{multiplicity} of a constituent \( A_i \) is the number of composition factors of \( V \) isomorphic to \( A_i \). We define the multiplicity of
an irreducible submodule \( W < V \) to be the multiplicity of the constituent of \( V \) to which \( W \) is isomorphic.

The following theorem is classical.

**Theorem 9.1.4** (Jordan-Hölder Theorem). Let \( G \) be a finite group with natural \( G \)-module \( V \) and suppose

\[
\{0_V\} = M_0 \subset \cdots \subset M_{n-1} \subset M_n = V
\]

and

\[
\{0_V\} = K_0 \subset \cdots \subset K_{m-1} \subset K_m = V
\]

are two composition series for \( G \). Then \( m = n \) and there is a one-to-one correspondence between the sets of composition factors of each series such that corresponding factors are isomorphic.

Now we present a few useful facts. In the following lemmas, let \( G \leq \mathrm{GL}_n(q) \) be reducible and view \( V \) as its natural module.

**Lemma 9.1.5.** Let \( W \) be a \( G \)-submodule of \( V \). If \( G \) stabilises \( W \), then \( G \) stabilises \( W r \), for all \( r \in \mathrm{N}_{\mathrm{GL}_n(q)}(G) \).

**Proof.** Let \( g \in G \), let \( r \in \mathrm{N}_{\mathrm{GL}_n(q)}(G) \) and let \( g_1 = r g r^{-1} \). Then

\[
W r g = W r (r^{-1} g_1 r) = W g_1 r = W r.
\]

Hence \( G \) stabilises \( W r \), for all \( r \in \mathrm{N}_{\mathrm{GL}_n(q)}(G) \). \( \square \)

**Lemma 9.1.6.** Let \( W \) be an irreducible \( G \)-submodule of \( V \) and let \( r \in \mathrm{N}_{\mathrm{GL}_n(q)}(G) \). Then \( W r \) is an irreducible \( G \)-submodule, \( \dim(W) = \dim(W r) \) and \( W r \) has the same multiplicity as \( W \).

**Proof.** Suppose \( W r \) properly contains a non-trivial \( G \)-submodule \( X \). Then by Lemma 9.1.5, the submodule \( X r^{-1} < W \) is also stabilised by \( G \), contradicting the fact that \( W \) is irreducible.

Now let \( W_1, W_2 \) be two irreducible submodules of \( V \). We show that \( W_1 \cong W_2 \) if and only if \( W_1 r \cong W_2 r \). Let \( \theta : V \to V \) be a \( G \)-isomorphism such that \( W_1 \theta = W_2 \), then \( W_1 r^{-1} \theta r = W_2 r \) and hence \( W_1 r \cong W_2 r \). Conversely, suppose \( \phi \) is a \( G \)-isomorphism such that \( W_1 r \phi = W_2 r \), then \( W_1 r \phi r^{-1} = W_2 \) and \( r \phi r^{-1} \) is an isomorphism between \( W_1 \) and \( W_2 \). Therefore, if we apply \( r \) to a composition series of \( V \), then every composition factor which was isomorphic to \( W_1 \) is now isomorphic to \( W_1 r \) and hence \( W_1 \) has the same multiplicity as \( W_1 r \). \( \square \)

**Lemma 9.1.7.** Let \( W \) be an irreducible \( G \)-submodule of \( V \) and let \( w \in W \). Then \( \{ w g : g \in G \} \) spans \( W \).
Proof. Clearly \( \langle \{ wg : g \in G \} \rangle \leq W \) and if \( \langle \{ wg : g \in G \} \rangle < W \) then \( W \) is not irreducible. Hence \( \{ wg : g \in G \} \) spans \( W \).

\[ \square \]

**Definition 9.1.8.** A \( G \)-module which may be decomposed as the direct sum of irreducible modules is **completely reducible**. Similarly, a group with a completely reducible natural module is a **completely reducible group**.

Let \( \{ e_1, e_2, \ldots, e_n \} \) be the standard basis for \( V \) described in Section 1.2. In the proof of the following lemma we use the notation \((-v-)\), where \( v := \beta_1 e_1 + \beta_2 e_2 + \cdots + \beta_n e_n \in V \), to represent the matrix row \( (\beta_1 \beta_2 \cdots \beta_n) \).

The following result applies standard theory for a change of basis, however we show how to construct the conjugating matrix explicitly, as it shall be used in our algorithm.

**Lemma 9.1.9.** If \( G \) is a completely reducible group then there exists \( y \in \text{GL}_n(q) \) such that \( yGy^{-1} \) is in block diagonal form.

**Proof.** Let \( A_1, A_2, \ldots, A_t \) be the irreducible constituents of \( V \), of dimensions \( d_1, d_2, \ldots, d_t \), respectively. Let \( B_{A_i} \) be a basis for \( A_i \), where \( B_{A_1} = [v_1, \ldots, v_{d_1}] \), \( B_{A_2} = [v_{d_1+1}, \ldots, v_{d_1+d_2}] \), and so on. The \( v_i \) form a basis \( B_V \) of \( V \). Let \( W_i := \langle \sum_{j<i} d_j + 1, \ldots, \sum_{j<i+1} d_j \rangle \), for each \( i \in \{1, \ldots, t\} \).

Consider the matrix

\[
y = \begin{pmatrix} -v_1 & \vdots & -v_n \\
-\vdots & \cdots & -\vdots \\
-v_n & \ldots & -v_1
\end{pmatrix},
\]

so that \( e_i y = v_i \), for all \( 1 \leq i \leq n \). We show that the action of \( yGy^{-1} \) preserves each \( W_i \). Let \( k \in \{1, \ldots, d_1\} \), then \( e_k \in W_1 \) and \( v_k \in B_{A_1} \). Let \( g \in G \), then there exist scalars \( \alpha_1, \alpha_2, \ldots, \alpha_{d_1} \in F_q \) such that \( v_k g = \alpha_1 e_1 + \cdots + \alpha_{d_1} e_{d_1} \in A_1 \), and

\[
e_k gyg^{-1} = v_k g^{-1}
= (\alpha_1 e_1 + \cdots + \alpha_{d_1} e_{d_1}) y^{-1}
= \alpha_1 e_1 + \cdots + \alpha_{d_1} e_{d_1}
\in W_1.
\]

We can make a similar statement for any \( e_j \in W_i \) and hence the subspaces \( W_i \) are each preserved by \( yGy^{-1} \). Writing out the action of \( yGy^{-1} \) with respect to \( e_1, \ldots, e_n \), we obtain a group of matrices in block diagonal form.

Let \( G \) be reducible and completely reducible, then the action of \( G \) on \( V \) preserves each term in a direct sum decomposition

\[
V = W_1 \oplus W_2 \oplus \cdots \oplus W_t
\]

(9.1)
of irreducible submodules. We require $t > 1$ or else $G$ is not reducible.

**Definition 9.1.10.** Let $W < V$ be an irreducible submodule, then the **homogeneous component** of $V$ containing $W$ is the submodule spanned by all submodules isomorphic to $W$.

Let $\{V_1, \ldots, V_k\}$ be the homogeneous components of $V$, then

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_k,$$

(9.2)

for some $1 \leq k \leq n$. Let $m_j$ be the multiplicity of an irreducible submodule $W_i$ contained in $V_j$, that is, the number of constituents of $V$ isomorphic to $W_i$.

We now present some categories into which a reducible group $G$ must fall.

**Definition 9.1.11.** Let $G \leq \text{GL}_n(q)$ be a $C_1$-group. The following categories for $G$ will be used to find an overgroup $R \geq N_{\text{GL}_n(q)}(G)$. The cases are named after the structure of $R$.

1. **Wreath Product case:** $G$ is completely reducible, preserves decomposition (9.2) with $k > 1$, and $\dim(V_i) = \dim(V_j)$ for all $i, j$.

2. **Tensor Product case:** $G$ is completely reducible and preserves decomposition (9.1). The $W_i$ are all pairwise isomorphic, i.e. $G$ preserves (9.2) with $k = 1$, and the $W_i$ are absolutely irreducible.

3. **Problem case:** $G$ is completely reducible and preserves decomposition (9.1). The $W_i$ are all pairwise isomorphic, i.e. $G$ preserves (9.2) with $k = 1$, and the $W_i$ are not absolutely irreducible.

4. **Direct Product case:** $G$ is completely reducible, preserving decomposition (9.2) with $k > 1$. $G$ also preserves a partition of the $V_i$ into sets $Y_1, \ldots, Y_s$, such that each $Y_j$ contains all $V_i$ with the same associated dimension and associated multiplicity, and $1 < s \leq k$.

5. **Submodule Stabiliser case:** $G$ is not completely reducible.

**Lemma 9.1.12.** A reducible group $G$ belongs to at least one of the categories given in Definition 9.1.11.

**Proof.** If $G$ is not completely reducible then $G$ lies in Case 5. Otherwise $G$ preserves the direct sum decomposition (9.1). Suppose all $W_i$ have the same dimension. If $G$ preserves (9.2) with $k = 1$ (so all $W_i$ are isomorphic) and all $W_i$ are absolutely irreducible, then $G$ lies in Case 2. If the $W_i$ are not absolutely irreducible, then $G$ lies in Case 3. Now assume that $G$ preserves (9.2) with $k > 1$, so that the $W_i$ are not all isomorphic. If all $W_i$ have the same multiplicity then $G$ lies in Case 1. Otherwise, the $V_i$ may be
partitioned according to their multiplicities. This partition is non-trivial, so $G$ lies in Case 4.

Now assume that the $W_i$ do not all have the same dimension. The $V_i$ may be partitioned into sets $Y_1, \ldots, Y_s$, where $Y_j$ contains all $V_i$ of the same associated dimension and associated multiplicity. This partition is non-trivial, so $G$ lies in Case 4.

We will examine each of the above cases in turn. For each case, except for the problem case, we specify an overgroup for $N_{\text{GL}_n}(q)(G)$, where $G$ satisfies the given condition.

**Definition 9.1.13.** Let $W = W_1 \oplus W_2 \oplus \cdots \oplus W_t$, where $t > 1$. Suppose $W_i \cong W_j$ for all $1 \leq i, j \leq t$ and the $W_i$ are irreducible. Let $\pi_i : W \to W_i$ be the projection map. A $G$-module $X \leq W$ embeds diagonally in $W$ if $\pi_i|_X$ is an isomorphism, for all $i$. That is to say, every element $x \in X$ can be uniquely written as $x = w_1 + \cdots + w_t$, where $w_i \in W_i$, and if $x \neq 0$ then not all $w_i$ are zero.

**Lemma 9.1.14.** Let $G$ act completely reducibly on $V$, preserving decomposition (9.1), and suppose $\dim(W_i) = d_i$ for all $1 \leq i \leq t$. Let $Y$ be an irreducible $d$-dimensional submodule of $V$. Then there is a subspace $S \leq V$ which is the sum of a subset of $\{W_1, W_2, \ldots, W_t\}$, such that $Y$ is diagonally embedded in $S$ and each $W_i \in S$ is isomorphic to $Y$.

**Proof.** The projection map $\pi_i : V \to W_i$ is a $G$-homomorphism. Restricting $\pi_i$ to $Y$, we obtain a $G$-homomorphism, $\pi_i|_Y : Y \to W_i$. By the irreducibility of $Y$ and of $W_i$, either $\text{Im}(\pi_i|_Y) = 0_Y$ and $\text{ker}(\pi_i|_Y) = W_i$ or else $\text{ker}(\pi_i|_Y) = 0_Y$ and $\text{Im}(\pi_i|_Y) = W_i$. Since $Y$ is non-zero, there exists some $i$ such that $\pi_i|_Y \neq 0$. Hence we have the latter case and $\pi_i|_Y$ is a $G$-isomorphism. Therefore $Y$ embeds diagonally in the set of $W_i$, where $i$ is such that $\pi_i|_Y \neq 0$, and $Y \cong W_i$ for each such $i$.

### 9.1.1 Change of basis matrix

Let $G \leq \text{GL}_n(q)$ be reducible and let $V$ be its natural module. To each of the cases give in Definition 9.1.11 is associated a change of basis matrix $\chi$ which conjugates $G$ into the given standard form. We employ this unconventional Greek notation for the change of basis matrix in each Aschbacher class we treat, in order to point out its common role. We now explain how to compute this change of basis matrix.

Let $A_1, \ldots, A_t$ be constituents of $V$ and let $A_i$ have dimension $d_i$ and multiplicity $m_i$. Let $V_i$ be the homogeneous component corresponding to $A_i$, noting that $V_i$ could have dimension 0, and let $G_i := G|_{V_i}$. Suppose we
require a change of basis matrix \( \chi \) such that

\[
\chi^{-1} G \chi = \begin{pmatrix}
G_1 & 0 & \cdots & 0 & 0 \\
0 & G_2 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & G_t & 0 \\
\star & \star & \cdots & \star & \star
\end{pmatrix},
\]

where \( \star \) represents a block of undetermined matrix entries and \( V \) is omitted if its dimension is 0. For each constituent \( A_i \) of \( V \), the MAGMA function \( \text{GHom}(A_i, V) \) returns a basis \( \Phi_i \) for the vector space \( \text{Hom}_G(A_i, V) \) of \( G \)-homomorphisms from \( A_i \) into \( V \) over \( \mathbb{F}_q \). The basis vectors of \( \Phi_i \) are given as \((d_i \times n)\)-matrices. Note that if \( \dim(\Phi_i) < m_i \) then \( V \) has some constituents of the same isomorphism type as \( A_i \) which are not submodules, and in particular \( G \) is not completely reducible. If \( |\Phi_i| > m_i \) then we replace \( \Phi_i \) by the first \( m_i \) vectors of \( \Phi_i \).

Denote by \(-\Phi_i\) the array given by stacking the matrices of \( \Phi_i \), and let

\[
\chi := \begin{pmatrix}
-\Phi_1 & -
-\Phi_2 & -
\vdots & 
-\Phi_t & -
-S & -
\end{pmatrix}
\]

where \( S \) is a stack of \((n - \sum_{i=1}^t |\Phi_i|)\) vectors of \( V \), which are linearly independent from the vectors of \( \Phi_i \) and which make \( \chi \) invertible. Then the matrix \( \chi \) conjugates \( G \) to the required form.

This construction will be repeatedly referred to in the following sections. The constituents \( A_i \) which are used to make \( \chi \) are specified in each case.

### 9.2 Finding Overgroups

We now examine the cases given in Definition 9.1.11, and give an overgroup for \( N_{\text{GL}_n(q)}(G) \) in each case. Throughout let \( V \) be the natural \( G \)-module.

#### 9.2.1 Wreath Product case

Suppose \( G \) preserves (9.2) with \( k > 1 \). That is, \( G \) is completely reducible and its action on \( V \) preserves each term in

\[
V = W_1 \oplus W_2 \oplus \cdots \oplus W_t,
\]

where the \( W_i \) are irreducible submodules and \( t > 1 \). Assume that each \( W_i \) has the same dimension \( d \) and multiplicity \( m > 1 \) and let \( A_1, \ldots, A_k \) be the
constituents of $V$ (so $k \leq t$). Let $\chi$ be the change of basis matrix created from the basis vectors of $\text{Hom}_G(A_i, V)$, for each $i \in \{1, \ldots, k\}$, as described in Subsection 9.1.1.

**Lemma 9.2.1.** Let $G$ be as above and let $V = V_1 \oplus \cdots \oplus V_k$, where each $V_i$ is the homogeneous component spanned by the $G$-submodules which are isomorphic to $A_i$.

1. Let $Y$ be a direct sum of $m$ isomorphic, irreducible $d$-dimensional $G$-submodules of $V$, then $Y = V_i$ for some $1 \leq i \leq k$.

2. An overgroup for $\text{N}_{\text{GL}_n(q)}(G)$ is $(\text{GL}_{n/k}(q) \wr S_k)^{\chi^{-1}}$.

**Proof.**

1. Let $X$ be an irreducible $d$-dimensional $G$-submodule in $Y$. Then by Lemma 9.1.14, there is some $1 \leq i \leq k$ such that $X$ is diagonally embedded in $V_i$. Hence $X \leq V_i$ and also $X$ is isomorphic to a constituent of $V_i$, by Lemma 9.1.14. So $X$ has multiplicity $m$ and $Y$ is equal to $V_i$.

2. Let $r \in \text{N}_{\text{GL}_n(q)}(G)$, then the subspace $V_i r = W_{i_1} r \oplus \cdots \oplus W_{i_m} r$. The $W_{i_j}$ are irreducible, $d$-dimensional $G$-submodules, by Lemma 9.1.6, and they are pairwise isomorphic, so have multiplicity $m$. Therefore there exists $j \in \{1, \ldots, k\}$ such that $V_i r = V_j$, by Part 1. Hence the action of $\text{N}_{\text{GL}_n(q)}(G)$ on $V$ induces a permutation on the set of homogeneous components; in other words, the $V_i$ form the blocks of a system of imprimitivity. Let $R$ be the full stabiliser in $\text{GL}_n(q)$ of this system, then $R$ has the shape $\text{GL}(V_1) \wr S_k$ by [32, Proposition 4.2.9] and $R$ is equal to $(\text{GL}_{n/k}(q) \wr S_k)^{\chi^{-1}}$. The group $R$ is a proper subgroup of $\text{GL}_n(q)$ as long as $k > 1$. Hence $R$ is an overgroup for $\text{N}_{\text{GL}_n(q)}(G)$.

Let $G|_{V_1}$ be the group induced by the action of $G$ on $V_1$. We might hope to recurse further by taking $(\text{N}_{\text{GL}(V_1)}(G|_{V_1}) \wr S_t/m)$ as an overgroup for $\text{N}_{\text{GL}_n(q)}(G)$. However $\text{N}_{\text{GL}(V_1)}(G|_{V_1})$ may not be equal to $\text{N}_{\text{GL}(V_2)}(G|_{V_2})$; for example, consider $G = \text{Sp}_d(q) \times \text{SL}_d(q)$.

**9.2.2 Tensor Product case**

Suppose $G$ preserves (9.2) with $k = 1$. That is, $G$ is completely reducible and its action on $V$ preserves each term in

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_t,$$

where $t > 1$ and the $W_i$ are irreducible submodules isomorphic to the sole constituent, $A$, of $V$. Suppose $A$ is absolutely irreducible and let $\chi$ be the change of basis matrix created from the basis vectors of $\text{Hom}_G(A, V)$, as
described in Subsection 9.1.1. Note that \( \dim(\text{Hom}_G(A,V)) = t \). We first consider the special case where \( \dim(A) = 1 \).

**Lemma 9.2.2.** Let \( G \leq \text{GL}_n(q) \) and let \( A \) be as above. If \( A \) has dimension 1, then \( N_{\text{GL}_n(q)}(G) = \text{GL}_n(q) \).

**Proof.** We show that \( G \) consists only of scalar matrices. Let \( \chi \) be as above and suppose \( g \in G \chi \), then \( g \) is a diagonal matrix with entries \( \alpha_1, \ldots, \alpha_n \) on the diagonal, where \( \alpha_i \in \mathbb{F}_q^* \). Let \( e_i \) be a basis vector of \( A \) and suppose there is a \( G \)-isomorphism \( \phi : \text{Span}(e_i) \to \text{Span}(e_j) \), such that \( e_i \phi = \lambda_i e_j \), for some \( \lambda_i \in \mathbb{F}_q^* \). Then

\[
(e_i g) \phi = (e_i \phi) g \\
\Rightarrow \alpha_i \lambda_i e_j = \alpha_j \lambda_i e_j \\
\Rightarrow \alpha_i = \alpha_j.
\]

So \( g \), and therefore \( g^{\chi^{-1}} \), is a scalar matrix and \( G \leq Z(\text{GL}_n(q)) \). \( \square \)

The above situation is dealt with in Step 2 of \textbf{NormaliserGL} (see Subsection 8.4). For the rest of the Tensor Product case we assume that \( \dim(A) > 1 \), i.e. \( t < n \).

Recall that the tensor product of matrix groups \( K \) and \( M \) is generated by the \textit{Kronecker products} of the generators of \( K \) with \( \text{id}_M \) and the generators of \( M \) with \( \text{id}_K \) (see Section 1.2 for details). The following is proved in [25].

**Lemma 9.2.3.** Let \( G \) and \( \chi \) be as above, with \( t \neq n \). Then \( N_{\text{GL}_n(q)}(G) \) is contained in a tensor product \( (L \otimes \text{GL}_{n/t}(q))^{\chi^{-1}} \), where \( L \leq \text{GL}_t(q) \).

**Proof.** Consider the action of \( r \in N_{\text{GL}_n(q)}(G) \) on \( V \). We shall describe the matrix \( M_r \) representing this action, with respect to a particular basis, and then show that the group \( M := \{ M_r : r \in N_{\text{GL}_n(q)}(G) \} \) is contained in a tensor product. We proceed by examining the action of \( r \) on \( W_1 \) and using the fact that the \( W_i \) are all isomorphic.

Let \( d = \dim(W_1) \), then by Lemma 9.1.5, the submodule \( W_1 r \) is a \( d \)-dimensional \( G \)-module isomorphic to \( W_1 \) and hence by Lemma 9.1.14, the submodule \( W_1 r \) can be diagonally embedded in some subset of the \( W_i \). Since the \( W_i \) are all isomorphic, we can define \( G \)-module isomorphisms \( \theta_i : W_1 \to W_i \), for each \( 1 \leq i \leq t \), and these maps form a basis for the vector space \( \text{Hom}_G(W_1, V) \) over \( \mathbb{F}_q \). There exists a \( G \)-module monomorphism \( \sigma : W_1 \to V \), such that \( W_1 \sigma = W_1 r \), given by \( \sigma := \lambda_{11} \theta_1 + \cdots + \lambda_{1t} \theta_t \), for some \( \lambda_{ij} \in \mathbb{F}_q \).
Let $B = \{e_1, e_2, \ldots, e_d\}$ be a basis for $W_1$. Then for each $e_i \in B$ there exist $a_{ij} \in \mathbb{F}_q$, such that

$$e_i r = \left( \sum_{j=1}^d a_{ij} e_j \right) \sigma$$

$$= \lambda_{1i} \left( \sum_{j=1}^d a_{ij} e_j \right) \theta_1 + \cdots + \lambda_{ti} \left( \sum_{j=1}^d a_{ij} e_j \right) \theta_t.$$

Let $F_r := (a_{ij})_{d \times d}$. Define a basis for $V$ by $B_V = B\theta_1 \cup B\theta_2 \cup \cdots \cup B\theta_t$ and let $M_r$ be the matrix representing the action of $r$ on $V$ with respect to $B_V$. Then the top $d$ rows of $M_r$ consist of $t$ square blocks of dimension $d$ given by $\lambda_{11} F_r, \ldots, \lambda_{tt} F_r$, from left to right.

Now we consider the action of $r$ on some other $W_i = W_1 \theta_i$. Note that $w \theta_i r = w \theta_i r'$, for all $w \in W_1$, and so $W_i r = W_1 r \theta_i r'$. Let $g \in G$, let $h := rgr^{-1}$ and recall that $\theta_i$ commutes with the action of $G$. Then

$$W_i \theta_i r' g = W_i r^{-1} \theta_i r (r^{-1} hr) = W_i r^{-1} \theta_i hr = W_i r^{-1} h \theta_i r = W_i r^{-1} (rgr^{-1}) \theta_i r = W_i g \theta_i r',$$

so $\theta_i r'$ commutes with the action of $G$. Therefore the map $\theta' = \sigma \theta_i r'$ is a $G$-isomorphism from $W_1$ to $W_i r$ and hence there exist $\lambda_{ij} \in \mathbb{F}_q$ such that $\theta' = \lambda_{1i} \theta_1 + \cdots + \lambda_{ti} \theta_t$. Now the rows of $M_r$ which correspond to its action on $W_i$, that is rows $\{d(i - 1) + 1, \ldots, di\}$ of $M_r$, consist of $t$ square blocks of dimension $d$, given by $\lambda_{11} F_r, \ldots, \lambda_{tt} F_r$.

Therefore $M_r$ is the Kronecker product of the matrix $L_r := (\lambda_{ij})_{t \times t}$ and the matrix $F_r \in \text{GL}(W_1)$. Let $L = \{L_r : r \in \text{N}_{\text{GL}_{n/t}(q)}(G)\}$, then the group $M := \{M_r : r \in \text{N}_{\text{GL}_{n}(q)}(G)\}$ representing the action of $\text{N}_{\text{GL}_{n}(q)}(G)$ on $V$ is contained in $L \otimes \text{GL}(W_1) = (L \otimes \text{GL}_{n/t}(q))^\times$.

Since we cannot compute $M$ without knowledge of $\text{N}_{\text{GL}_{n}(q)}(G)$, we take for our overgroup $R := (\text{GL}_{n}(q) \otimes \text{GL}_{n/t}(q))^\times \geq M^\times$. The group $R$ is a proper subgroup of $\text{GL}_{n}(q)$, as long as $1 < t < n$. We know that $t > 1$, since $G$ is reducible, and we have already assumed that $t < n$, or else Lemma 9.2.2 shows that $G$ is a group of scalar matrices.
9.2.3 Problem case

Suppose $G$ preserves (9.2) with $k = 1$. That is $G$ is completely reducible and its action on $V$ preserves each term in

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_t,$$

where the $W_i$ are pairwise isomorphic submodules which are irreducible, but not absolutely irreducible. The normaliser $N_{\text{GL}_n(q)}(G) \leq (\text{GL}_n/t(q^*) \otimes \text{GL}_t(q)) \cap \text{GL}_n(q)$, for some $s$, by [10]. However we have not had time to deal with this case, so we default to the original algorithm.

9.2.4 Direct Product case

Suppose $G$ preserves (9.2) with $k > 1$. That is, $G$ is completely reducible and its action on $V$ preserves each term in

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_k,$$

where $k > 1$ and each $V_i$ is the homogeneous component with associated constituent $A_i$. We partition the $V_i$ as follows. First partition the $V_i$ according to the dimension $b_i$ of $A_i$, then partition these sets according to the multiplicity $m_i$ of $A_i$, and let $Y_1, \ldots, Y_s$ be the submodules of $V$ generated by the resulting sets. The action of $G$ fixes each $Y_j$. We may assume that $s > 1$, since otherwise all the $V_i$ have the same dimension and multiplicity, and hence $G$ lies in the Wreath Product case.

Let $\chi$ be the change of basis matrix created from the basis vectors of $\text{Hom}_G(A_i, V)$, for each $i \in \{1, \ldots, k\}$, as described in Subsection 9.1.1. Let $f_i$ be the dimension of $Y_i$, then an overgroup for $N_{\text{GL}_n(q)}(G)$ is as follows.

**Lemma 9.2.4.** Let $G$ be as described above and let $R$ be the group of block diagonal matrices of the form

$$
\begin{pmatrix}
B_1 & 0 & \cdots & 0 \\
0 & B_2 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & B_s
\end{pmatrix},
$$

where $B_i \in \text{GL}_{f_i}(q)$. Then $R\chi^{-1}$ is an overgroup for $N_{\text{GL}_n(q)}(G)$.

**Proof.** Since $N_{\text{GL}_n(q)}(G)^\chi$ is in block diagonal form, each block corresponds to a subgroup of $\text{GL}_{f_i}(q)$. Let $W_i$ be an irreducible submodule in $Y_i$, let $r \in N_{\text{GL}_n(q)}(G)^\chi$ and let $r_i := r|_{Y_i}$, then $Wr_i \leq Y_i$, by Lemma 9.1.6. Hence $Y_i r_i = Y_i$ and $r_i \in \text{GL}(Y_i)$ for each $i$. If $s > 1$, then clearly $R < \text{GL}_n(q)$, and therefore $R\chi^{-1}$ is an overgroup for $N_{\text{GL}_n(q)}(G)$. \qed
We use recursion to find an even smaller overgroup as follows. Let \( G_i := G|_{Y_i} \) and let \( f_i := \dim(Y_i) \). Use \text{NormaliserGL}(G_i;\text{Overgroup} := \text{true})\) to find an overgroup \( R_i \) for each \( N_{\text{GL}_n(q)}(G_i) \). Then
\[
R := (R_1 \times R_2 \times \ldots, \times R_s)^{\chi^{-1}}
\]
is an overgroup for \( N_{\text{GL}_n(q)}(G) \). Note that, in general,
\[
N_{\text{GL}_n(q)}(G) \neq (N_{\text{GL}_{f_1}(q)}(G_1) \times N_{\text{GL}_{f_2}(q)}(G_2) \times \cdots \times N_{\text{GL}_{f_s}(q)}(G_s))^{\chi^{-1}},
\]
so we do not calculate each individual normaliser.

### 9.2.5 Submodule Stabiliser case

Now suppose that \( G \) is not completely reducible. In this case we take our overgroup \( R \) to be the stabiliser of an appropriate \( G \)-submodule of \( V \), as we shall describe below.

Let \( W \) be an irreducible \( b \)-dimensional \( G \)-submodule of \( V \), and let \( m \) be the number of constituents which are isomorphic to \( W \) and are submodules. Suppose any other irreducible \( G \)-submodule of \( V \) of dimension \( b \) which is not isomorphic to \( W \) has multiplicity different from \( m \). Let \( V_1 \) be the homogeneous component generated by all irreducible submodules isomorphic to \( W \), and denote the dimension of \( V_1 \) by \( d := mb \). Let \( \chi \) be the change of basis matrix formed from the basis vectors of \( \text{GHom}_G(W,V) \), as described in Subsection 9.1.1, then
\[
\text{Stab}_{\text{GL}_n(q)}(V_1) = \text{Stab}_{\text{GL}_n(q)}(\text{GL}_d(q))^{\chi^{-1}}.
\]

**Lemma 9.2.5.** Let \( G \) and \( V_1 \) be as above. Then the group \( \text{Stab}_{\text{GL}_n(q)}(V_1) \) of shape
\[
q^{d(n-d)} \cdot (\text{GL}_d(q) \times \text{GL}_{n-d}(q))
\]
is an overgroup for \( N_{\text{GL}_n(q)}(G) \).

**Proof.** Let \( r \in N_{\text{GL}_n(q)}(G) \). Then by Lemma 9.1.6 the submodule \( Wr \) has the same dimension and multiplicity as \( W \), which implies that \( V_1r = V_1 \). Hence \( N_{\text{GL}_n(q)}(G) \leq \text{Stab}_{\text{GL}_n(q)}(V_1) \), the shape of which is given in [32, Proposition 4.1.17]. Clearly \( \text{Stab}_{\text{GL}_n(q)}(V_1) \leq \text{GL}_n(q) \) unless \( W = V \), in which case \( G \) is irreducible. Hence \( \text{Stab}_{\text{GL}_n(q)}(V_1) \) is an overgroup for \( N_{\text{GL}_n(q)}(G) \).

The above argument can be applied more generally. Let \( V_1, \ldots, V_k \) be the homogeneous components of \( V \) and partition the \( V_i \) as in the Direct Product case, obtaining sets \( Y_1, \ldots, Y_s \). Note that this time the \( V_i \) do not span \( V \). Let \( S \) be a \( G \)-submodule generated by a subset of the \( Y_j \) described above and let \( \dim(S) = d \). Let \( m_i \) and \( b_i \) be the multiplicity and dimension, respectively, of the subspaces belonging to \( Y_i \) and note that for any \( V_i \leq S \), if...
there exists \( j \) such that both \( b_i = b_j \) and \( m_i = m_j \), then \( V_j \) is also contained in \( S \). Let \( \chi \) be the change of basis matrix created from the basis vectors of \( \text{Hom}_G(A_i, V) \), for each constituent \( A_i \in S \), as described in Subsection 9.1.1. Then \( \text{Stab}_{\text{GL}_n(q)}((\text{GL}_d(q))^{x^{-1}} = \text{Stab}_{\text{GL}_n(q)}(S) \).

**Corollary 9.2.6.** Let \( S \) be as above, then \( Sr = S \), for all \( r \in \text{N}_{\text{GL}_n(q)}(G) \). The stabiliser \( \text{Stab}_{\text{GL}_n(q)}(S) \) is an overgroup for \( \text{N}_{\text{GL}_n(q)}(G) \).

Suppose \( V \) has irreducible \( G \)-submodules of more than one dimension or multiplicity. Then we have a choice of which combination of the \( Y_i \) to stabilise and we try to choose the set which provides the overgroup of smallest order. The stabiliser in \( \text{GL}_n(q) \) of a \( d \)-dimensional subspace has shape

\[ q^{d(n-d)}; (\text{GL}_d(q) \times \text{GL}_{n-d}(q)). \]

Since \( |\text{GL}_d(q)| \approx q^{d^2-1} \), the order of this stabiliser is approximately

\[ q^{d(n-d)}q^{d^2-1}q^{(n-d)^2-1} = q^{n^2+d^2-dn-2}, \]

which is minimal when \( d = n/2 \). We let \( R \) be the stabiliser of the combination of \( Y_i \) with dimension closest to \( n/2 \), in order to make our overgroup as small as possible (in general).

**Theorem 9.2.7.** Let \( G < \text{GL}_n(q) \) be a reducible group which does not lie in the Problem case described in Definition 9.1.11. Then we can find an overgroup \( R \), such that \( \text{N}_{\text{GL}_n(q)}(G) \leq R < \text{GL}_n(q) \).

Every reducible group \( G < \text{GL}_n(q) \) falls into at least one of the cases we have examined. For each case except the Problem case, the overgroup \( R \) is smaller than \( \text{GL}_n(q) \), as long as \( G \) is non-scalar, and so \( \text{N}_R(G) = \text{N}_{\text{GL}_n(q)}(G) \) should be faster to compute for sufficiently large \( n \) and \( q \).

We now present an algorithm which forms part of \( \text{NormaliserGL} \) for Aschbacher class \( C_1 \).

### 9.3 The algorithm: \text{NormaliserReducible}

In this section we expand the term “overgroup” to include \( \text{GL}_n(q) \), for convenience.

A group \( G \leq \text{GL}_n(q) \) can be recognised as reducible using the algorithms of [26], [29] and [57], in time polynomial in \( n \) and \( \log q \). We now give a rough explanation of the algorithm \text{NormaliserReducible} which takes as input a reducible matrix group \( G \leq \text{GL}_n(q) \), and returns an overgroup \( R \), such that \( \text{N}_{\text{GL}_n(q)}(G) \leq R \), for certain \( G \). The algorithm only fails when \( G \) lies in the Problem case described in Subsection 9.2.3, and in this situation it returns \( \text{GL}_n(q) \).
Step 1. Let $V := \text{GModule}(G)$. Calculate the constituents $A_1, \ldots, A_t$ of $V$ and their multiplicities $m_i$, using \text{ConstituentsWithMultiplicities}(V). For $1 \leq i \leq t$, compute $\text{Hom}_G(A_i, V)$ and let $\Phi_i$ denote its basis. Use \text{IsAbsolutelyIrreducible} to check whether each constituent is absolutely irreducible. Use the function \text{IsDecomposable} to check whether $V$ can be written as a direct sum of $G$-modules. Then check the dimensions of these submodules to determine whether $G$ is completely reducible.

Step 2. Define sets $Y_1, Y_2, \ldots, Y_s$ containing all absolutely irreducible submodules of the same dimension $d_i$ and multiplicity $m_i$, as in Section 9.2.4. Note that any $Y_i$ may contain non-isomorphic constituents. Calculate the dimensions of each possible collection of the $Y_i$.

If $G$ is not completely reducible, then we are in the Submodule Stabiliser case. Let $S$ be the set of $Y_i$, the sum of whose dimensions is as close to $n/2$ as possible, and let $d := \dim(S)$. Calculate the change of basis matrix $\chi$ using the $\Phi_j$ associated with the constituents of $Y_i \in S$, as described in Subsection 9.1.1. Return $R := \text{Stab}_{\text{GL}_n(q)}(\text{GL}_d(q))^{\chi^{-1}}$.

Step 3. Otherwise, $G$ is completely reducible. If each $Y_i$ contains precisely one isomorphism type, then the $Y_i$ are the homogeneous components given in (9.2); let $k = s$. Create the change of basis matrix $\chi$ using all of the $\Phi_i$, as described in Subsection 9.1.1. One of the following holds.

- Case $k = 1$: There is precisely one $Y_i$ and either
  1. the $A_j$ contained in $Y_i$ are not absolutely irreducible. This is the Problem case so the algorithm fails. Return $R := \text{GL}_n(q)$; or
  2. the $A_j$ contained in $Y_i$ are absolutely irreducible and we are in the Tensor Product case. Return $R := (\text{GL}_d(q) \otimes \text{GL}_{d_1 m_1}(q))^{\chi^{-1}}$.

- Case $k > 1$: There is more than one $Y_i$ and we are in the Direct Product case. For each $i \in \{1, \ldots, k\}$ we use our algorithm recursively, calculating $R_i := \text{NormaliserGL}(G|Y_i; \text{Overgroup} := \text{true})$. Then $R_i$ is an overgroup for $N_{\text{GL}_d(q)}(G|Y_i)$. Return

$$R := \text{DirectProduct}(R_1, R_2, \ldots, R_k)^{\chi^{-1}}.$$ 

Step 4. Otherwise, each $Y_i$ contains more than one isomorphism type. Either

- Case $k = 1$: there is just one $Y_i$ and we are in the Wreath Product case. Create the change of basis matrix $\chi$ using $\Phi_1$, as described in Subsection 9.1.1. Return $R := (\text{GL}_{d_1}(q) \wr S_t)^{\chi^{-1}}$; or

118
• **Case** $k > 1$: there is more than one $Y_i$ and we are in the Direct Product case. Construct the change of basis matrix $\chi$ using all of the $\Phi_i$, as described in Subsection 9.1.1. For each $i \in \{1, \ldots, k\}$ calculate $R_i := \text{NormaliserGL}(G|_{Y_i}; \text{Overgroup} := \text{true})$ and return

$$R := \text{DirectProduct}(R_1, R_2, \ldots, R_k)^{\chi^{-1}}.$$ 

This concludes our treatment of the groups in Aschbacher class $C_1$.

## 9.4 Timings

We now give timings data for calculating the normaliser in $\text{GL}_n(q)$ of a $C_1$-group using $\text{NormaliserGL}$. First we describe a method for making a list of up to 200 test groups. We obtain a list of representatives of the conjugacy classes of reducible maximal subgroups of $\text{SL}_n(q)$ by assigning $\text{CM} := \text{ClassicalMaximals("L", n, q; classes := \{1\})}$. For each group $H$ in $\text{CM}$ make 20 subgroups, each generated by 2 random elements of $H$, and add them to a list $A$. For each group $K$ in $A$ make 10 subgroups, each generated by 2 random elements of $K$, and add the reducible ones to a list $\text{gps}$, discarding any duplicates.

For several values of $n$ and $q$ we constructed the list $\text{gps}$ as above, and let $\text{test}$ be the first 100 groups in the list $\text{gps}$. For all $G$ in $\text{test}$ we timed the computation of $\text{NormaliserGL}(G)$ and the mean of these times appears in bold font in the table below. In a new MAGMA session, we timed the computation of $\text{Normaliser}(\text{GL}(n,q), G)$ for the same groups $G$, and the mean of these times is given below its bold counterpart. All values are given to three decimal places. The entry $> 300$ indicates that, for at least one group $G$ in $\text{test}$, the computation of $\text{Normaliser(GL}(n,q), G)$ took more than 300 seconds. A blank table cell indicates that either the computational time for $\text{NormaliserGL}(G)$ exceeded 300 seconds, for at least one group $G$ in $\text{test}$, or else creating test data for these values of $n$ and $q$ was too time consuming.

For each value of $n$ and $q$ which did not time out we checked that the groups returned by $\text{NormaliserGL}(G)$ and $\text{Normaliser(GL}(n,q), G)$ were the same. The test data includes groups from each of the different cases given in Definition 9.1.11.
Table 9.1: Time to compute $N_{GL_n(q)}(G)$, for $G \in C_1$ (100 trials)

<table>
<thead>
<tr>
<th>n</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>q=3</td>
<td>0.009</td>
<td>0.031</td>
<td>0.012</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.015</td>
<td>0.047</td>
<td>0.320</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0.009</td>
<td>0.157</td>
<td>3.952</td>
<td>0.336</td>
</tr>
<tr>
<td></td>
<td>0.015</td>
<td>0.189</td>
<td>5.956</td>
<td>&gt; 300</td>
</tr>
<tr>
<td>5</td>
<td>0.038</td>
<td>1.149</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.041</td>
<td>1.263</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0.189</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.219</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>0.321</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.514</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 10

\( C_2 \): Imprimitive groups

10.1 Introduction

In this chapter we describe Aschbacher class \( C_2 \), the imprimitive groups, and present an algorithm \texttt{NormaliserImprimitive} which calculates an overgroup \( R \), such that \( N_{\text{GL}_n(q)}(G) \leq R \), where \( G \) is a certain type of \( C_2 \)-group. Let \( G \leq \text{GL}_n(q) \) be absolutely irreducible and let \( E := \{e_1, e_2, \ldots, e_n\} \) be the natural basis for \( V := \mathbb{F}_q^n \) as described in Section 1.2. Aschbacher class \( C_2 \) consists of all absolutely irreducible groups \( G \leq \text{GL}_n(q) \) which are imprimitive.

**Definition 10.1.1.** Let \( G \leq \text{GL}_n(q) \) act absolutely irreducibly on \( V \) and let \( B := \{V_1, \ldots, V_t\} \) be a set of pairwise disjoint subspaces spanning \( V \), all of the same dimension \( m := n/t \). If the action of \( G \) on \( V \) permutes the \( V_i \) transitively, then \( G \) is imprimitive with block system \( B \). We write \( V = V_1 + \cdots + V_t \) and we call \( t \) the length of the block system.

Denote by \( \text{GL}_n(q)_B \) the subgroup of \( \text{GL}_n(q) \) which preserves the block system \( B \). We now describe the structure of an imprimitive group \( G \).

**Lemma 10.1.2.** Let \( G \leq \text{GL}_n(q) \) act absolutely irreducibly on \( V \), as above. Then \( G \) is conjugate in \( \text{GL}_n(q) \) to a subgroup of \( \text{GL}_m(q) \wr S_t \).

**Proof.** Clearly \( G \) is a subgroup of \( \text{GL}_n(q)_B \cong \text{GL}(V_1) \wr S_t \). Define a set of basis vectors \( \{a_{j1}, \ldots, a_{jm}\} \) for \( V_j \) and let \( x \) be the matrix whose rows are \( a_{11}, a_{1m}, a_{21}, \ldots, a_{2m}, \ldots, a_{tm} \). We show that the group \( xGx^{-1} \) acts imprimitively on \( V \) with block system

\[
E := \{\langle e_1, \ldots, e_m \rangle, \langle e_{m+1}, \ldots, e_{2m} \rangle, \ldots, \langle e_{(t-1)m+1}, \ldots, e_n \rangle\},
\]

and hence \( xGx^{-1} \leq \text{GL}_m(q) \wr S_t \).

Note that

\[
e_1x = a_{11}, \ e_2x = a_{12}, \ldots,
\]
which implies that
\[ a_{11}x^{-1} = e_1, \ a_{12}x^{-1} = e_2, \ldots. \]

Now we show that \( \langle e_1, \ldots, e_m \rangle \) is mapped to another block of \( E \) by \( xGx^{-1} \).

Let \( g \in G \) and suppose \( V_ig = V_j \). Then
\[
\langle e_1, \ldots, e_m \rangle (xgx^{-1}) = \langle a_{11}, \ldots, a_{1m} \rangle gx^{-1} = V_1gx^{-1} = V_jx^{-1}
\]
\[ = \langle a_{1j}, \ldots, a_{mj} \rangle x^{-1} = \langle e_{(j-1)m+1}, \ldots, e_{jm} \rangle. \]

The above holds analogously for the other blocks of \( E \), and hence \( xGx^{-1} \leq GL_m(q) \wr S_t \).

### 10.2 Finding normalisers of \( C_2 \)-groups

Given an absolutely irreducible imprimitive group \( G \), we wish to find an over-group \( R \) such that \( N_{GL_n(q)}(G) \leq R < GL_n(q) \). Then \( N_R(G) = N_{GL_n(q)}(G) \) and calculating \( N_R(G) \) should be quicker than computing \( N_{GL_n(q)}(G) \), for large enough \( n \) and \( q \). The group \( R \) is chosen by considering certain structures stabilised by \( N_{GL_n(q)}(G) \).

**Lemma 10.2.1.** Let \( G \) be an imprimitive group preserving the block system \( B := \{ V_1, \ldots, V_t \} \) and let \( r \in N_{GL_n(q)}(G) \). Then \( Br \) is a system of imprimitivity of length \( t \), stabilised by \( G \).

**Proof.** Let \( g_1 \in G \) and let \( g_2 = rg_1r^{-1} \), then
\[
Br g_1 = Br (r^{-1}g_2r) = Bg_2r = Br,
\]

since \( Bg = B \) for all \( g \in G \). Now the subspaces \( V_i r \) of \( Br \) are all pairwise disjoint subspaces of the same dimension which span \( V \). Hence \( Br \) is a system of imprimitivity for \( G \) of length \( t \). \( \square \)

The action of \( G \) on \( B \) permutes the \( V_i \) and hence induces a permutation of the set \( \{ 1, \ldots, t \} \). Let \( \phi : G \to S_t \) be the homomorphism associated with this action. Then the group \( K := \ker(\phi) \leq G \) consists of the elements of \( G \) which fix \( V_i \), for all \( i \). We call \( K \) the block kernel of \( B \) in \( G \).

**Lemma 10.2.2.** Let \( K \leq G \) be the block kernel of \( B \) in \( G \), and let \( r \in N_{GL_n(q)}(G) \). Then \( r^{-1}Kr \) is the block kernel of \( Br \) in \( G \).
Proof. Let $D$ be the block kernel of $Br$ in $G$. First we show that $r^{-1}Kr$ fixes the blocks of $Br$. Let $k \in K$, then

$$V_ir(r^{-1}kr) = V_ir = V_i,$$

for all $V_i \in B$, and hence $r^{-1}Kr \subseteq D$.

Now we show that $D \subseteq r^{-1}Kr$. Let $d \in D$, then

$$V_ird = V_i \iff V_i rdr^{-1} = V_i, \text{ for all } i \iff rdr^{-1} \in K \iff d \in r^{-1}Kr.$$

Hence $D = r^{-1}Kr$.

The following result will be useful later on.

**Corollary 10.2.3.** Let $B$ be a block system for an absolutely irreducible group $G$. If $K$ is the block kernel for $B$ in $G$ and $K \leq N_{GL_n(q)}(G)$, then $N_{GL_n(q)}(G) \leq GL_n(q)\{B\}$.

Proof. Let $r \in N_{GL_n(q)}(G)$. If $Br \neq B$ then the block kernels of $Br$ and $B$ are different and hence $r^{-1}Kr \neq K$, by Lemma 10.2.2, a contradiction. Hence $Br = B$ and $N_{GL_n(q)}(G) \leq GL_n(q)\{B\}$.

10.2.1 Groups stabilising one block system

We first consider the case when $G$ preserves precisely one block system of length $t$.

**Lemma 10.2.4.** Let $G$ be imprimitive and let $B := \{V_1, \ldots, V_t\}$ be the unique system of imprimitivity of length $t$ that is stabilised by $G$. Then $GL_n(q)\{B\}$ is an overgroup for $N_{GL_n(q)}(G)$.

Proof. Given any $r \in N_{GL_n(q)}(G)$ we know that $Br$ is a system of imprimitivity for $G$, by Lemma 10.2.1. Thus $Br = B$, by the uniqueness of $B$, and hence $N_{GL_n(q)}(G) \leq GL_n(q)\{B\}$.

The order of $GL_n(q)\{B\}$ is approximately $(q^{n^2})^t.t! = q^{nm}.t!$ which is in general considerably smaller than $q^{n^2} \approx |GL_n(q)|$. Also, there exist vectors of $V$ with orbits of length at most $t(q^m - 1)$ under the action of $GL_n(q)\{B\}$. In general this is much smaller than $q^{nm} - 1$, the largest orbit of a vector under $GL_n(q)$. Hence the normaliser of $G$ inside $GL_n(q)\{B\}$ should be faster to compute than $N_{GL_n(q)}(G)$, for large enough $n$ and $q$. 

123
Lemma 10.2.1. It could be that $B$

**Proof.** Let $GL$.

The group $GL$.

Lemma 10.2.5. Let $G, B_1$ and $B_2$ be as above. Then either $N_{GL_n(q)}(G) \leq GL_n(q){B_1}$, or else there exists an element $r \in N_{GL_n(q)}(G)$, such that $B_1r = B_2$ and $N_{GL_n(q)}(G) = \langle N_{GL_n(q)}(B_1) (G), r \rangle$.

**Proof.** Let $r \in N_{GL_n(q)}(G)$, then $B_1r$ is a block system stabilised by $G$, by Lemma 10.2.1. It could be that $B_1r = B_1$, for all $r \in N_{GL_n(q)}(G)$, in which case $N_{GL_n(q)}(G) \leq GL_n(q){B_1}$.

Otherwise, $B_1r = B_2$ and hence $B_2r = B_1$. Let $x \in N_{GL_n(q)}(G)$ be another element such that $B_1x = B_2$. Then $B_1x = B_1r$, so $N_{GL_n(q)}(B_1)(G) = N_{GL_n(q)}(B_2)(G)$ and $r$ is in the coset $GL_n(q){B_1}x$.

Now, $N_{GL_n(q)}(G){B_1} = N_{GL_n(q)}(B_1)(G)$ and

$$N_{GL_n(q)}(B_1)(G) \leq N_{GL_n(q)}(G),$$

therefore $N_{GL_n(q)}(G) = \langle N_{GL_n(q)}(B_1)(G), r \rangle$.

We now explain how to find a $r \in N_{GL_n(q)}(G)$ which exchanges the $B_i$. The group $G$ stabilises precisely two block systems, $B_1$ and $B_2$, of length $t$. This fact is determined computationally as follows. Obtain the block kernel $K_1$ of $B_1$ and search the normal subgroups of $G$ for another reducible subgroup of the same order which is $G$-conjugate to $K_1$ but not equal to $K_1$. If there is precisely one subgroup, $K_2$, with this property, then $G$ stabilises precisely two block systems. This process gives us a conjugating element $x \in GL_n(q)$ such that $K_1^x = K_2$, and hence $B_1x = B_2$.

By the proof of Lemma 10.2.5, there exists $s \in GL_n(q){B_1}$ such that $r = sx$. Since $r$ normalises $G$,

$$r^{-1}Gr = G$$

$$\Rightarrow (sx)^{-1}Gsx = G$$

$$\Rightarrow s^{-1}Gs = xGx^{-1}.$$

If $G$ and $xGx^{-1}$ are not conjugate in $GL_n(q){B_1}$, then all elements of $N_{GL_n(q)}(G)$ fix both block systems and hence $R := GL_n(q){B_1}$ is an overgroup for $N_{GL_n(q)}(G)$. Otherwise, we let $H := \text{Stabiliser}(G, B_1)$ and compute $\text{IsConjugate}(H, G, G^x)$ to obtain an element $s \in GL_n(q){B_1}$ such that $s(xGx^{-1})s^{-1} = G$. Then $sx \in N_{GL_n(q)}(G)$ and we let $r := sx$.

10.2.3 Groups stabilising more than two block systems

While investigating examples of imprimitive groups we have found that it is possible, but relatively uncommon, for all lengths of block systems stabilised
by an imprimitive group $G \leq \mathrm{GL}_n(q)$ to occur more than twice. When a group $G$ has been found with this property, $G$ is often the normaliser in $\mathrm{GL}_n(q)$ of an extraspecial group and so lies in the Aschbacher class $C_6$.

10.3 Computational methods

We now describe the methods used in the function $\text{NormaliserImprimitive}$ to find an overgroup $R$, such that $N_{\mathrm{GL}_n(q)}(G) \leq R$, where $G \in C_2$ stabilises no more than 2 block systems.

The function $\text{IsPrimitive}(G)$ uses the algorithms of [25] to determine whether an absolutely irreducible group $G$ is imprimitive, and if so this function returns a block system $B$ of $G$ and block kernel $K$ of $B$ in $G$. Let $G$ be an imprimitive group. We use various tests of increasing expense to determine whether there are any normal subgroups of $G$ which are conjugate to $K$ in $\mathrm{GL}_n(q)$. If not, then $G$ preserves a unique block system, by Corollary 10.2.3.

If there is another normal subgroup $H$ conjugate to $K$ inside $\mathrm{GL}_n(q)$, with conjugating element $x$, then use the method given in Section 10.2.2 together with the algorithms of [60] to find an element $r \in N_{\mathrm{GL}_n(q)}(G)$ for which $x^{-1}Kx = r^{-1}Kr$. If no such $r$ exists then $N_{\mathrm{GL}_n(q)}(G) \leq \mathrm{GL}_n(q)$.

If there are more than two distinct normal subgroups conjugate to $K$ inside $\mathrm{GL}_n(q)$ but not equal to $K$, then $G$ preserves more than two block systems and $\text{NormaliserImprimitive}(G)$ fails to find an overgroup for $N_{\mathrm{GL}_n(q)}(G)$. However, in the examples we have found, either $n$ is small or one of our other methods finds an overgroup.

10.3.1 The algorithm: $\text{NormaliserImprimitive}$

Let $G$ be an imprimitive group. The following algorithm tries to find an overgroup $R$, such that $N_{\mathrm{GL}_n(q)}(G) \leq R$. It also returns $\text{full\_norm:=true}$ if it is known that $R = N_{\mathrm{GL}_n(q)}(G)$ and $\text{false}$ otherwise.

**Step 1.** Compute $B$ using $\text{Blocks}(G)$ and $K$ using $\text{Stabiliser}(G,B)$.

**Step 2.** Let $\chi$ be the change of basis matrix formed from the image of $G$-homomorphisms from $B$ into the $G$-module of $G$, as described in Subsection 9.1.1. Compute $\mathrm{GL}_n(q)\{B\} = (\mathrm{GL}_n/t(q) \wr S_t)^{-1}$, where $t$ is the number of blocks in $B$.

**Step 3.** Use $\text{NormalSubgroups}(G;\text{OrderEqual:=}|K|)$ to obtain a list $L$ of all normal subgroups $H$ of $G$ such that $|H| = |K|$, keep those for which $H$ is reducible and $H \neq K$. 

125
If $|L| = 0$ then $G$ preserves only one block system. Return $R := GL_n(q)_{\{B\}}$ and full_norm:=FALSE.

**Step 4.** Otherwise, compute the following group-theoretic invariants of $K$ and $H$, each time checking if the invariants are equal. As soon as one invariant of $H$ is not equal to its associate in $K$, remove $H$ from $L$ and proceed to the next group in $L$. Stop when all groups in $L$ have been considered.

1. ChiefFactors($K$)
2. Constituents(GModule($K$))
3. multiset of orbit lengths.

If $|L| = 0$ then $G$ preserves only one block system. Return $R := GL_n(q)_{\{B\}}$ and full_norm:=FALSE.

**Step 5.** Otherwise, compute IsGLConjugate($H, K$) for each $H \in L$. If they are not conjugate then remove $H$ from $L$.

- If $|L| = 0$ then $G$ preserves only one block system. Return $R := GL_n(q)_{\{B\}}$ and full_norm:=FALSE.
- Else, if $|L| \geq 2$ then $G$ preserves more than 2 block systems. The algorithm fails and we follow the method given in Section 8.3 to find $N_{GL_n(q)}(G)$.

**Step 6.** Otherwise, $G$ preserves precisely 2 block systems. Let $H$ be the sole group in $L$ and let $x$ be the element conjugating $H$ to $K$. Compute IsConjugate($GL_n(q)_{\{B\}}, G, xGx^{-1}$).

- If this returns true, and a conjugating element $s$, then set $r := sx$. Then $r \in N_{GL_n(q)}(G)$, by the discussion following Lemma 10.2.5. Compute $N := Normaliser(GL_n(q)_{\{B\}}, G)$. Return $R := \langle N, r \rangle$ and full_norm:=TRUE.
- Otherwise, return $R := GL_n(q)_{\{B\}}$ and full_norm:=FALSE.

This concludes our treatment of the groups in Aschbacher class $C_2$.

### 10.4 Timings

Here we give timings data for calculating the normaliser in $GL_n(q)$ of a $C_2$-group using NormaliserGL. The test groups have been made in two ways. Let $q$ be prime and let $q^n < 4096$, then we can access all irreducible subgroups of $GL_n(q)$ either from the MAGMA database of irreducible matrix groups (when $q^n < 2500$) or else from the data generated in Chapter 3.

To obtain more test groups, we assign $S := ClassicalMaximals("L", n, q : classes:=\{2\})$ and generate a new set subs of up to 10 subgroups
generated by 2 random elements of each of the groups in \( S \), discounting any repeated groups or groups that are not imprimitive. We then take maximal subgroups of entries in \( \text{subs} \), discounting any repeats and adding the imprimitive ones to \( \text{subs} \). This is continued until either \( \text{subs} \) contains at least 100 groups, or no new groups are found (up to conjugacy). The groups obtained by this method may be of relatively large order.

For several values of \( n \) and \( q \), and for each of the above methods, we constructed a list \( \text{gps} \) of groups, and let \( \text{test} \) be the first 100 groups in \( \text{gps} \), or let \( \text{test} := \text{gps} \) if there were fewer than 100 entries in \( \text{gps} \). For all \( G \) in \( \text{test} \) we timed the computation of \( \text{NormaliserGL}(G) \) and the mean of these times appears in bold font in the table below. In a new Magma session, we timed the computation of \( \text{Normaliser(GL(n,q),G)} \), for the same groups \( G \), and the mean of these times is given below its bold counterpart. Where the size of the data set \( \text{test} \) is less than 100, the number of groups tested is given in brackets. A blank table cell indicates that either the computational time for \( \text{NormaliserGL}(G) \) exceeded 300 seconds, for at least one group \( G \) in \( \text{test} \), or else creating test data for these values of \( n \) and \( q \) was too time consuming. The entry \( > 300 \) indicates that for at least one group \( G \) in \( \text{test} \), the computation of \( \text{Normaliser(GL(n,q),G)} \) took more than 300 seconds to compute.

For most values of \( n \) and \( q \), the computation of \( \text{NormaliserGL}(G) \) is very fast, with the possible exception of a handful of groups \( G \). For this reason, the mean alone is not always an ideal indication of the efficiency of the algorithm. Let \( \mu_{\text{new}} \) and \( \mu_{\text{old}} \) be the mean of the computation times for \( \text{NormaliserGL}(G) \) and \( \text{Normaliser(GL(n,q),G)} \), respectively, and let \( m_{\text{new}} \) and \( m_{\text{old}} \) be the corresponding median values of the computation times. Where \( \mu_{\text{new}} \) is greater than \( \mu_{\text{old}} \), but \( m_{\text{new}} \) is less than or equal to \( m_{\text{old}} \), the values of \( m_{\text{new}} \) and \( m_{\text{old}} \) are given in italic font. All values are given to three decimal places.

For each value of \( n \) and \( q \) which did not time out we checked that the groups returned by \( \text{NormaliserGL}(G) \) and \( \text{Normaliser(GL(n,q),G)} \) were the same. The test data includes groups preserving one block system, two block systems and more than two block systems of the same length.
Table 10.1: Time to compute $N_{\text{GL}_n(q)}(G)$, for $G \in C_2$ in irreducible matrix group database (100 trials)

<table>
<thead>
<tr>
<th>n</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>q=2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0.029 (49)</td>
<td>0.025 (13)</td>
<td>0.030</td>
<td>0.019</td>
<td>0.046</td>
<td>0.130</td>
</tr>
<tr>
<td>5</td>
<td>0.050</td>
<td>0.042 (46)</td>
<td>0.008</td>
<td>0.009</td>
<td>0.017</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0.068</td>
<td>0.015</td>
<td>0.030 (12)</td>
<td>0.061 (35)</td>
<td>0.019</td>
<td>0.046</td>
</tr>
</tbody>
</table>
Table 10.2: Time to compute $N_{\text{GL}_n(q)}(G)$, for $G \in C_2$ generated using ClassicalMaximals (100 trials)

<table>
<thead>
<tr>
<th>n=4</th>
<th>mean</th>
<th>median</th>
<th>5</th>
<th>mean</th>
<th>median</th>
<th>6</th>
<th>mean</th>
<th>median</th>
<th>7</th>
<th>mean</th>
<th>median</th>
<th>8</th>
<th>mean</th>
<th>median</th>
</tr>
</thead>
<tbody>
<tr>
<td>q=4</td>
<td>0.010 (94)</td>
<td>0.108</td>
<td>0.060</td>
<td>3.609</td>
<td>0.160</td>
<td>0.004</td>
<td>0.075</td>
<td>0.070</td>
<td>6.402</td>
<td>4.270</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0.040 (47)</td>
<td>0.401</td>
<td>0.070</td>
<td>0.902</td>
<td>0.120</td>
<td>0.029</td>
<td>0.342</td>
<td>0.240</td>
<td>62.671</td>
<td>52.150</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0.233</td>
<td>0.075</td>
<td>2.046</td>
<td>0.145</td>
<td>303.167</td>
<td>0.670</td>
<td>0.101</td>
<td>0.100</td>
<td>2.008</td>
<td>1.930</td>
<td>295.471</td>
<td>282.170</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>0.019</td>
<td>0.023 (18)</td>
<td>0.257</td>
<td>0.060</td>
<td>0.017</td>
<td>0.155</td>
<td>6.974</td>
<td>4.945</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>0.078</td>
<td>0.066</td>
<td>10.016</td>
<td>0.230</td>
<td>0.040</td>
<td>0.388</td>
<td>66.868</td>
<td>18.875</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>0.091</td>
<td>0.040</td>
<td>14.228</td>
<td>30.092</td>
<td>0.170 (99)</td>
<td>0.061</td>
<td>0.060</td>
<td>0.976</td>
<td>2.195</td>
<td>2.200</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>0.145</td>
<td>0.070</td>
<td>45.538</td>
<td>0.865</td>
<td>0.106</td>
<td>0.105</td>
<td>2.623</td>
<td>2.565</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 11

$C_3$: Semilinear groups

11.1 Introduction

The next Aschbacher class we shall analyse is $C_3$, the semilinear groups. We begin with some definitions, before describing the groups belonging to $C_3$. Finally, we present the algorithm \texttt{NormaliserSemilinear}, which returns an overgroup for the normaliser in $\GL_n(q)$ of certain $C_3$-groups. Throughout this chapter, let $G \leq \GL_n(q)$ be irreducible.

Let $F_{q^s}$ be a field extension of $F_q$. The map $\theta \in \Aut(F_{q^s})$ is an automorphism of the field extension $F_{q^s}/F_q$ (or a $F_q$-automorphism of $F_{q^s}$) if $\theta$ fixes all elements of $F_q$. The group of all such automorphisms is the Galois group $\Gal(F_{q^s}/F_q)$.

11.1.1 Conway polynomials

It is useful when treating fields and matrix groups computationally to always retrieve the same representation of $F_q$. We can write the extension field $F_{p^n}$ of $F_p$ as the quotient ring $F_p[x]/(f(x))$, for some irreducible polynomial $f(x)$ in $F_p[x]$ of degree $n$. Conway polynomials are a standardised set of such polynomials.

Let $P = \sum_{i=0}^{n} a_i x^i$ be a non-constant polynomial in $F_q[x]$ of degree $n$. Then $P$ is monic if $a_n = 1$ and $P$ is irreducible if it cannot be written as the product of two or more non-constant polynomials in $F_q[x]$. If $P$ is the minimal polynomial of a primitive element of $F_{q^n}$ then $P$ is primitive.

Let $p$ be prime and let $q = p^n$. The definition of Conway polynomials requires us to specify an ordering on the set of polynomials of degree $n$ over $F_p$. For $n = 1$ we order the elements of $F_p$ by $0 < 1 < \cdots < p - 1$. For $n > 1$ there is a recursive definition. Let $g(x) = g_0 + \cdots + g_n x^n$ and $h(x) = h_0 + \cdots + h_n x^n$, then we define $g < h$ if and only if there is an index $k$ with $g_i = h_i$ for $i > k$ and $(-1)^{n-k} g_k < (-1)^{n-k} h_k$.

**Definition 11.1.1.** The Conway polynomial $C_{p,n}$ is the smallest monic poly-
nomial of degree \( n \) over \( \mathbb{F}_q \), with respect to the above ordering, which is irreducible and primitive, and which has the following property: for each proper divisor \( m \) of \( n \), the \( (p^n - 1)/(p^m - 1) \)-th power of a root of \( C_{p,n}(x) \) is a root of \( C_{p,m}(x) \).

When available, Conway polynomials are used in MAGMA and GAP for the construction of finite fields. Further details and a database of Conway polynomials may be found in [39].

11.2 Defining groups over larger fields

Before describing Aschbacher class \( C_3 \), we must explain how a vector space, and hence a matrix group, can be defined over different fields.

**Lemma 11.2.1.** Let \( s \) be a divisor of \( n \), then there is a \( \mathbb{F}_q \)-vector space isomorphism between \( \mathbb{F}_{nq} \) and \( \mathbb{F}_{n/sq} \).

**Proof.** An element of \( \mathbb{F}_{sq} \) can be written uniquely as a polynomial \( b_0 + b_1x + \cdots + b_{s-1}x^{s-1} \), where \( b_i \in \mathbb{F}_q \). Let \( (a_0, \ldots, a_{n-1}) \in \mathbb{F}_q^n \) and define \( \phi : \mathbb{F}_q^n \to \mathbb{F}_{n/sq} \) by

\[
(a_0, \ldots, a_{n-1}) = \left( \sum_{i=0}^{s-1} a_i x^i, \sum_{i=0}^{s-1} a_{(s+i)} x^i, \ldots, \sum_{i=0}^{s-1} a_{(n-s+i)} x^i \right).
\]

We prove that \( \phi \) is a vector space isomorphism. It suffices to prove the result when \( s = n \). In what follows, let \( (a_0, \ldots, a_{s-1}), (b_0, \ldots, b_{s-1}) \in \mathbb{F}_q^s \).

**Proof that \( \phi \) is a homomorphism of additive groups:**

\[
(a_0, \ldots, a_{s-1}) + (b_0, \ldots, b_{s-1}) = \left( \sum_{i=0}^{s-1} a_i x^i + \sum_{i=0}^{s-1} b_i x^i \right)
= \left( \sum_{i=0}^{s-1} (a_i + b_i) x^i \right) = \phi \left( (a_0 + b_0, \ldots, a_{s-1} + b_{s-1}) \right) = \phi \left( [(a_0, \ldots, a_{s-1}) + (b_0, \ldots, b_{s-1})] \right).
\]

**Proof that \( \phi \) is a bijection:**

\[
(a_0, \ldots, a_{s-1}) = (b_0, \ldots, b_{s-1}) \quad \Rightarrow \quad \sum_{i=0}^{s-1} a_i x^i = \sum_{i=0}^{s-1} b_i x^i.
\]

The latter equality is between elements of \( \mathbb{F}_q \), so \( a_i = b_i \) for all \( i \in \{0, \ldots, s-1\} \) and hence \( \phi \) is injective. The orders of \( \mathbb{F}_q[x] \) and \( \mathbb{F}_q^s \) are equal, so \( \phi \) is surjective.
Proof that $\phi$ commutes with multiplication by scalars in $F_q$: Let $b \in F_q$, then
\[
(a_0, \ldots, a_{s-1})b\phi = (a_0 b, \ldots, a_{s-1} b)\phi
= \sum_{i=0}^{s-1} a_i b x^i
= \left(\sum_{i=0}^{s-1} a_i x^i\right) b
= (a_0, \ldots, a_{s-1})\phi b.
\]
Hence we have proved that $\phi$ is a $F_q$-vector space isomorphism.

11.2.1 Embedding $GL_{n/s}(q^s)$ in $GL_n(q)$

Let $s > 1$ divide $n$ and let $\varphi$ be the $F_q$-isomorphism between $F^1_q$ and $F^s_q$ given in Lemma 11.2.1. We use $\varphi$ to define a map $\phi$ embedding $GL_{n/s}(q^s)$ in $GL_n(q)$. For now, suppose $s = n$ and let $v := (a_0, \ldots, a_{s-1}) \in F^s_q$. An element $\lambda \in GL_1(q^s) \cap GL_1(q)$ corresponds to a scalar matrix in $GL_s(q)$ under $\phi$.

Let $\sum_{i=0}^{s-1} p_i x^i$ be a monic polynomial for the field extension $F_{q^s}/F_q$ and let $y \in GL_1(q^s)$ be such that $y\phi = x$ is a primitive element of $F_{q^s}$. Then
\[
(v\phi)(y\phi) = \sum_{i=0}^{s-2} a_i x^{i+1} - a_{s-1} \sum_{i=0}^{s-1} p_i x^i
= -a_{s-1}p_0 + (a_0 - a_{s-1}p_1)x + \cdots + (a_{s-2} - a_{s-1}p_{s-1})x^{s-1}
= (a_0, \ldots, a_{s-1})A\phi
= v A\phi,
\]
where $A \in GL_s(q)$ is the matrix
\[
A := \begin{pmatrix}
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 1 \\
-p_0 & -p_1 & -p_2 & \cdots & -p_{s-1}
\end{pmatrix}.
\]

Now suppose $s < n$ and let $X$ be the diagonal block matrix composed of $n/s$ copies of $A$. Let $w \in F^n_q$, then multiplication of $w\phi$ by $x$ corresponds to multiplication of $w$ by $X$. We embed a matrix $g$ of $GL_{n/s}(q^s)$ in $GL_n(q)$ by replacing each entry $x^i$ of $g$ by the matrix $A^i$. See [27] for more details.

We illustrate this embedding with an example.

132
Example 11.2.2. Let $n = 4$, $q = 3$ and $s = 2$. Let $a_i \in \mathbb{F}_3$ for $0 \leq i \leq 3$, then $(a_0, a_1, a_2, a_3) \phi = (a_0 + a_1x, a_2 + a_3x)$. We consider multiplication in $\mathbb{F}_3^4$ by the element $x \notin \mathbb{F}_3$ and show the equivalent operation in $\mathbb{F}_3^4$. Let $x^2 - x - 1$ be a polynomial for the field extension.

$$
(a_0, a_1, a_2, a_3) \phi x = (a_0 + a_1x, a_2 + a_3x) \\
= (a_0x + a_1x^2, a_2x + a_3x^2) \\
= (a_1 + (a_0 + a_1)x, a_3 + (a_2 + a_3)x) \\
= (a_1, a_0 + a_1, a_3, a_2 + a_3) \phi \\
= (a_0, a_1, a_2, a_3) \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \phi,
$$

as expected.

11.3 Aschbacher class $C_3$

Let $V := \mathbb{F}_q^n$, and let $s > 1$ be a divisor of $n$. Then $G \leq \text{GL}_{n/s}(q^s)$ acts on $V$ via the embedding described above.

Let $W := \mathbb{F}_q^{n/s}$ and recall from Definition 1.2.3 that the set of all invertible semilinear maps $\theta : W \to W$ forms $\Gamma \text{L}_{n/s}(q^s)$, the semilinear group of $W$. If an irreducible group $G$ consists of semilinear automorphisms, we say $G$ acts semilinearly. We now define the class $C_3$.

**Definition 11.3.1.** Let $G \leq \text{GL}_n(q)$ be an irreducible group, then $G$ lies in Aschbacher class $C_3$ if there exists some $s > 1$ dividing $n$ and a vector space isomorphism $\phi : \mathbb{F}_q^n \to \mathbb{F}_q^{n/s}$, such that $G \phi$ acts semilinearly on $\mathbb{F}_q^{n/s}$, where $\phi$ is as defined in Subsection 11.2.1. Hence $G$ is isomorphic to a subgroup of $\Gamma \text{L}_{n/s}(q^s)$. We say $G$ is of semilinear type.

A $C_3$-group may or may not be absolutely irreducible, as the following lemma shows.

**Lemma 11.3.2.** A group $H \leq \text{GL}_{n/s}(q^s)$ embedded in $\text{GL}_n(q)$, as above, acts reducibly on the vector space $\mathbb{F}_q^n$.

**Proof.** Let the embedding of $\text{GL}_{n/s}(q^s)$ in $\text{GL}_n(q)$ be as defined above and let $C$ be a matrix in $\text{GL}_s(q)$ corresponding to a generator of $\mathbb{F}_q^s$. Then up to conjugacy, elements of $H$ embedded in $\text{GL}_n(q)$ are matrices divided into $n/s$ sets of $s \times s$ blocks, each of which contains an element of $\langle C \rangle \cup \{0\}$.

Let $P_x$ be a characteristic polynomial for $C$, in other words $P_x$ is a defining polynomial for $\mathbb{F}_q^s$ over $\mathbb{F}_q$. The polynomial $P_x$ splits into $s$ linear factors $\{\lambda_1, \ldots, \lambda_s\}$ when written over $\mathbb{F}_q^s$. The $\lambda_i$ are eigenvalues for $C$ and the eigenvectors of $C$ are the non-zero $v \in \mathbb{F}_q^s$ such that $Cv = \lambda_i v$. 

133
Let $v \in \mathbb{F}_q^s$, be an eigenvector for $C$ and let $v_1, \ldots, v_{n/s} \in \mathbb{F}_q^s$ be vectors corresponding to $v$, for each of the blocks. Then each matrix of $H$ maps the subspace $W := \langle v_1, v_2, \ldots, v_{n/s} \rangle$ to itself, hence $H$ acts reducibly on $\mathbb{F}_q^s$. \hfill \square

Hence if $G$ acts semilinearly with all field automorphisms trivial, then $G$ acts reducibly on $\mathbb{F}_q^s$: that is, $G$ is not absolutely irreducible. These $C_3$-groups will be treated separately.

### 11.4 Case 1: $G$ is not absolutely irreducible

Let $G \leq \text{GL}_n(q)$ be irreducible and let $s > 1$ be an integer such that $G$ is reducible over the extension field $\mathbb{F}_{q^s}$ of $\mathbb{F}_q$. Then the centraliser $C_{\text{GL}_n(q)}(G)$ is isomorphic to the group of scalar matrices with entries in $\mathbb{F}_{q^s}$, by a corollary to Lemma 1.4.1. We identify the scalar group with its associated field and write $C_{\text{GL}_n(q)}(G) \cong \mathbb{F}_{q^s}$.

Given a semilinear group $G$, we will try to find an overgroup $R$ such that $N_{\text{GL}_n(q)}(G) \leq R < \text{GL}_n(q)$. Then calculating the normaliser of $G$ inside $R$ should take less time than computing $N_{\text{GL}_n(q)}(G)$, for large enough $n$ and $q$. The following lemmas will be used to find an overgroup for $N_{\text{GL}_n(q)}(G)$.

#### Lemma 11.4.1. Let $H$ be a group and let $G \leq H$, then $C_H(G) \leq N_H(G)$.

*Proof.* The centraliser $C_H(G)$ is a subgroup of $N_H(G)$, since $c^{-1}Gc = G$ for all $c \in C_H(G)$. Let $\theta : N_H(G) \to \text{Aut}(G)$ be the homomorphism induced by the conjugation action of $N_H(G)$ on $G$. Then $C_H(G) = \ker(\theta)$ and hence $C_H(G) \leq N_H(G)$. \hfill \square

#### Lemma 11.4.2. Let $G \leq \text{GL}_n(q)$ be irreducible over $\mathbb{F}_q$ but reducible over the extension field $\mathbb{F}_{q^s}$, for some $s > 1$ dividing $n$. Then $N_{\text{GL}_n(q)}(C_{\text{GL}_n(q)}(G))$ is a subgroup of $\Pi_{n/s}(q^s)$.

*Proof.* The group $C_{\text{GL}_n(q)}(G)$ is isomorphic to $\mathbb{F}_{q^s}^*$, as stated above. We show that the conjugation action of $N_{\text{GL}_n(q)}(C_{\text{GL}_n(q)}(G))$ on $C_{\text{GL}_n(q)}(G)$ preserves its additive and multiplicative structure.

Let $Z \in \text{GL}_n(q)$ correspond to a scalar matrix $Z_1 \in Z(\text{GL}_{n/s}(q^s))$, such that $\langle Z \rangle \cong \mathbb{F}_{q^s}^*$. The action of $N_{\text{GL}_n(q)}(\langle Z \rangle)$ on $\langle Z \rangle$ preserves its multiplicative structure, since

$$N^{-1}(AB)N = (N^{-1}AN)(N^{-1}BN),$$

for all $N, A, B \in \text{GL}_n(q)$.

Let $\{0\}$ represent the $n \times n$ zero-matrix, then $\langle Z \rangle \cup \{0\} \cong \mathbb{F}_{q^s}$ forms an additive group. The action of $N_{\text{GL}_n(q)}(\langle Z \rangle)$ on $\langle Z \rangle \cup \{0\}$ preserves its additive structure, since

$$N^{-1}(A + B)N = N^{-1}AN + N^{-1}BN,$$
for all $N, A, B \in \text{GL}_n(q) \cup \{0\}$.

Hence $N_{\text{GL}_n(q)}(\langle Z \rangle)$ acts on $\langle Z \rangle \cup \{0\}$ via field automorphisms. The matrices of $\langle Z \rangle$ which correspond to elements of $\mathbb{F}_q$ are scalars of $\text{GL}_n(q)$, which are centralised by $N_{\text{GL}_n(q)}(\langle Z \rangle)$. Hence $N_{\text{GL}_n(q)}(\langle Z \rangle)$ acts on $\langle Z \rangle \cup \{0\}$ by elements of $\text{Gal}(\mathbb{F}_{q^s}:\mathbb{F}_q)$, which implies that $N_{\text{GL}_n(q)}(C_{\text{GL}_n(q)}(G)) \leq \Gamma_{\text{L}_n/s}(q^s)$.

**Remark:** In fact, since $C_{\text{GL}_n(q)}(G) \cong \mathbb{F}_{q^s}^*$, it is not hard to see that $N_{\text{GL}_n(q)}(C_{\text{GL}_n(q)}(G)) = \Gamma_{\text{L}_n/s}(q^s)$.

We now use the above lemmas to present an overgroup for $N_{\text{GL}_n(q)}(G)$.

**Lemma 11.4.3.** Let $G \leq \text{GL}_n(q)$ be irreducible over $\mathbb{F}_q$ but reducible over the extension field $\mathbb{F}_{q^s}$. Either $n = q = 2$, or else $N_{\text{GL}_n(q)}(G) \leq \Gamma_{\text{L}_n/s}(q^s)$ is an overgroup for $N_{\text{GL}_n(q)}(G)$.

**Proof.** Apply Lemma 11.4.1 with $H = \text{GL}_n(q)$, then with suitable embedding $N_{\text{GL}_n(q)}(G) \leq N_{\text{GL}_n(q)}(C_{\text{GL}_n(q)}(G))$.

Now applying Lemma 11.4.2, we deduce that $N_{\text{GL}_n(q)}(G) \leq \Gamma_{\text{L}_n/s}(q^s)$. With the exception of $\text{GL}_2(2) = \Gamma_{\text{L}_1}(4)$, the group $\Gamma_{\text{L}_n/s}(q^s)$ is smaller than $\text{GL}_n(q)$ and hence is an overgroup for $N_{\text{GL}_n(q)}(G)$.

**11.4.1 Algorithm 1**

Let $G \leq \text{GL}_n(q)$ be irreducible but not absolutely irreducible. This can be identified in low-degree polynomial time [10]. The algorithm to compute an overgroup $R$ for $N_{\text{GL}_n(q)}(G)$ makes use of the centralisers of $G$ and of $\Gamma_{\text{L}_n/s}(p^s)$ in order to find an element conjugating $G$ into $\Gamma_{\text{L}_n/s}(p^s)$.

**Lemma 11.4.4.** We can construct a generator for the centralising field of $\Gamma_{\text{L}_n/s}(p^s)$ using Conway polynomials.

**Proof.** Let $C_{p,s} = \sum_{i=0}^s p_i x^i$ be a Conway polynomial. Recall from Section 11.2.1 that the matrix

$$ A := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -p_0 & -p_1 & -p_2 & \cdots & -p_{s-1} \end{pmatrix} \in \text{GL}_s(p) $$

corresponds to the element $x$ in $\mathbb{F}_{p^s}$. The matrix $A$ is a Singer cycle of $\text{GL}_s(p)$, that is, it has order $p^s - 1$ and hence $A$ generates the field $\mathbb{F}_{p^s}^*$. Let
Let $G \leq \text{GL}_n(q)$ be irreducible but not absolutely irreducible and if $n = 2$ then let $q > 2$. The following algorithm takes $G$ as input and returns an overgroup $R$ such that $\text{N}_{\Gamma\text{L}_n}(q)(G) \leq R$.

**Step 1.** Use $\text{IsAbsolutelyIrreducible}(G)$ to find a matrix algebra generator $Z_G$ for $\Gamma\text{L}_n(q)(G)$.

**Step 2.** Obtain a generator $Z_{\Gamma}$ for the centralising field of the standard embedding of $\Gamma\text{L}_{n/s}(q^s)$, as explained in Lemma 11.4.4.

**Step 3.** $|Z_{\Gamma}| = q^s - 1$ and $|Z_G|$ divides $q^s - 1$, so let $a := q^s - 1/|Z_G|$. Set $Z_{\Gamma} := Z_G^a$ so that $|Z_G| = |Z_{\Gamma}|$.

**Step 4.** For $1 \leq i \leq q^s - 1$ with gcd($i, |Z_{\Gamma}|) = 1$, use $\text{IsSimilar}$ to test $Z_{\Gamma}^i$ and $Z_G$ for conjugacy in $\text{GL}_n(q)$. As all Singer cycles are conjugate, this will succeed and return a conjugating element $\chi$, for some $i$.

**Step 5.** Use the algorithms of [27] to construct $\Gamma\text{L}_{n/s}(q^s)$ and return the overgroup $R := \Gamma\text{L}_{n/s}(q^s)^{\chi^{-1}}$.

We now look at the remaining $C_3$-groups.

**11.5 Case 2: $G$ is absolutely irreducible**

Suppose $G \leq \text{GL}_n(q)$ is an absolutely irreducible group belonging to $C_3$. Then $G$ can be embedded in a semilinear group $\Gamma\text{L}_{n/s}(q^s)$, for some $s$ dividing $n$. Recall that elements of $G$ correspond to automorphisms of $V := \mathbb{F}_q^n$ and hence there exists a well-defined map $\psi : G \to \text{Gal}(\mathbb{F}_{q^s} : \mathbb{F}_q)$.

**Lemma 11.5.1.** The map $\psi$ is surjective.

**Proof.** The group $\text{Gal}(\mathbb{F}_{q^s} : \mathbb{F}_q) \cong \mathbb{Z}_s$. Suppose $G\psi = Z_a$, where $s = ab$ for some positive integers $a, b > 1$. The group $K := \ker(\psi)$ is irreducible and acts linearly over the extension field $\mathbb{F}_{q^s}$. Hence $K$ embeds naturally into $\text{GL}_n(q^s)$. The action of $G = K.Z_a$ stabilises some subspace of $V$ over $\mathbb{F}_{q^s}$, by Lemma 11.3.2, and hence is not absolutely irreducible. This contradicts the hypothesis and so $G\phi = Z_a$. \qed
11.5.1 One embedding

For a given $s$ there could be more than one map $\psi_1, \psi_2 : G \to \text{Gal}(\mathbb{F}_{q^s} : \mathbb{F}_q)$ satisfying the above, and hence more than one way of embedding $G$ in $\Gamma L_{n/s}(q^s)$. First, however, consider a semilinear group $G$ with a unique embedding.

**Lemma 11.5.2.** Let $K \trianglelefteq G$ and suppose that if $H \neq K$ is another normal subgroup of $G$ then $G/H \cong G/K$. Then $K$ is characteristic in $G$.

**Proof.** Let $\pi : G \to G/K$ be the natural homomorphism and let $\sigma \in \text{Aut}(G)$. Then $\sigma^{-1} \pi : G \to G/K$ is a surjective homomorphism whose kernel is the set of $x \in G$ such that $x(\sigma^{-1} \pi) \in K$; in other words $x \sigma^{-1} \in \ker \pi$. Hence $\ker (\sigma^{-1} \pi) = K \sigma$, which implies that $G/(K \sigma) \cong G/K$, by the first isomorphism theorem. Therefore $K \sigma = K$ and $K \text{char } G$. \hfill $\Box$

The following is a repeat of Lemma 8.2.1.

**Lemma 11.5.3.** Let $H$ be a group with $G \leq H$ and let $K$ be a characteristic subgroup of $G$. Then $N_H(G) \leq N_H(K)$.

We use these lemmas to prove the following theorem.

**Theorem 11.5.4.** Let $G$ be an absolutely irreducible group and suppose there a unique map $\psi : G \to \text{Gal}(\mathbb{F}_{q^s} : \mathbb{F}_q)$. Let $K = \ker(\psi)$, then $N_{\text{GL}_n(q)}(K)$ is an overgroup for $N_{\text{GL}_n(q)}(G)$.

**Proof.** The group $K \trianglelefteq G$ and if there were another subgroup $L$ such that $G/K \cong G/L$, then we could construct another map $\phi : G \to \text{Gal}(\mathbb{F}_{q^s} : \mathbb{F}_q)$ with $L = \ker(\phi)$, contradicting the hypothesis. Hence $K$ is characteristic in $G$, by Lemma 11.5.2 and therefore $N_{\text{GL}_n(q)}(G) \leq N_{\text{GL}_n(q)}(K)$, by Lemma 11.5.3. \hfill $\Box$

We perform the following computational tests to determine whether or not $G$ can be embedded in $\Gamma L_{n/s}(q^s)$ in more than one way.

**Lemma 11.5.5.** Let $G \leq \text{GL}_n(q)$ be an absolutely irreducible semilinear group and let $\psi_1, \psi_2 : G \to \text{Gal}(\mathbb{F}_{q^s} : \mathbb{F}_q)$ have isomorphic kernels $K_1$ and $K_2$, respectively. Let $P := \{p_1, p_2, \ldots, p_t\}$ be the set of prime factors of $s$. If the number $|G/G'|/s$ is not divisible by any prime in $P$ then $\text{Im}(\psi_1) = \text{Im}(\psi_2)$.

**Proof.** The images of the maps $\psi_1$ and $\psi_2$ are both isomorphic to $\mathbb{Z}_s = \text{Gal}(\mathbb{F}_{q^s} : \mathbb{F}_q)$, by Lemma 11.5.1. Since $G/G'$ is the largest abelian quotient of $G$, it must have $G/K_1$ and $G/K_2$ as quotients. Let

$$G/G' = \mathbb{Z}_s \times \mathbb{Z}_{a_1} \times \mathbb{Z}_{a_2} \times \cdots \times \mathbb{Z}_{a_t}$$
where the $a_i$ are all prime and the $f_i$ are positive integers. If $P \cap \{a_1, \ldots, a_t\}$ is empty, then $G/K_1 = G/K_2$ and hence $\text{Im}(\psi_1) = \text{Im}(\psi_2)$. 

If the above test does not prove that $\psi_1 = \psi_2$, then we search the normal subgroups of $G/G'$ for a subgroup $L/G'$, such that $L$ is irreducible but not absolutely irreducible and $|L/G'| = |K_1/G'|$. If $L/G' \neq K_1/G'$ then $L$ is the kernel of another embedding $\psi_2$.

11.5.2 Two or more embeddings

If there are two or more maps $\psi : G \to \text{Gal}(F_{q^s} : F_q)$, then this method fails to find an overgroup. We use the method given in Section 8.3 to find an overgroup for $N_{\text{GL}_n(q)}(G)$.

11.5.3 Algorithm 2

Let $G \leq \text{GL}_n(q)$ be an absolutely irreducible $C_3$-group with associated field extension $F_{q^s}$. This can be recognised as such by the algorithms of [25]. We now present an algorithm to calculate an overgroup $R$ for $N_{\text{GL}_n(q)}(G)$, as long as $G$ can be embedded in $\Gamma_{\mathfrak{l}_{n/s}}(q^s)$ in only one way. If this condition does not hold then the algorithm fails. If the derived group $G'$ has already been calculated in the course of $\text{NormaliserGL}$, prior to reaching this function, then we can avoid the potentially expensive recalculation of $G'$.

**Step 1.** Use the function $\text{WriteOverLargerField}$ to obtain $K := \ker(\psi)$, for some $\psi : G \to \text{Gal}(F_{q^s} : F_q)$.

**Step 2.** If $\gcd(s, |G : G'|/s) = 1$ then $\psi$ is unique. Return the overgroup $R := N_{\text{GL}_n(q)}(K)$.

**Step 3.** Otherwise, compute $\theta : G \to G/G'$ and make a list $M$ of normal subgroups of $G/G'$ which have the same order as $K/G'$, and whose preimage in $G$ is irreducible but not absolutely irreducible.

**Step 4.** If $|M| = 1$ then return $R := N_{\text{GL}_n(q)}(K)$. Otherwise use the method given in Section 8.3.

11.5.4 The algorithm: $\text{NormaliserSemilinear}$

We form a function $\text{NormaliserSemilinear}$ from algorithms 1 and 2, which returns an overgroup $R$ such that $N_{\text{GL}_n(q)}(G) \leq R$, for certain $C_3$-groups $G$.

This concludes our treatment of the $C_3$-groups.
11.6 Timings

We now give timings data for computing the normaliser of a $C_3$-group using $\text{NormaliserGL}$. The test groups have been made in two ways. Let $q$ be prime and let $q^n < 4096$, then we can access all irreducible subgroups of $\text{GL}_n(q)$, either from the MAGMA database of irreducible matrix groups (when $q^n < 2500$) or else from the data generated in Chapter 3.

To obtain more test groups, we assign $S := \text{ClassicalMaximals("L", n, q : classes:=\{3\})}$ and generate a new set $\text{gps}$ of up to 10 random two-generated subgroups of the groups in $S$, discounting any repeated groups and keeping only the irreducible groups. We then take maximal subgroups of entries in $\text{gps}$, discounting any repeats, and add them to $\text{gps}$. This is continued until either $\text{gps}$ contains at least 100 groups, or no new groups are found (up to conjugacy). The groups obtained by this method may be of relatively large order.

For several values of $n$ and $q$, and for each of the above methods, we constructed a list $\text{gps}$ of groups, and let $\text{test}$ be the first 100 groups in $\text{gps}$, or let $\text{test} := \text{gps}$ if there were fewer than 100 entries in $\text{gps}$. For all $G$ in $\text{test}$ we timed the computation of $\text{NormaliserGL}(G)$ and the mean of these times appears in bold font in the table below. In a new MAGMA session, we timed the computation of $\text{Normaliser}(\text{GL}(n,q), G)$, for the same groups $G$, and the mean of these times is given below its bold counterpart. Where the size of the data set $\text{test}$ is less than 100, the number of groups tested is given in brackets. A blank table cell indicates that either the computational time for $\text{NormaliserGL}(G)$ exceeded 300 seconds, for at least one group $G$ in $\text{test}$, or else creating test data for these values of $n$ and $q$ was too time consuming. The entry $> 300$ indicates that for at least one group $G$ in $\text{test}$, the computation of $\text{Normaliser}(\text{GL}(n,q), G)$ took more than 300 seconds.

For most values of $n$ and $q$, the computation of $\text{NormaliserGL}(G)$ is very fast, with the possible exception of a handful of groups $G$. For this reason, the mean alone is not always an ideal indication of the efficiency of the algorithm. Let $\mu_{\text{new}}$ and $\mu_{\text{old}}$ be the mean of the computation times for $\text{NormaliserGL}(G)$ and $\text{Normaliser}(\text{GL}(n,q), G)$, respectively, and let $m_{\text{new}}$ and $m_{\text{old}}$ be the corresponding median values of the computation times. Where $\mu_{\text{new}}$ is greater than $\mu_{\text{old}}$, but $m_{\text{new}}$ is less than or equal to $m_{\text{old}}$, the values of $m_{\text{new}}$ and $m_{\text{old}}$ are given in italic font. All values are given to three decimal places.

For each value of $n$ and $q$ which did not time out we checked that the groups returned by $\text{NormaliserGL}(G)$ and $\text{Normaliser}(\text{GL}(n,q), G)$ were the same. The test data includes absolutely irreducible $C_3$ groups with one embedding and with two or more embeddings, as well as non-absolutely irreducible $C_3$ groups.
<table>
<thead>
<tr>
<th>n</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>q=2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0.010 (63)</td>
<td>0.016 (8)</td>
<td>0.019</td>
<td>0.035 (4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0.016</td>
<td>0.010</td>
<td>0.028</td>
<td>0.188</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0.036</td>
<td>0.018</td>
<td>0.009</td>
<td>0.005</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 11.1: Time to compute $N_{\text{GL}_n(q)}(G)$, for $G \in \mathcal{C}_3$ in irreducible matrix group database (100 trials)
Table 11.2: Time to compute $N_{G_{n,q}}(G)$, for $G \in \mathcal{C}_3$ generated using ClassicalMaximals (100 trials)

<table>
<thead>
<tr>
<th>$n=4$</th>
<th>$q=4$</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>mean</td>
<td>median</td>
<td>mean</td>
<td>median</td>
<td>mean</td>
</tr>
<tr>
<td>0.10 (54)</td>
<td>0.022 (13)</td>
<td>0.291</td>
<td>0.084 (14)</td>
<td></td>
</tr>
<tr>
<td>0.007</td>
<td>0.018</td>
<td>0.020</td>
<td>&gt; 300</td>
<td>2.489</td>
</tr>
<tr>
<td>0.024</td>
<td>0.047 (13)</td>
<td>0.040</td>
<td>1.096</td>
<td>0.655 (2)</td>
</tr>
<tr>
<td>0.018</td>
<td>0.046</td>
<td>0.040</td>
<td>&gt; 300</td>
<td>31.055</td>
</tr>
<tr>
<td>0.034</td>
<td>0.145 (2)</td>
<td>0.039</td>
<td>0.605</td>
<td>10.209 (13)</td>
</tr>
<tr>
<td>0.044</td>
<td>0.549 (13)</td>
<td>0.544</td>
<td>0.516</td>
<td>&gt; 300</td>
</tr>
<tr>
<td>0.166</td>
<td>0.281 (26)</td>
<td>0.186</td>
<td>0.827</td>
<td>28.297 (52)</td>
</tr>
<tr>
<td>2.956</td>
<td>0.180</td>
<td>1.138 (8)</td>
<td>0.452</td>
<td>7.339</td>
</tr>
<tr>
<td>0.857</td>
<td>1.230 (2)</td>
<td>&gt; 300</td>
<td>98.720</td>
<td>&gt; 300</td>
</tr>
</tbody>
</table>
Chapter 12

\( \mathcal{C}_5 \): Subfield groups

12.1 Introduction

In this chapter, we define the groups belonging to Aschbacher class \( \mathcal{C}_5 \) and describe a function \texttt{NormaliserSubfield} which finds an overgroup \( R \) such that \( N_{\text{GL}_n(q)}(G) \leq R \) for certain \( \mathcal{C}_5 \)-groups, \( G \). Throughout this chapter we let \( G \leq \text{GL}_n(q) \) be absolutely irreducible and we abbreviate \( Z(\text{GL}_n(q)) \) to \( Z \).

Definition 12.1.1. An absolutely irreducible group \( G := \langle g_1, \ldots, g_n \rangle \) lies in \( \mathcal{C}_5 \) if there exists a subfield \( \mathbb{F}_{q_0} \subset \mathbb{F}_q \), a matrix \( t \in \text{GL}_n(q) \), and \( \beta_1, \ldots, \beta_m \in \mathbb{F}_q^* \) such that \( t^{-1} g_i t = \beta_i h_i \), with \( h_i \in \text{GL}_n(q_0) \).

We refer to \( \mathcal{C}_5 \)-groups as subfield groups. In general, \( G \) is subfield if it can be written over \( \mathbb{F}_{q_0} \) modulo scalars. Let \( \mathcal{A} \) be the set of subfield groups for which \( \beta_i = 1 \), for all \( 1 \leq i \leq m \), so that \( G \in \mathcal{A} \) if \( G \) is conjugate in \( \text{GL}_n(q) \) to a subgroup of \( \text{GL}_n(q_0) \).

We can determine whether a group \( G \) is subfield using the \texttt{Magma} function \texttt{IsOverSmallerField}(G) which uses the algorithms of [21] and [22]. When the \texttt{Scalars} parameter of this function is set to \texttt{false}, it identifies whether \( G \) lies in the set \( \mathcal{A} \).

Given a group \( G \), we wish to find an overgroup \( R \) for \( N_{\text{GL}_n(q)}(G) \) such that \( N_{\text{GL}_n(q)}(G) \leq R < \text{GL}_n(q) \), then computing \( N_R(G) \) should be quicker than computing \( N_{\text{GL}_n(q)}(G) \), for large enough \( n \) and \( q \). We now describe a method to find an overgroup for the normaliser in \( \text{GL}_n(q) \) of a group in \( \mathcal{A} \).

12.2 Overgroup for \( N_{\text{GL}_n(q)}(G) \) when \( G \in \mathcal{A} \)

Let \( G \) be a subfield group which is conjugate in \( \text{GL}_n(q) \) to a subgroup of \( \text{GL}_n(q_0) \), where \( q_0 \) properly divides \( q \). We begin with some definitions before presenting a theorem which will help us to determine an overgroup for \( N_{\text{GL}_n(q)}(G) \).
Definition 12.2.1. Let $G$ be a group, then a $\mathbb{F}_q$-representation of $G$ of degree $n$ is a homomorphism $T : G \rightarrow \text{GL}_n(q)$. Let $K$ be an arbitrary field, then two $\mathbb{F}_q$-representations $T$ and $U$ are $K$-equivalent if they have the same degree $n$ and there exists a fixed matrix $X \in \text{GL}_n(K)$, such that $T(g) = X^{-1}U(g)X$, for all $g \in G$.

Theorem 12.2.2. ([17, Thm 29.7]) Let $T$ and $U$ be $\mathbb{F}_q$-representations of a matrix group $G$, both of the same degree. If $T$ and $U$ are $\mathbb{F}_q$-equivalent, then $T$ and $U$ are $\mathbb{F}_q^0$-equivalent.

We use this result to find an overgroup for the normaliser in $\text{GL}_n(q_0)$ of a group $G \in A$. Recall that $Z := Z(\text{GL}_n(q_0))$.

Lemma 12.2.3. Let $G$ be an absolutely irreducible group that is conjugate in $\text{GL}_n(q)$ to a subgroup of $\text{GL}_n(q_0)$. Then $\langle \text{GL}_n(q_0), Z \rangle$ is an overgroup for $\text{N}_{\text{GL}_n(q)}(G)$.

Proof. Let $r \in \text{N}_{\text{GL}_n(q)}(G)$, then by Theorem 12.2.2 there exists $y \in \text{GL}_n(q_0)$ such that $y^{-1}(r^{-1}gr)y = g$ for all $g \in G$ and hence $ry$ centralises $G$. Hence $ry \in Z$, by Schur’s lemma 1.4.1, and therefore $r \in \langle \text{GL}_n(q_0), Z \rangle =: R$. Clearly $|R| < |\text{GL}_n(q)|$ and so this is an overgroup for $\text{N}_{\text{GL}_n(q)}(G)$.

The next theorem follows from Aschbacher’s theorem [3] and gives a method to find an even smaller overgroup for $\text{N}_{\text{GL}_n(q)}(G)$.

Lemma 12.2.4. Let $G$ be a subfield group in $A$ and let $t \in \text{GL}_n(q)$ such that $t^{-1}gt \in \text{GL}_n(q_0)$ for all $g \in G$. Then either $t^{-1}Gt$ contains a subgroup isomorphic to $\text{SL}_n(q_0)$ or else $t^{-1}Gt$ is contained in some Aschbacher class $C_i$, with respect to $\text{GL}_n(q_0)$.

Hence if $t^{-1}Gt$ does not contain a subgroup isomorphic to $\text{SL}_n(q_0)$ and $R$ is a $C_i$-overgroup for $\text{N}_{\text{GL}_n(q_0)}(G)$ inside $\text{GL}_n(q_0)$, then $\langle R, Z \rangle$ is a $C_5$-overgroup for $\text{N}_{\text{GL}_n(q)}(G)$ inside $\text{GL}_n(q)$.

12.2.1 Subfield groups not in $A$

If $G$ is a subfield group not contained in $A$ then we use the methods of Section 8.3 to try to find an overgroup for $\text{N}_{\text{GL}_n(q)}(G)$.

Proposition 12.2.5. If the derived group $G'$ of a subfield group $G$ is absolutely irreducible, then it is in $A$.

Proof. Let $g_1^{-1}g_2^{-1}g_1g_2 \in G'$, where $g_1, g_2 \in G$ and for $i \in \{1, 2\}$, suppose
$t^{-1}g_it = \beta_ih_i$, where $\beta_i \in \mathbb{F}_q^*$ and $h_i \in \text{GL}_n(q_0)$. Then
\[
\begin{align*}
t^{-1}(g_1^{-1}g_2^{-1}g_1g_2)t & = (t^{-1}g_1^{-1}t)(t^{-1}g_2^{-1}t)(t^{-1}g_1t)(t^{-1}g_2t) \\
& = (\beta_1h_1)^{-1}(\beta_2h_2)^{-1}(\beta_1h_1)(\beta_2h_2) \\
& = \beta_1^{-1}\beta_2^{-1}\beta_2h_1^{-1}h_2^{-1}h_1h_2 \\
& = h_1^{-1}h_2^{-1}h_1h_2,
\end{align*}
\]

since the $\beta_i$ are scalars. This is an element of $\text{GL}_n(q_0)$ and hence if $G'$ is absolutely irreducible, then $G'$ is a $C_5$-group lying in $\mathcal{A}$.

Hence, we can calculate an overgroup $R$ for $N_{\text{GL}_n(q)}(G')$, as described above, and $R$ is an overgroup for $N_{\text{GL}_n(q)}(G)$.

### 12.3 The algorithm: NormaliserSubfield

Let $G \leq \text{GL}_n(q)$ be absolutely irreducible and conjugate in $\text{GL}_n(q)$ to a group $H \leq \text{GL}_n(q_0)$. This is determined by $\text{IsOverSmallerField}(G : \text{Scalars}:=\text{false})$. The function $\text{NormaliserSubfield}(G)$ returns an overgroup $R$ such that $N_{\text{GL}_n(q)}(G) \leq R$.

**Step 1.** Let $\chi := \text{SmallerFieldBasis}(G)$, then $G^\chi = H$.

**Step 2.** Compute $R_2$ using $\text{NormaliserGL}(H : \text{Overgroup}:=\text{true})$.

**Step 3.** Return $R := \langle R_2, Z \rangle^{\chi^{-1}}$.

This concludes our treatment of the $C_5$-groups.

### 12.4 Timings

We now give timings data for computing the normaliser in $\text{GL}_n(q)$ of a $C_5$-group using $\text{NormaliserSubfield}$. We generate example groups for testing by the following method. Fix $n$ and $q$ and use $\text{ClassicalMaximals("L",n,q : \text{classes}:=\{5\})}$ to obtain a list $\mathcal{CM}$ of $C_5$-groups which are maximal in $\text{GL}_n(q)$. For each $G$ in $\mathcal{CM}$, create 10 subgroups, each generated by 2 random elements of $G$, and add them to a list $\mathcal{gps}$, discarding any duplicates and any groups that are not absolutely irreducible. Now compute the maximal subgroups of each $G$ in $\mathcal{gps}$ and add them to $\mathcal{gps}$ if they are not already there (up to conjugacy). Continue until either $\mathcal{gps}$ contains at least 100 groups, or else no new groups are found (up to conjugacy).

For several values of $n$ and $q$ we constructed a list $\mathcal{gps}$ of groups as described above, and let $\mathcal{test}$ be the first 100 groups in $\mathcal{gps}$, or let $\mathcal{test}:=\mathcal{gps}$.
if there were fewer than 100 entries in gps. For all $G$ in test we timed the computation of $\text{NormaliserGL}(G)$ and the mean of these times appears in bold font in the table below. In a new Magma session, we timed the computation of $\text{Normaliser}(\text{GL}(n,q),G)$, for the same groups $G$, and the mean of these times is given below its bold counterpart. Where the size of the data set test is less than 100, the number of groups tested is given in brackets. A blank table cell indicates that either the computational time for $\text{NormaliserGL}(G)$ exceeded 300 seconds, for at least one group $G$ in test, or else creating test data for these values of $n$ and $q$ was too time consuming.

For most values of $n$ and $q$, the computation of $\text{NormaliserGL}(G)$ is very fast, with the possible exception of a handful of groups $G$. For this reason, the mean alone is not always an ideal indication of the efficiency of the algorithm. Let $\mu_{\text{new}}$ and $\mu_{\text{old}}$ be the mean of the computation times for $\text{NormaliserGL}(G)$ and $\text{Normaliser}(\text{GL}(n,q),G)$, respectively, and let $m_{\text{new}}$ and $m_{\text{old}}$ be the corresponding median values of the computation times. Where $\mu_{\text{new}}$ is greater than $\mu_{\text{old}}$, but $m_{\text{new}}$ is less than or equal to $m_{\text{old}}$, the values of $m_{\text{new}}$ and $m_{\text{old}}$ are given in italic font. All values are given to three decimal places.

For each value of $n$ and $q$ which did not time out we checked that the groups returned by $\text{NormaliserGL}(G)$ and $\text{Normaliser}(\text{GL}(n,q),G)$ were the same. The test data includes subfield groups lying both inside and outside the set $A$. 
Table 12.1: Time to compute $N_{GL_n(q)}(G)$, for $G \in C_5$ (100 trials)

<table>
<thead>
<tr>
<th>n=4</th>
<th>$q=4$</th>
<th>0.013 (79)</th>
<th>0.017 (10)</th>
<th>0.010</th>
<th>0.083</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.004</td>
<td>0.014</td>
<td>0.014</td>
<td></td>
<td>3.700</td>
</tr>
<tr>
<td>8</td>
<td>0.012 (71)</td>
<td>0.031 (10)</td>
<td>0.050</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.014</td>
<td>0.161</td>
<td>4.685</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>0.043</td>
<td>0.040</td>
<td>2.134</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.042</td>
<td>0.040</td>
<td>&gt; 300</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>0.027</td>
<td>2.324</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.119</td>
<td>18.409</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>0.110</td>
<td>1.701</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.905</td>
<td>&gt; 300</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 13

\( \mathcal{C}_8 \): Classical Groups

13.1 Preliminaries

In this section we describe Aschbacher class \( \mathcal{C}_8 \) and present an algorithm \texttt{NormaliserClassical} to find an overgroup \( R \) such that \( N_{\text{GL}_n(q)}(G) \leq R \), for a group \( G \in \mathcal{C}_8 \). Then computing the normaliser of \( G \) inside \( R \) should be faster than computing \( N_{\text{GL}_n(q)}(G) \), for large enough \( n \) and \( q \).

We go on to define another class \( \mathcal{C}'_8 \) which is related to \( \mathcal{C}_8 \), and explain how to find an overgroup \( R \) such that \( N_{\text{GL}_n(q)}(G) \leq R \), for certain groups \( G \in \mathcal{C}'_8 \\setminus \mathcal{C}_8 \). We begin with some general definitions and notation.

Throughout this section, let \( G \leq \text{GL}_n(q) \) be an absolutely irreducible group. Recall that \( G \) is quasisimple if it is perfect and the projective group \( G/Z(G) \) is non-abelian simple. The quasisimple classical groups are \( \text{SL}_n(q) \), \( \text{Sp}_n(q) \), \( \text{SU}_n(q) \) and \( \Omega_\epsilon^n(q) \), for \( \epsilon \in \{\circ, +, -\} \), with the exception of certain small values of \( n \) and \( q \) for which the projective group \( G/Z(G) \) is not simple (see Theorem 1.5.11). Details of the classical groups may be found in Chapter 1.5.

\textbf{Definition 13.1.1.} An absolutely irreducible group \( G \leq \text{GL}_n(q) \) lies in class \( \mathcal{C}_8 \) if there is a quasisimple classical group \( C \) in its natural representation, such that \( C \leq G \leq N_{\text{GL}_n(q)}(C) \).

The following result characterises the \( \mathcal{C}_8 \)-groups and is proved in [32, Proposition 2.10.6 (i)].

\textbf{Lemma 13.1.2.} Let \( G \in \{\text{SL}_n(q), \text{Sp}_n(q), \text{SU}_n(q), \Omega_\circ^n(q), \Omega_+^n(q), \Omega_-^n(q), \text{SO}_\circ^n(q), \text{SO}_+^n(q)\} \). Then \( G \) is absolutely irreducible on \( \mathbb{F}_q^n \) if and only if \( G \neq \Omega_\pm_2^n(q) \), for all \( q \) and \( G \neq \text{SO}_2^\pm_2(q) \), for \( q \) odd.

We now present some short results about forms and normalisers in general, before examining the \( \mathcal{C}_8 \)-groups and describing methods to find \( N_{\text{GL}_n(q)}(G) \), for certain \( G \in \mathcal{C}_8 \).
13.2 Forms and normalisers

For the rest of this section, let \( u := 2 \) in the unitary case and \( u := 1 \) otherwise. Define \( \sigma \in \text{Aut}(\mathbb{F}_{q^u}^*) \) by \( \lambda \sigma = \lambda^u \), so that \( \sigma \) acts like the identity on \( \mathbb{F}_{q^u}^* \) unless \( u = 2 \), when \( \sigma \) is an involution. For \( g \in \text{GL}_n(q^u) \), we write \( g \sigma \) for the matrix obtained by applying \( \sigma \) to each entry of \( g \) and note that \( (g \sigma)^T = g^T \sigma \).

Recall from Corollary 1.4.2, that the centraliser \( C_{\text{GL}_n(q)}(G) \) of an absolutely irreducible group \( G \) is \( \mathbb{F}_q^* \), the scalar subgroup of \( \text{GL}_n(q) \).

**Lemma 13.2.1.** An absolutely irreducible group \( G \leq \text{GL}_n(q^u) \) preserves at most one classical form of a given type, up to scalar multiplication.

**Proof.** First we prove the result for classical forms which are not quadratic in characteristic 2. Let \( f_1 \) and \( f_2 \) be distinct forms of either symplectic or unitary type, or else the associated symmetric forms of quadratic forms in characteristic other than 2. Let \( F_1, F_2 \) be the corresponding matrix representations of \( f_1 \) and \( f_2 \), as described in Subsection 1.5.2. Then for all \( g \in G \) we have \( gF_1(g^T \sigma) = F_1 \) and \( gF_2(g^T \sigma) = F_2 \), so \( g = F_2(g^{-T} \sigma)F_2^{-1} \) and \( gF_1 = F_1(g^{-T} \sigma) \). This implies that \( F_1^{-1}gF_1 = g^{-T} \sigma \) and hence \( F_2(F_1^{-1}gF_1)F_2^{-1} = g \). This shows that \( F_1F_2^{-1} \) centralises \( G \) and hence is scalar, as \( G \) is absolutely irreducible and using Corollary 1.4.2. Therefore \( f_1 = \lambda f_2 \), for some \( \lambda \in \mathbb{F}_q^* \).

Now suppose that \( G \) preserves two quadratic forms, \( Q_1 \) and \( Q_2 \), in characteristic 2, with associated matrix representations \( M_1 \) and \( M_2 \). For \( i \in \{1, 2\} \), let \( f_i \) be the symmetric form associated to \( Q_i \) and let \( M_i \) be its associated matrix. Then \( M_i + M_i^T = F_i \). By the preceding paragraphs, there exists \( \lambda \in \mathbb{F}_q^* \) such that \( f_1 = \lambda f_2 \), so it suffices to show that the diagonal entries of \( M_1 \) are equal to those of \( M_2 \), up to scalar multiplication. Let \( v \in V \), then as \( G \) is irreducible, there exists some \( g \in G \) such that \( vg \neq v \). Let \( w = v + vg \), then \( w \neq 0 \), since \( v \neq vg \). Now, \( (v)Q_i = (vg)Q_i \), since \( G \) preserves \( Q_i \). So

\[
(w)Q_i = (v + vg)Q_i
= (v)Q_i + (vg)Q_i + (v, vg)f_i
= 2(v)Q_i + (v, vg)f_i
= (v, vg)f_i,
\]

and since \( f_1 = \lambda f_2 \), we deduce that \( (w)Q_1 = \lambda(w)Q_2 \). As \( G \) is absolutely irreducible, we may choose \( g_1, \ldots, g_n \in G \) such that \( \{wg_1, \ldots, wg_n\} \) is a basis for \( V \), and since \( (wg_i)Q_1 = \lambda(wg_j)Q_2 \) for all \( i, j \), the result is proved.

We now use the preceding facts to prove a result about the normaliser in \( \text{GL}_n(q^u) \) of a classical group.
Lemma 13.2.2. Let $G \leq \text{GL}_n(q^n)$ be an absolutely irreducible group, preserving a classical form. Then $N_{\text{GL}_n(q^n)}(G)$ preserves this form up to scalar multiplication.

Proof. First suppose the form $f$ preserved by $G$ is not quadratic, and let $F$ be its matrix representation. Let $g \in G$, $x \in N_{\text{GL}_n(q^n)}(G)$ and $g_1 := xgx^{-1}$, then

$$F = gF(g^T \sigma)$$
$$xF(x^T \sigma) = x(gF(g^T \sigma))(x^T \sigma)$$
$$= x(x^{-1}g_1x)F(x^{-1}g_1x)^T \sigma(x^T \sigma)$$
$$= g_1xF(x^T g_1^{-1} x^{-T} x^T) \sigma$$
$$= g_1(xF(x^T \sigma))g_1^T \sigma.$$ 

So $xFx^T \sigma$ is a form preserved by $G$ and hence $xFx^T \sigma = \lambda F$, for some $\lambda \in \mathbb{F}_{q^n}$, by Lemma 13.2.1.

Now suppose $G$ preserves a quadratic form $Q$, and let $Q_x$ be the quadratic form given by $(v)Q_x = (vx)Q$, for all $v \in V$. Let $r \in N_{\text{GL}_n(q)}(G)$, then

$$(vg)Q_r = (vgr)Q$$
$$= (vrg_1)Q$$
$$= (vr)Q$$
$$= (v)Q_r.$$ 

Hence $Q_r$ is a scalar multiple of $Q$, by Lemma 13.2.1 and $N_{\text{GL}_n(q)}(G)$ preserves $Q$ up to scalar multiplication.

Using Lemma 13.2.2, we can now deduce the normaliser of a quasisimple classical group.

Lemma 13.2.3. Let $C$ be a quasisimple classical group, then the normaliser of $C$ in $\text{GL}_n(q^n)$ is given in Table 13.1.

Proof. By Lemma 13.1.2 the group $C$ is absolutely irreducible and by Lemma 13.2.2, the normaliser of an absolutely irreducible quasisimple classical group preserves the associated classical form up to scalar multiplication. The groups fitting this description are described in Subsections 1.5.3–1.5.6 and given in Table 13.1.

Now we examine the groups contained in $C_8$. 

149
Table 13.1: $N_{\text{GL}_n(q^u)}(C)$ for quasisimple classical group $C$

<table>
<thead>
<tr>
<th>$C$</th>
<th>$N_{\text{GL}_n(q^u)}(C)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{SL}_n(q)$</td>
<td>$\text{GL}_n(q)$</td>
</tr>
<tr>
<td>$\text{Sp}_n(q)$</td>
<td>$\text{CSP}_n(q)$</td>
</tr>
<tr>
<td>$\text{SU}_n(q)$</td>
<td>$\text{CU}_n(q)$</td>
</tr>
<tr>
<td>$\Omega^e_n(q)$</td>
<td>$\text{CO}^e_n(q)$</td>
</tr>
</tbody>
</table>

13.3 Normaliser of a $C_8$-group

Recall that $u := 2$ in the unitary case and $u := 1$ otherwise. The class $C_8$ contains all groups $G$ such that $C \leq G \leq N_{\text{GL}_n(q^u)}(C)$, for some quasisimple classical group $C$.

The Magma function RecogniseClassical determines whether an absolutely irreducible group $G$ contains a quasisimple classical group, which we call $C$. We explain below that in most cases $N_{\text{GL}_n(q^u)}(G) = N_{\text{GL}_n(q^u)}(C)$, so we can simply write down $N_{\text{GL}_n(q^u)}(G)$. When this is not the case we give an overgroup $R$, such that $N_{\text{GL}_n(q^u)}(G) \leq R < \text{GL}_n(q^u)$.

We begin by analysing the normaliser in $\text{GL}_n(q^u)$ of the quasisimple group, for each of the classical types. Recall that $\text{Out}(G) := \text{Aut}(G)/\text{Inn}(G)$ and see Table 1.6 for details of the outer automorphism group of a classical group.

An element $x \in N_{\text{GL}_n(q^u)}(C)$ belongs to at least one of the following three categories.

- $x \in C$,
- $x \in \mathbb{F}^{*}_{q^u}$ is a scalar matrix centralising $C$,
- conjugation by $x$ induces an outer automorphism of $C$.

These categories may intersect. We shall write $N_{\text{GL}_n(q^u)}(C) = \mathbb{F}^{*}_{q^u}.C.A$, where $A$ is a subgroup of $\text{Out}(C)$; note that this extension is not necessarily split.

**Theorem 13.3.1.** Let $C$ be a quasisimple classical group and let

$N_{\text{GL}_n(q^u)}(C) = \mathbb{F}^{*}_{q^u}.C.A$.

Table 1.6 gives the structure of $A$ for each of the classical types.

**Proof.** The normaliser in $\text{GL}_n(q^u)$ of a quasisimple classical group $C$ is given in Table 13.1. For each type of quasisimple classical group $C$, Table 1.6 gives $\text{Out}(C)$. Using this together with [32, Sections 2.2–2.8] we deduce the structure of $A$ for each classical type.
**Linear:** Let $C := SL_n(q)$, then $N_{GL_n(q)}(C) = GL_n(q)$ and by [32, Section 2.2]

$$|A| = |PGL_n(q) : PSL_n(q)| = (n, q - 1).$$

**Symplectic:** Let $C := Sp_{2m}(q)$, then $N_{GL_{2m}(q)}(C) = CSp_{2m}(q)$ and by [32, Section 2.4]

$$|A| = |PCSp_{2m}(q) : PSp_{2m}(q)| = (2, q - 1).$$

**Unitary:** Let $C := SU_n(q)$, then $N_{GL_n(q^2)}(C) = CU_n(q)$ and by [32, Section 2.3]

$$|A| = |PCU_n(q) : PSU_n(q)| = (n, q + 1).$$

**Orthogonal, odd dimension:** Let $C := \Omega_{2m+1}(q)$, then $N_{GL_{2m+1}(q)}(C) = CO_{2m+1}(q)$ and by [32, Section 2.5]

$$|A| = |PCO_{2m+1}(q) : P\Omega_{2m+1}(q)| = 2.$$

**Orthogonal, even dimension:** Let $C := \Omega_{\pm 2m}(q)$ with $q$ even, then $N_{GL_{2m}(q)}(C) = CO_{\pm 2m}(q)$ and by [32, Sections 2.7 and 2.8]

$$|A| = |PCO_{\pm 2m}(q) : P\Omega_{\pm 2m}(q)| = 2.$$  

When $q$ is odd, in the $+$ case

$$A = \begin{cases} Z_2 \times Z_2 & \frac{n}{4} (q - 1) \text{ odd} \\ D_8 & \frac{n}{4} (q - 1) \text{ even} \end{cases}$$

and in the $-$ case

$$A = \begin{cases} Z_2 \times Z_2 & \frac{n}{4} (q - 1) \text{ even} \\ D_8 & \frac{n}{4} (q - 1) \text{ odd} \end{cases}$$

Hence Table 13.2 gives the structure of $A$, for each quasisimple classical group.

Using Table 13.2, we can immediately deduce the normaliser in $GL_n(q^*)$ of most quasisimple classical groups.

**Theorem 13.3.2.** Let $G$ contain a quasisimple classical group $C$, in its natural representation, as a normal subgroup. Then

1. $N_{GL_n(q^*)}(G) \leq N_{GL_n(q^*)}(C)$.  

151
Table 13.2: $N_{GL_n(q^u)}(C) = F_{q^u}^\ast.C.A$ for quasisimple classical group $C$

<table>
<thead>
<tr>
<th>$C$</th>
<th>Conditions</th>
<th>$A$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$SL_n(q)$</td>
<td>$n &gt; 1$</td>
<td>$Z_{(n,q-1)}$</td>
</tr>
<tr>
<td>$Sp_{2m}(q)$</td>
<td>$q$ even</td>
<td>$1$</td>
</tr>
<tr>
<td>$SU_n(q)$</td>
<td>$q$ odd</td>
<td>$Z_2$</td>
</tr>
<tr>
<td>$Ω_{2m+1}^\pm(q)$</td>
<td>$m &gt; 0$ and $q$ odd</td>
<td>$Z_2$</td>
</tr>
<tr>
<td>$Ω_{2m}^\pm(q)$</td>
<td>$q$ even</td>
<td>$Z_2 \times Z_2$</td>
</tr>
<tr>
<td>$Ω_{2m}^\pm(q)$</td>
<td>$q$ odd and $\frac{q}{4}(q-1)$ odd</td>
<td>$D_8$</td>
</tr>
<tr>
<td>$Ω_{2m}^\pm(q)$</td>
<td>$q$ odd and $\frac{q}{4}(q-1)$ even</td>
<td>$Z_2 \times Z_2$</td>
</tr>
</tbody>
</table>

2. Assume $C$ is not an orthogonal group of even dimension and odd characteristic. Then $N_{GL_n(q^u)}(G) = N_{GL_n(q^u)}(C)$. 

**Proof.** Let $N_{GL_n(q^u)}(C) = F_{q^u}^\ast.C.A$, as before.

1. From Theorem 13.3.1, the group $A$ is either abelian or is $D_8$. Hence \( C/Z(C) \) is the only non-abelian simple factor of $G/Z(C)$. The group $C$ is characteristic in $G$, so any $x \in GL_n(q)$ which fixes $G$ under conjugation also fixes $C$ under conjugation; hence $N_{GL_n(q^u)}(G) \leq N_{GL_n(q^u)}(C)$.

2. Assume $C$ is not an orthogonal group of even dimension and odd characteristic. Let $x \in N_{GL_n(q^u)}(C)$ and $g \in G$. Then

\[
(Cx^{-1})(Cg)(Cx) = Cg,
\]

since $G \leq N_{GL_n(q^u)}(C)$ and $N_{GL_n(q^u)}(C)/C$ is abelian, by Theorem 13.3.1. So $x^{-1}gx = cg$ for some $c \in C$, and hence $x^{-1}Gx \leq G$. In other words, $N_{GL_n(q^u)}(C) \leq N_{GL_n(q^u)}(G)$.

Now we consider the excluded case.

**Theorem 13.3.3.** Let $C = Ω_{2m}^\pm(q)$ with $q$ odd and let $C \leq G \leq N_{GL_n(q)}(C)$. Then $CO_{2m}^\pm(q)$ is an overgroup for $N_{GL_n(q)}(G)$.

**Proof.** The normaliser $N_{GL_n(q)}(G) \leq N_{GL_n(q)}(C)$, by Lemma 13.3.2 and $N_{GL_n(q)}(C) = CO_{2m}^\pm(q)$ by Lemma 13.2.3. This group is smaller than $GL_n(q)$, so is an overgroup for $N_{GL_n(q)}(G)$.
We have described how to find an overgroup for $N_{\text{GL}_n(q^u)}(G)$, where $G \in C_8$. Usually this overgroup is the normaliser itself, unless $G$ is an orthogonal group, $n$ is even and $q$ is odd. In the next section we consider a class of groups which is related to $C_8$, and explain how to find an overgroup for the normaliser of certain groups in this class.

13.4 Class $C'_8$

**Definition 13.4.1.** Class $C'_8$ consists of all absolutely irreducible groups which preserve a non-degenerate, non-trivial classical form.

Recall that $u := 2$ in the unitary case, and $u := 1$ otherwise. Let $G \leq \text{GL}_n(q^u)$ be an absolutely irreducible group preserving a non-degenerate classical form $f$. Then $G$ is contained in one of $\{\text{Sp}_n(q), \text{GU}_n(q), \text{GO}^\epsilon_n(q)\}$, where $\epsilon \in \{\circ, +, -\}$. If $G$ contains the quasisimple classical group associated with $f$ then $G \in C_8$ and we apply the method of the previous section, so suppose $G \in C'_8 \setminus C_8$.

**Theorem 13.4.2.** Let $G \leq \text{GL}_n(q^u)$ be in the class $C'_8$, preserving a form $f$, and let $n > 2$ if $f$ is symplectic or unitary. Then an overgroup for $N_{\text{GL}_n(q^u)}(G)$ is one of the following.

$$R = \begin{cases} 
\text{CSp}_n(q) & \text{if } G \leq \text{Sp}_n(q), \\
\text{CU}_n(q) & \text{if } G \leq \text{GU}_n(q), \\
\text{CO}^\epsilon_n(q) & \text{if } G \leq \text{GO}^\epsilon_n(q).
\end{cases}$$

**Proof.** By Lemma 13.2.2, the group $N_{\text{GL}_n(q^u)}(G)$ preserves $f$ up to scalar multiplication. Let $R$ be the group above associated with $f$, then $R \geq N_{\text{GL}_n(q^u)}(G)$, by Lemma 13.2.3. The group $R$ is smaller than $\text{GL}_n(q^u)$ and hence $R$ is an overgroup for $N_{\text{GL}_n(q^u)}(G)$. \hfill $\Box$

Note that we exclude the linear case here, since the associated group $R$ of a linear group $G$ is $\text{GL}_n(q)$ itself and thus not an overgroup for $N_{\text{GL}_n(q^u)}(G)$.

13.5 The algorithm: NormaliserClassical

The MAGMA functions we use are based on algorithms presented in [11], [12], [13], [52], [53], [54], [55] and [58].

Let $G \leq \text{GL}_n(q^u)$ be in the union of classes $C_8$ and $C'_8$. We present the algorithm `NormaliserClassical`, which takes as input $G$, a record `class_form` and a boolean `contains_QS`. The record `class_form` is the result of `ClassicalForms(G; Scalars:=true)`. It contains the string "type" indicating the type of form preserved by $G$ (possibly up to scalars) as well as a matrix $f$ of the form, if "type" does not equal "linear". The boolean `contains_QS` is the result of `RecogniseClassical(G)`, as defined on page
150, and for the purposes of this algorithm this determines whether $G$ contains $\text{SL}_n(q)$, $\text{Sp}_n(q)$, $\text{SU}_n(q)$ or $\Omega'_n(q)$, where $\epsilon \in \{\circ, +, -\}$.

The function $\text{NormaliserClassical}$ returns an overgroup $R$, such that $\text{N}_{GL_n(q^u)}(G) \leq R$, and a boolean $\text{full\_norm}$, which indicates whether $R = \text{N}_{GL_n(q^u)}(G)$.

### 13.5.1 NormaliserClassical in NormaliserGL

Note the positioning of $\text{NormaliserClassical}$ in $\text{NormaliserGL}$. If $G$ is a $C_8$-group then we can write down an overgroup $R$ for $\text{N}_{GL_n(q^u)}(G)$ immediately, and in most cases $R = \text{N}_{GL_n(q^u)}(G)$. Hence $\text{RecogniseClassical}$ is run early in $\text{NormaliserGL}$.

$\text{NormaliserClassical}$ is also used later in $\text{NormaliserGL}$, once $G$ has been identified as absolutely irreducible and $\text{ClassicalForms}$ has determined that $G$ preserves a classical form absolutely; hence $G \in C'_8$.

**Lemma 13.5.1.** If $G$ preserves a sesquilinear classical form $f$ or a quadratic form $Q$, up to scalars, then $G'$ preserves the form absolutely.

**Proof.** We use the usual commutator notation $[g, h] := g^{-1}h^{-1}gh$. Let $v, w \in V$, and suppose for all $g \in G$ there exists $\lambda_g \in \mathbb{F}_{q^u}^*$ such that $(vg, wg)f = \lambda_g(v, w)f$, or $(vg)Q = \lambda_g(v)Q$. Note that $\lambda_{g^{-1}} = (\lambda_g)^{-1}$, then

\[
(v[g, h], w[g, h])f = (\lambda_g)^{-1}(\lambda_h)^{-1}\lambda_g\lambda_h(v, w)f
= (v, w)f
\]

or

\[
(v[g, h])Q = (\lambda_g)^{-1}(\lambda_h)^{-1}\lambda_g\lambda_h(v)Q
= (v)Q.
\]

Hence if $G$ preserves the form $f$ or $Q$ up to scalar multiplication, then $G'$ preserves the same form absolutely. $\square$

We try to obtain an overgroup $R$ for $\text{N}_{GL_n(q^u)}(G')$ using the function $\text{NormaliserGL}(G'; \text{Overgroup}: = \text{true})$. If $G$ is not perfect, $G'$ has non-scalar elements and $G'$ is absolutely irreducible, then $G' \in C'_8$ and we would expect to find an overgroup for $\text{N}_{GL_n(q^u)}(G')$ by Step 11 of a call to $\text{NormaliserGL}(G')$, at the latest. If $G'$ is not scalar, does not lie in the Problem case of $C_1$ and is not absolutely irreducible, then an overgroup for the normaliser in $\text{GL}_n(q^u)$ of $G'$ is calculated in Step 5 or Step 6 of the call to $\text{NormaliserGL}(G')$. Hence, by Lemma 8.2.2, $R$ is an overgroup for $\text{N}_{GL_n(q^u)}(G)$.

Now we present the algorithm $\text{NormaliserClassical}$. Let $C$ be the standard representation in MAGMA of $\text{SL}_n(q)$, $\text{Sp}_n(q)$, $\text{SU}_n(q)$ or $\Omega'_n(q)$, where $\epsilon \in \{\circ, +, -\}$, depending on "type".
Step 1. Use \texttt{TransformForm}(f,"type") to obtain a matrix \( \chi \) such that \( C \leq G^\chi \).

Step 2. Construct \( R := N_{\text{GL}_n(q^n)}(C) \), using the results of Section 13.3 and the algorithms of [27].

Step 3. If \texttt{contains_QS=TRUE}, then \( R^\chi - 1 \) is an overgroup for the normaliser \( N_{\text{GL}_n(q^n)}(G) \). Return the overgroup \( R^\chi - 1 \). If \( G \) is an orthogonal type group of even dimension, with \( q \) odd, then return \texttt{full_norm=FALSE}, otherwise return \texttt{full_norm=TRUE}.

Step 4. If \texttt{contains_QS=FALSE}, then \( G \in \mathcal{C}_8' \). Determine an overgroup \( R^\chi - 1 \) for \( N_{\text{GL}_n(q^n)}(G) \) using Theorem 13.4.2 and construct \( R \) using the algorithms of [27]. Return \( R^\chi - 1 \) and \texttt{full_norm=FALSE}.

This concludes our treatment of the \( \mathcal{C}_8 \) - and \( \mathcal{C}_8' \)-groups.

13.6 Timings

We now give timings data for computing the normaliser in \( \text{GL}_n(q) \) of a group lying in \( \mathcal{C}_8 \cup \mathcal{C}_8' \), using \texttt{NormaliserGL}. We make test groups belonging to \( \mathcal{C}_8 \) and to \( \mathcal{C}_8' \setminus \mathcal{C}_8 \) for each classical type, excluding the linear type groups for \( \mathcal{C}_8' \).

For the linear-type \( \mathcal{C}_8 \)-groups we compute a list \texttt{l-groups} of 20 subgroups as follows. Let \( Z \) be a random scalar matrix of \( \text{GL}_n(q) \) and let \( Y \) be a random element of \( \text{GL}_n(q) \). Construct \( G := \langle \text{SL}_n(q), Z \rangle^Y \) and add \( G \) to \texttt{l-groups}.

By Lemma 13.1.2, the group \( G \) is an absolutely irreducible classical group of linear type.

For the symplectic-type \( \mathcal{C}_8 \)-groups we let \( C := \text{Sp}_n(q) \) and compute a list \texttt{s-groups} of 20 subgroups as follows. Let \( Z \) be a random scalar matrix of \( \text{GL}_n(q) \) and let \( Y \) be a random element of \( \text{GL}_n(q) \). Construct \( G := \langle C, Z \rangle^Y \) and add \( G \) to \texttt{s-groups}. Repeat 10 times. By Lemma 13.1.2, the group \( G \) is an absolutely irreducible classical group of symplectic type. Then we let \( C := \text{CSp}_n(q) \) and compute a further 10 subgroups in the same way.

For the unitary-type \( \mathcal{C}_8 \)-groups we compute a list \texttt{u-groups} of 20 subgroups as follows. Let \( Z \) be a random scalar matrix of \( \text{GL}_n(q^2) \), let \( X \) be a random non-scalar element of \( \text{GU}_n(q^2) \), which is not contained in \( \text{SU}_n(q) \) and let \( Y \) be a random element of \( \text{GL}_n(q^2) \). Construct \( G := \langle \text{SU}_n(q), Z, X \rangle^Y \) and add \( G \) to \texttt{u-groups}. By Lemma 13.1.2, the group \( G \) is an absolutely irreducible classical group of unitary type.

For the orthogonal-type \( \mathcal{C}_8 \)-groups we compute a list \texttt{o-groups} of 20 subgroups as follows. Let \( \phi : \text{CO}_n^\epsilon(q) \rightarrow \text{CO}_n^\epsilon(q)/\Omega_n^\epsilon(q) \), let \( H \) be a random subgroup of \( \text{Im}(\phi) \) and for each \( H \) let \( K \) be its preimage in \( \text{CO}_n(q) \). Let
\( G := \langle K, Z \rangle^Y \), where \( Z \) is a random scalar matrix of \( \text{GL}_n(q) \) and \( Y \) is a random element of \( \text{GL}_n(q) \), and add \( G \) to \( \text{o-groups} \) if it is absolutely irreducible. By Lemma 13.1.2, the group \( G \) is an absolutely irreducible classical group of the same orthogonal type with exceptions in dimension 2.

For the \( C'_8 \setminus C_8 \)-groups of each non-linear classical type, we compute a list of up to 25 groups as follows. Let \( M \) be the associated conformal group and create a list \( \text{subs} \) of 5 subgroups generated by 2 random elements of \( M \), which are absolutely irreducible and do not contain \( \text{SL}_n(q) \), \( \text{Sp}_n(q) \), \( \text{SU}_n(q) \) or \( \Omega^n_\epsilon(q) \), for \( \epsilon \in \{\circ, +, -\} \). For each \( G \) in \( \text{subs} \), create a list of 5 subgroups generated by 2 random elements of \( G \) and keep those which are absolutely irreducible.

For several values of \( n \) and \( q \) we constructed a list \( \text{test} \) of groups in each of the ways above. For all \( G \) in \( \text{test} \) we timed the computation of the function \( \text{NormaliserGL}(G) \) and the mean of these times appears in bold font in the table below. In a new MAGMA session, we timed the computation of \( \text{Normaliser}(\text{GL}(n,q^u),G) \), for the same groups \( G \), and the mean of these times is given below its bold counterpart. A blank table cell indicates that creating test data for these values of \( n \) and \( q \) was too time consuming. When the number of groups tested is less than that stated in the caption, the number of trials is given in brackets in the relevant cell. All values are given to three decimal places. The entry > 100 indicates that for at least one \( G \) in \( \text{test} \) the computation of \( \text{Normaliser}(\text{GL}(n,q^u),G) \) took more than 100 seconds.

For each value of \( n \) and \( q \) which did not time out we checked that the groups returned by \( \text{NormaliserGL}(G) \) and \( \text{Normaliser}(\text{GL}(n,q^u),G) \) were the same. The test data includes classical groups of all possible types in both \( C_8 \) and \( C'_8 \).

<table>
<thead>
<tr>
<th>n</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>q=4</td>
<td>0.006</td>
<td>0.006</td>
<td>0.007</td>
<td>0.006</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.016</td>
<td>0.200</td>
<td>23.191</td>
<td>&gt; 100</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0.005</td>
<td>0.005</td>
<td>0.006</td>
<td>0.006</td>
<td>0.006</td>
</tr>
<tr>
<td></td>
<td>0.085</td>
<td>2.360</td>
<td>30.439</td>
<td>&gt; 100</td>
<td>&gt; 100</td>
</tr>
<tr>
<td>7</td>
<td>0.005</td>
<td>0.006</td>
<td>0.006</td>
<td>0.006</td>
<td>0.007</td>
</tr>
<tr>
<td></td>
<td>0.547</td>
<td>&gt; 100</td>
<td>&gt; 100</td>
<td>&gt; 100</td>
<td>&gt; 100</td>
</tr>
</tbody>
</table>
Table 13.4: Time to compute $N_{\text{GL}_n(q)}(G)$, for $G \in C_8$ containing $\text{Sp}_n(q)$ (20 trials)

<table>
<thead>
<tr>
<th>$n$</th>
<th>4</th>
<th>6</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>$q=4$</td>
<td>0.020</td>
<td>0.009</td>
<td>0.010</td>
</tr>
<tr>
<td></td>
<td>0.018</td>
<td>4.024</td>
<td>&gt; 100</td>
</tr>
<tr>
<td>5</td>
<td>0.009</td>
<td>0.008</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.052</td>
<td>&gt; 100</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0.010</td>
<td>0.008</td>
<td>0.004</td>
</tr>
<tr>
<td></td>
<td>0.308</td>
<td>&gt; 100</td>
<td>&gt; 100</td>
</tr>
<tr>
<td>8</td>
<td>0.122</td>
<td>0.009</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.905</td>
<td>&gt; 100</td>
<td></td>
</tr>
</tbody>
</table>

Table 13.5: Time to compute $N_{\text{GL}_n(q)}(G)$, for $G \in C_8$ containing $\text{SU}_n(q)$ (20 trials)

<table>
<thead>
<tr>
<th>$n$</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>$q=2$</td>
<td>0.010</td>
<td>0.012</td>
<td>0.012</td>
</tr>
<tr>
<td></td>
<td>0.009</td>
<td>0.042</td>
<td>0.443</td>
</tr>
<tr>
<td>3</td>
<td>0.013</td>
<td>0.010</td>
<td>0.015</td>
</tr>
<tr>
<td></td>
<td>0.222</td>
<td>12.630</td>
<td>&gt;100</td>
</tr>
<tr>
<td>4</td>
<td>0.012</td>
<td>0.010</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6.369</td>
<td>0.045</td>
<td></td>
</tr>
</tbody>
</table>

Table 13.6: Time to compute $N_{\text{GL}_n(q)}(G)$, for $G \in C_8$ containing $\Omega_n(q)$ (20 trials)

<table>
<thead>
<tr>
<th>$n$</th>
<th>3</th>
<th>5</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>$q=5$</td>
<td>0.010</td>
<td>0.011</td>
<td>0.008</td>
</tr>
<tr>
<td></td>
<td>0.004</td>
<td>0.104</td>
<td>26.604</td>
</tr>
<tr>
<td>7</td>
<td>0.010</td>
<td>0.011</td>
<td>0.008</td>
</tr>
<tr>
<td></td>
<td>0.006</td>
<td>0.773</td>
<td>&gt; 100</td>
</tr>
<tr>
<td>9</td>
<td>0.012</td>
<td>0.013</td>
<td>0.009</td>
</tr>
<tr>
<td></td>
<td>0.008</td>
<td>3.954</td>
<td>&gt; 100</td>
</tr>
</tbody>
</table>
Table 13.7: Time to compute \( \text{N}_{\text{GL}_n(q)}(G) \), for \( G \in C_8 \) containing \( \Omega^+_n(q) \) (20 trials)

<table>
<thead>
<tr>
<th>n</th>
<th>4</th>
<th>6</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>q=4</td>
<td>0.015</td>
<td>0.013</td>
<td>0.020</td>
</tr>
<tr>
<td></td>
<td>0.008</td>
<td>0.308</td>
<td>48.871</td>
</tr>
<tr>
<td>5</td>
<td>0.009</td>
<td>0.010</td>
<td>0.012</td>
</tr>
<tr>
<td></td>
<td>0.016</td>
<td>2.095</td>
<td>&gt; 100</td>
</tr>
<tr>
<td>7</td>
<td>0.017</td>
<td>0.011</td>
<td>0.018</td>
</tr>
<tr>
<td></td>
<td>0.043</td>
<td>20.648</td>
<td>&gt; 100</td>
</tr>
</tbody>
</table>

Table 13.8: Time to compute \( \text{N}_{\text{GL}_n(q)}(G) \), for \( G \in C_8 \) containing \( \Omega^-_n(q) \) (20 trials)

<table>
<thead>
<tr>
<th>n</th>
<th>4</th>
<th>6</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>q=4</td>
<td>0.012</td>
<td>0.012</td>
<td>0.015</td>
</tr>
<tr>
<td></td>
<td>0.008</td>
<td>0.398</td>
<td>&gt; 100</td>
</tr>
<tr>
<td>5</td>
<td>0.009</td>
<td>0.009</td>
<td>0.010</td>
</tr>
<tr>
<td></td>
<td>0.017</td>
<td>2.037</td>
<td>&gt; 100</td>
</tr>
<tr>
<td>7</td>
<td>0.009</td>
<td>0.009</td>
<td>0.011</td>
</tr>
<tr>
<td></td>
<td>0.049</td>
<td>36.228</td>
<td>&gt; 100</td>
</tr>
</tbody>
</table>

Table 13.9: Time to compute \( \text{N}_{\text{GL}_n(q)}(G) \), for \( G \in C_8' \) preserving a symplectic form (25 trials)

<table>
<thead>
<tr>
<th>n</th>
<th>4</th>
<th>6</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>q=4</td>
<td>0.014</td>
<td>0.055</td>
<td>0.008</td>
</tr>
<tr>
<td></td>
<td>0.017</td>
<td>3.265</td>
<td>&gt; 100</td>
</tr>
<tr>
<td>5</td>
<td>0.020 (20)</td>
<td>0.006</td>
<td>0.007</td>
</tr>
<tr>
<td></td>
<td>0.026</td>
<td>60.241</td>
<td>&gt; 100</td>
</tr>
<tr>
<td>7</td>
<td>0.007</td>
<td>0.008</td>
<td>&gt; 100</td>
</tr>
<tr>
<td>8</td>
<td>0.008</td>
<td>&gt; 100</td>
<td></td>
</tr>
</tbody>
</table>
Table 13.10: Time to compute $N_{GL_n(q)}(G)$, for $G \in C'_8$ preserving a unitary form (25 trials)

<table>
<thead>
<tr>
<th>n</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>q=2</td>
<td>0.021 (14)</td>
<td>0.027 (18)</td>
</tr>
<tr>
<td></td>
<td>0.006</td>
<td>0.017</td>
</tr>
<tr>
<td>3</td>
<td>0.022</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.102</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0.178</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.316</td>
<td></td>
</tr>
</tbody>
</table>

Table 13.11: Time to compute $N_{GL_n(q)}(G)$, for $G \in C'_8$ preserving an orthogonal form in odd dimension (25 trials)

<table>
<thead>
<tr>
<th>n</th>
<th>5</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>q=3</td>
<td>0.019 (20)</td>
<td>0.013</td>
</tr>
<tr>
<td></td>
<td>0.010</td>
<td>0.132</td>
</tr>
<tr>
<td>5</td>
<td>0.048 (19)</td>
<td>0.007</td>
</tr>
<tr>
<td></td>
<td>0.029</td>
<td>16.188</td>
</tr>
</tbody>
</table>

Table 13.12: Time to compute $N_{GL_n(q)}(G)$, for $G \in C'_8$ preserving an orthogonal plus form (25 trials)

<table>
<thead>
<tr>
<th>n</th>
<th>4</th>
<th>6</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>q=4</td>
<td></td>
<td>0.013 (15)</td>
<td>0.019</td>
</tr>
<tr>
<td></td>
<td>0.296</td>
<td></td>
<td>25.703</td>
</tr>
<tr>
<td>5</td>
<td>0.033 (15)</td>
<td>0.010</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.015</td>
<td>2.124</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0.046 (5)</td>
<td>0.012</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.050</td>
<td>&gt; 100</td>
<td></td>
</tr>
</tbody>
</table>

159
Table 13.13: Time to compute $N_{\text{GL}_n(q)}(G)$, for $G \in C'_8$ preserving an orthogonal minus form (25 trials)

<table>
<thead>
<tr>
<th>q=4</th>
<th>4</th>
<th>6</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.020 (5)</td>
<td>0.014</td>
<td>0.357</td>
</tr>
<tr>
<td>5</td>
<td>0.033</td>
<td>0.011 (15)</td>
<td>0.011</td>
</tr>
<tr>
<td>7</td>
<td>0.027 (11)</td>
<td>0.010 (20)</td>
<td>0.011</td>
</tr>
</tbody>
</table>
Chapter 14

Future work

The algorithm NormaliserGL described here will be added to MAGMA for general use. The attached disc gives some example groups $G$, which the reader can use to compare the efficiency of our algorithm NormaliserGL($G$) with MAGMA’s existing algorithm Normaliser(GL($n$, $q$), $G$). Note that this algorithm was developed in MAGMA V2.14-12.

The ultimate goal is to complete this project by extending the algorithm to include the missing Aschbacher classes $\{C_4, C_6, C_7, C_9\}$. Of course, some groups in these classes are already covered. For example, $C_9$-groups which preserve non-degenerate classical forms, or $C_4$-groups that also lie in $C_2 \cup C_3$. We now give some specific suggestions for future work in this area.

14.1 $C_6$: Extraspecial normalisers

Recall the definition of an extraspecial group from Section 1.6. The following theorem could be implemented to find an overgroup for $N_{\text{GL}}(q)(G)$, for some groups $G \in C_6$.

**Theorem 14.1.1.** Let $G$ be a $C_6$-group which normalises precisely one extraspecial group $S := s^{1+2m}$. Then $N_{\text{GL}}(q)(G) \leq N_{\text{GL}}(q)(S)$.

**Proof.** The subgroup $S$ is characteristic in $G$, so the result follows from Lemma 8.2.1. \qed

Now suppose that $G$ normalises precisely two extraspecial subgroups, $S_1$ and $S_2$, of the same order and exponent. Then these groups are conjugate in $\text{GL}_n(q)$.

**Conjecture 14.1.2.** Let $G$, $S_1$ and $S_2$ be as above and let $N(S_i) := N_{\text{GL}}(q)(S_i)$. Then either $N_{\text{GL}}(q)(G) \leq N(S_i)$ or else there exists an element $y \in N_{\text{GL}}(q)(G)$ such that $S_1^y = S_2$ and the group $R := \langle N_{N(S_1)}(G), y \rangle$ is an overgroup for $N_{\text{GL}}(q)(G)$.  

161
In order to obtain an element \( y \in N_{GL_n}(G) \) which conjugates the \( S_i \), we could use a method similar to that used for class \( C_2 \) in Chapter 10.

14.2 \( C_1 \): Further recursion

Let \( M_{k,l}(q) \) denote the set of all \((k \times l)\)-dimensional matrices with entries in \( \mathbb{F}_q \). Suppose \( G \) is reducible but not completely reducible. Then there exists \( \chi \in GL_n(q) \) such that, for all \( g \in G \)

\[
\chi^{-1}g\chi = \begin{pmatrix} A & 0 \\ X & B \end{pmatrix},
\]

where \( A \in GL_{n_1}(q) \), \( B \in GL_{n_2}(q) \), \( X \in M_{n_2,n_1}(q) \) and \( n_1 + n_2 = n \).

**Conjecture 14.2.1.** Let \( M \) be the group generated by all matrices of the form \( \begin{pmatrix} A & 0 \\ X & B \end{pmatrix} \), where \( A \in N_{GL_{n_1}(q)}(A) \), \( B \in N_{GL_{n_2}(q)}(B) \), and \( X \in M_{n_2,n_1}(q) \). Then \( M \) is an overgroup for \( N_{GL_n}(G)^\chi \).

14.3 Characteristic subgroups

Lemma 8.2.1 states that \( N_{GL_n}(G) \leq N_{GL_n}(H) \), for any characteristic subgroup \( H \) of \( G \). This technique could be applied to other easily calculated characteristic subgroups of \( G \), such as the following.

**Lemma 14.3.1.** Let \( G \) be a non-scalar nilpotent group and suppose

\[
|G| = p_1^{m_1}p_2^{m_2} \ldots p_t^{m_t},
\]

where each \( p_i \) is prime, \( t > 1 \) and \( m_i > 1 \), for at least one \( 1 \leq i \leq t \). Then there is a Sylow subgroup \( S < G \), for which \( N_{GL_n}(G) \leq N_{GL_n}(S) < GL_n(q) \).

**Proof.** A nilpotent group can be written as a direct product of its Sylow subgroups. By the nature of \( G \) described above, there exists a proper, non-trivial, non-cyclic Sylow subgroup \( S \) of \( G \). Each Sylow subgroup is characteristic in \( G \) and hence \( N_{GL_n}(G) \leq N_{GL_n}(S) \), by Lemma 8.2.1.

Hence, with \( S \) and \( G \) defined as above, \( N_{GL_n}(S) \) is an overgroup for \( N_{GL_n}(G) \), provided that \( N_{GL_n}(S) < GL_n(q) \).
14.4 Future work

Further work on this topic could include studying normalisers of matrix groups $G \leq \GL_n(q)$ belonging to the Aschbacher classes $\mathcal{C}_4$, $\mathcal{C}_6$, $\mathcal{C}_7$ and $\mathcal{C}_9$ and finding overgroups for them. For most of the Aschbacher classes we have dealt with, there are some groups $G$ in the class for which the algorithm $\Normaliser\GL$ fails and we ultimately default to Magma’s original function. Our algorithm would be improved by finding overgroups for the normalisers of all subgroups in each Aschbacher class. Some examples are as follows.

We could examine the properties of normalisers of $\mathcal{C}_2$-groups which preserve three or more systems of imprimitivity and of $\mathcal{C}_3$-groups which embed in the semilinear group in more than one way. In particular, we would like to find an overgroup for $\NGL_n(q)(G)$, where $G$ is a reducible group lying in the Problem case of Subsection 9.2.3.

Another direction for future work could be computing overgroups for $\NX(G)$, where $X \in \{\Sp_n(q), \GU_n(q), \GOO_n(q), \GO^\pm_n(q)\}$ and $G \leq X$. A suggested method is to use the versions of Aschbacher’s theorem associated with each of the classical types and proceed similarly.
Bibliography


167


