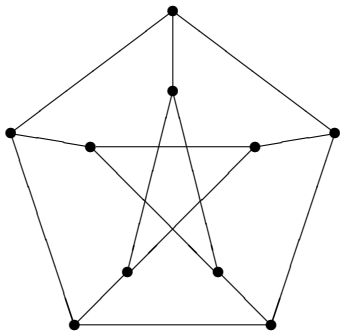
On the Symmetric Generation of Finite Groups

by

Benjamin Thomas Fairbairn

A thesis submitted to
The University of Birmingham
for the degree of
Doctor of Philosophy



School of Mathematics
The University of Birmingham
November 2008

Abstract

In this thesis we discuss some uses and applications of the techniques in Symmetric generation.

In Chapter 1 we introduce the notions of symmetric generation.

In Chapter 2 we discuss symmetric presentations defined by symmetric generating sets that are preserved by a group acting on them transitively but imprimitively.

In Chapter 3 our attention turns to Coxeter groups. We show how the Coxeter-Moser presentations traditionally associated with the families of finite Coxeter groups of types A_n, D_n and E_n (ie the "simply laced" Coxeter groups) may be interpreted as symmetric presentations and as such may be naturally arrived at by elementary means.

In Chapter 4 we classify the irreducible monomial representations of the groups $L_2(q)$ and use these to define symmetric generating sets of various groups.

Synopsis

Mathematicians' capture the idea of symmetry with the concept of a 'group' and since symmetry is an increasingly ubiquitous concept not only throughout mathematics, but also in the physical sciences and beyond, the importance of the problem of understanding groups is more pressing than ever.

An important class of groups are the finite groups. Just as numbers may be broken down into prime numbers that cannot be broken down further, the celebrated theorem of Jordan and Hölder tells us that finite groups may be broken down into 'simple groups' that cannot be broken down further. One of the grandest research projects in history was the Classification of the Finite Simple Groups involving an enormous international effort involving hundreds of mathematicians. Despite the proof of this grand theorem having been completed nearly 30 years ago, it remains poorly understood and is still intensely studied by a large number of mathematicians across the globe.

In this thesis we discuss one approach to studying groups that lends itself particularly well to the study of finite simple groups.

Let G be a group and let $T \subset G$ be a generating set for G. Let $H \leqslant G$ be the largest subgroup of G that acts on T by conjugation. For most generating sets H will be trivial. Sometimes, however, H can act transitively so that in some sense all the elements of T 'look the same' and the action of H endows T with an underlying combinatorial structure. Turning this idea on its head, we can ask what possibilities there are for G given a group

H and running on the assumptions that $H \leqslant G$ and that H acts transitively on some generating set for G. Several general results can restrict the structure of G under these circumstances and in particular these techniques of 'symmetric generation' can be used to produce elementary constructions of various interesting groups. In this thesis we shall discuss a variety of aspects of this general approach.

In Chapter 1 we give the basic definitions associated with symmetric generation and define the notation that shall be used throughout this thesis. In particular, we shall state several of the general lemmata alluded to above. We proceed to describe the main theorems of the remaining chapters using the notation that is defined in Chapter 1.

Several of the General lemmata used in defining symmetric generating sets require that the action of H on T is primitive however interesting symmetric presentations may be obtained using imprimitive actions too. In Chapter 2 we discuss symmetric generating sets defined by imprimitive actions. More specifically, we prove the following theorem.

Theorem A Consider the factored progenitor

$$\frac{2^{\star 6} : \mathrm{D}_{12}}{(26)(35)t_1t_4}. \qquad (\diamondsuit\spadesuit)$$

(a) The only groups of the form $L_2(2^r).d$ that are homomorphic images of $(\diamondsuit\spadesuit)$ are the groups $L_2(2^{2r}).2$. In particular, the groups $L_2(2^r)$ are never images of $(\diamondsuit\spadesuit)$.

(b) No group of the form $L_2(3^r).d$ is a homomorphic image of $(\diamondsuit\spadesuit)$.

(c) Let $p \geqslant 5$ be a prime and

$$G := \begin{cases} PSL_2(p) & \mathrm{p} \equiv \pm 1 \pmod{24}; \\ PGL_2(p) & \mathrm{p} \not\equiv \pm 1 \pmod{24}. \end{cases}$$

Then G is a homomorphic image of $(\diamondsuit\spadesuit)$.

We then proceed to discuss the special case of imprimitive actions defined using wreath products and their uses in extending symmetric generating sets of small groups to symmetric generating sets of large groups. More specifically we prove the following theorem.

Theorem B Let $r \geqslant 2$. (i) The group $(2^r + 1) \times L_2(2^r)$ (and therefore the group $L_2(2^r)$) is a homomorphic image of the progenitor $2^{\star(2^r+1)} : (2^r + 1)$.

(ii) The group $SU_3(2^r)$ (and therefore the group $U_3(2^r)$) is a homomorphic image of the progenitor $2^{\star((2r+1)+(2r+1))} : ((2^r+1) \wr 2)$. Furthermore the symmetric generators in a block of the action defining this progenitor along with the subgroup $(2^r + 1)^2 \leqslant (2^r + 1) \wr 2$ generate a maximal subgroup with structure $(2^r + 1) \times L_2(2^r)$ that stabilizes a non-isotropic vector in the module naturally acted by $SU_3(2^r)$ (and so any symmetric presentation of $SU_3(2^r)$ as an image of this progenitor may be given as a wreathed extension of a symmetric presentation given in part (i)).

In Chapter 3 our attention turns to an important class of groups known as reflection groups. In particular we show how the techniques of symmetric generation may be employed to arrive at the presentations most naturally associated with some of the more interesting members of this important class of groups without a priori knowledge of them. More specifically we prove the following theorem.

Theorem C Let S_n be the symmetric group acting on n objects and $W(\Phi)$ denote the Weyl group of the root system Φ. Then:

1.

$$\frac{2^{\star\binom{n}{1}} : S_n}{(t_1(1,2))^3} \cong W(A_n)$$

2.

$$\frac{2^{\star\binom{n}{2}} : S_n}{(t_{12}(2,3))^3} \cong W(D_n) \text{ for } n \geqslant 4$$

3.

$$\frac{2^{\star\binom{n}{3}} : S_n}{(t_{123}(3,4))^3} \cong W(E_n) \text{ for } n = 6, 7, 8.$$

We go on to use this theorem to motivate an investigation of symmetric presentations closely related to those given in Theorem C. Most notably we are naturally led to the following new presentation of the almost simple group M_{12}:2.

Theorem D

$$\frac{2^{\star\binom{5}{2}} : \mathrm{S}_5}{(t_{1,2}(2,3)(4,5))^5, (t_{1,2}t_{3,4})^2} \cong \mathrm{M}_{12} : 2$$

In our final chapter our attention turns to the special case in which the elements of T are not involutions, so that the action of H does not necessarily just permute the elements of T. These have been intensely studied before in several of the cases when H is a finite simple group. In this chapter we classify the 'monomial representations' that enable us to consider such actions of a very large class of finite simple groups. More specifically we prove the following theorem.

Theorem E The only irreducible monomial representations of the groups $L_2(q)$ are the following.

- Any linear representation;
- Any representation of $\mathrm{L}_2(2)$ all of which are writable over $\mathbb{Q}$;
- Any representation of $\mathrm{L}_2(3)$, the non-trivial linear representations being writable over $\mathbb{Q}(\zeta_4)$ and the 3 dimensional representation being writable over $\mathbb{Q}$;

- The 7 dimensional representation of $\mathrm{L}_2(7)$, writable over $\mathbb{Q}$;
- Any irreducible $q+1$ dimensional representation of $L_2(q)$, writable over $\mathbb{Q}(\zeta_d)$ where d is some divisor of $q-1$ depending on the representation.

We go on to sketch the proofs of analogous results for various groups closely related to those considered in the above Theorem E. We then go on to use these representations to exhibit new symmetric generating sets of a variety of finite groups.

"With regard to errors in general, whether falling under the denomination of mental, typographical, or accidental, we are conscious of being able to point to a greater number than any critic whatsoever. Men who are acquainted with the innumerable difficulties attending the execution of a work of such an extensive nature will make proper allowances. To these we appeal, and shall rest satisfied with the judgment they pronounce."

From the 'Atlas of finite groups'
citing the preface to the first edition
of the Encyclopedia Britanica, 1771

Acknowledgements

First and foremost I am deeply indebted to my PhD supervisor Professor Robert Turner Curtis for his continued support and guidance over the past three and a half years as well as introducing me to the beautiful ideas and concepts that appear in this thesis.

Cheers EPSRC for cash!

Now, the full list of friends, family, tiddlywinks players and ever-tolerant office-mates is far too long to give here despite my gratitude to them all for the ongoing encouragement, support, cake and beer. A special mention goes to the following individuals: Professor Chris Parker for continuing advice, support and guidance throughout my time in Birmingham; Dr John Bray for advice on using the invaluable 'Double Coset Enumerator', particularly during the more embryonic stages of this undertaking; Dr Kay Magaard for invaluable discussions concerning his recent work with Professor Gerhard Hiss relevant to Chapter 4; Professor Rob Wilson for paper writing tips, job references and general mathematical discussions; Dr David Craven for his comments regarding the contents of paragraph five on page 63; Dr Jürgen Müller for his comments regarding the content of Chapter 3 and the subsequent papers(s) that came from it; my examiners Dr Ralf Gramlich and Dr John Humphreys for their many helpful comments and suggested amendments to this thesis and finally I wish to thank Professor Richard Weiss for enlightening mathematical discussions and his many job references.

Contents

Chapter 1

Introduction

1.1 The Finite Simple Groups

One of the crowning glories of (late) 20^{th} century mathematics was the Classification of Finite Simple Groups. Roughly this states that every finite simple group is one of

- The cyclic groups of prime order;
- The alternating groups, A_n with $n \geqslant 5$;
- The groups of Lie type or;
- The 26 'sporadic' groups.

The statement of this Theorem alone is extremely complex and many of the objects appearing in the statement are hard to define. This is made particularly difficult by the fact that the finite simple groups differ so wildly in their nature. Some are most naturally viewed as permutation groups (such as the alternating groups and the Mathieu sporadic groups); some are naturally viewed as matrix groups (the handful of families of groups of Lie type arising as classical groups) whilst some appear to admit no straightforward description at all (the numerous families of 'exceptional' groups of Lie type and the larger

sporadic groups). Unsurprisingly, the only known proof of a theorem this complex is extremely long and complex, making it almost impossible to understand these objects (though there are notable efforts to 'revise' the original proof and there are several active attempts at producing alternative proofs). Since this Theorem has an ever growing number of applications to solving problems in a variety of areas of mathematics, the problem of understanding it is becoming increasingly important.

One common approach to understanding these groups is to exhibit some form of 'nice' generating sets for them. There have been several approaching along these lines produced. For instance, using Wilson's 'standard generators', many of which may be found on the online version of the ATLAS [62], we can easily identify when two copies of a group are the same, aiding our ability to compute with and thus understand many of these groups (see Wilson, [61], for further details).

In this thesis we shall discuss another form of 'nice' generating set first investigated by Curtis [22], namely generating sets endowed with an underlying combinatorial structure that is preserved by a non-trivial group of automorphisms called a 'symmetric generating set'. Several general Lemmata restricting the structure of such a generating set are known. Consequently, consideration of what such a generating set can look like often leads to extremely natural constructions of groups that can often be easily verified by hand. We proceed to describe the techniques of symmetric generation in more detail.

1.2 Symmetric Generation I: Involutory Generators

In this section we shall describe the techniques of involutory symmetric generation ie the special case of symmetric generation in which the elements in the symmetric generating set are involutions. The techniques of symmetric generation furnish constructions of some quite complex structures using the barest minimum of machinery. It also helps to 'explain' the existence of some exceptional objects, such as sporadic groups, in terms of

the slightly odd behaviour of much more down-to-Earth groups. Furthermore it becomes possible to relate the structure of the group as a whole to the combinatorial structure of the generating set - an object usually smaller and easier to describe. There are several reasons for wanting to give the definitions in this special case separately.

- This special case is sufficient for most of this thesis (more specifically the Chapters 2 and 3).
- All the definitions are substantially simpler in this case.
- This special case admits several general lemmata for restricting the structure of symmetric generating sets that do not hold more generally. We give many of these in Section 1.3.
- There are general lemmata suggesting that involutory symmetric generation is particularly well-suited to the study of finite simple groups, especially given that all non-abelian simple finite groups contain involutions by the Odd Order Theorem.

Throughout this thesis we shall use the standard ATLAS notation for groups as described in [19]. Furthermore we shall write $\mathbb{F}_q$ to denote the finite field containing q elements.

Let $2^{\star n}$ denote the free group generated by n involutions. We write $\{t_1, t_2, \ldots, t_n\}$ for a set of generators of this free product. A permutation $\pi \in S_n$ induces an automorphism of this free product $\widehat{\pi}$ by permuting its generators namely

$$t_i^{\widehat{\pi}} := \pi^{-1} t_i \pi = t_{\pi(i)}. \qquad (\diamondsuit)$$

Given a group $N \leqslant S_n$ we can use this action to form a semi-direct product $\mathcal{P} := 2^{\star n} : N$.

When N acts transitively we call $\mathcal{P}$ a *progenitor*. (Note that some of the early papers on symmetric generation insisted that N acts at least 2-transitively.) Elements of $\mathcal{P}$ can

all be written as a relator of the form the form πw where $\pi \in N$ and w is a word in the symmetric generators using ($\diamondsuit$). Consequently any finitely generated subgroup of $\mathcal{P}$ may be expressed as $H := \langle w_1\pi_1, \ldots, w_r\pi_r \rangle$ for some r. In particular, if we factor $\mathcal{P}$ by the normal closure of H we write

$$\frac{2^{\star n} : N}{w_1\pi_1, \ldots, w_r\pi_r} = G. \qquad (\spadesuit)$$

We say the progenitor $\mathcal{P}$ is factored by the relations $w_1\pi_1, \ldots, w_r\pi_r$. Whenever we write a relator $w\pi$ we shall tacitly be referring to the relation $w\pi = id$ thus we shall henceforth only refer to relations, when *senso stricto* we mean relators. We call G the *target group* of ($\spadesuit$) and the expression ($\spadesuit$) a *symmetric presentation* of G. Often these relations can be written in a more compact form by simply writing $(\pi w)^d$ for some positive integer d. It is the opinion of the author that no confusion should arise from calling both $t \in \mathcal{P}$ and its image in G a *symmetric generator*. Similarly no confusion should arise from calling both $N \leqslant \mathcal{P}$ and its image in G the *control group*. We define the *length* of the relation πw to be the number of symmetric generators in w.

Henceforth we shall slightly abuse notation in writing t_i both for a generator of $2^{\star n}$ and for its homomorphic image in G. Similarly we shall write N both for the control group in $\mathcal{P}$ and for the homomorphic image of N in G. Again, it is the opinion of the author that no confusion should arise from this.

Note that it is possible that the image of N in G is not faithful, particularly if N is soluble, as it will be on several occasions in this thesis. We shall only consider presentations in which the image of N is faithful in this thesis, thus in several places we will motivate avoiding factoring a progenitor $\mathcal{P}$ by a particular set of relations $\mathcal{R}$ by proving that the image of the control group in $\mathcal{P}/\mathcal{R}$ is not faithful.

We are immediately confronted with the question of how to decide if G is finite or not. To do this we resort to an enumeration of the cosets of N in G. Let $g \in G$. We have that $gN \subset NgN$. Consequently the number of double cosets of the form NwN in G will

usually be smaller than the number of single cosets of the form wN in G, where w is a word in the symmetric generators, making them much easier to enumerate. To do this we make the following definitions.

Let G be a group with a subgroup $H \leqslant G$ and let w be some coset representative for H in G. We define the *coset stabilizing subgroup* of H to be the subgroup of H defined by

$$H^{(w)} := \{\pi \in H | Hw\pi = Hw\}.$$

This is clearly a subgroup of H and there are $|H : H^{(w)}|$ right cosets of H in the double coset HwH. We can enumerate these cosets using procedures such as the celebrated Todd-Coxeter algorithm [58]. The sum of these numbers then gives the index of H in G. We can thus determine the order of G and in particular prove it is finite.

John Bray has written a double coset enumeration program for precisely this purpose [11]. We shall repeatedly make use of his program in this thesis and consequently we give a detailed description of its use in Section 1.4.

When performing a double coset enumeration by hand we shall write $[w]$ to denote the double coset NwN for some word in the symmetric generators w. Furthermore we shall write $[\star]$ for the double coset $[id]$ and similarly $N^{(\star)}(= N)$ for the coset stabilizing subgroup of this coset. Given two words in the symmetric generators w and w' we shall write $w \sim w'$ if $[w] = [w']$.

A notable application of involutory symmetric generation has been to provide a compact means of storing, transmitting and computing with elements of groups. For instance, in [23], Curtis provides a symmetric presentation of the sporadic group J_1 defining the group as a certain homomorphic image of the progenitor $2^{\star 11} : \mathrm{L}_2(11)$. Curtis and Hasan were subsequently able to use this expression to write programs giving the elements of J_1 in the form πw where $\pi \in \mathrm{L}_2(11) \leq \mathrm{S}_{11}$ is a permutation and w is a word in the symmetric generators of length at most 4 (see [30]). Their 'program B' used the relations obtained

when performing an enumeration of the double cosets of the form $\mathrm{L}_2(11)w\mathrm{L}_2(11)$ in J_1 to shorten long words of the symmetric generators giving words in the desired form. Elements of the group can thus be represented as a string of at most 11+4=15 symbols, and typically fewer, in way that is practical to use.

More recently, and perhaps more impressively, Curtis and the author have produced a similar program for the Conway group $\cdot 0$, a group substantially larger than J_1, in [29, 37]. Using a symmetric presentation of $\cdot 0$ due to Bray and Curtis [12] (described on page 18) we can represent elements of $\cdot 0$ as a string of at most 64 symbols and typically far fewer. This represents a considerable saving compared to representing an element of $\cdot 0$ as a permutation of 196560 symbols or as a 24×24 matrix (ie as a string of 24^2=576 symbols).

1.3 Some General Lemmata

The following Lemma, whilst easy to prove, turns out to be remarkably powerful in naturally leading us to relations that can define interesting symmetric presentations.

Lemma 1.1 (The Famous Lemma)

$$\langle t_i, t_j \rangle \cap N \leqslant C_N(Stab_N(i,j))$$

Here we have written $stab_N(i,j)$ to denote the pointwise stabilizer in N of the set $\{i,j\}$. This naturally extends to the case of $r \geqslant 3$ symmetric generators, so that in particular, if the stabilizer of i and j stabilizes further points then a word in the symmetric generators corresponding to all the points that are stabilized may be of interest.

Lemma 1.2 (The Extended Famous Lemma)

$$\langle t_{i_1}, \ldots, t_{i_r} \rangle \cap N \leqslant C_N(Stab_N(i_1, \ldots, i_r))$$

These two lemmata were first proved by Curtis in [22]. The first of these was later dubbed the 'Famous Lemma' by Bray in [8]. Consequently we shall henceforth only refer to the first of these as The 'Famous Lemma' and to the second as the 'Extended Famous Lemma'.

Several other general lemmata exist and are used to great effect in a variety of constructions. Whilst the above two lemmata tell us which elements of the control group to use when finding relations to factor a progenitor by, they give no indication of what form these words should take. To this end we give the following two lemmata.

Lemma 1.3 (The First Parity Lemma) Let $\mathcal{P} = 2^{\star n} : N$ be a progenitor in which the control group, N, is perfect. Then any homomorphic image of $\mathcal{P}$ is either perfect or possesses a perfect subgroup of index 2. If w is a word in the symmetric generators of odd length then the factored progenitor

$$\frac{2^{\star n} : N}{\pi w}$$

is perfect.

The proof of this lemma is given by Curtis in [28, Corollary 3.1].

The following lemma is another useful tool when determining the length of a natural relation to factor a given progenitor by. Whilst elementary in nature, it appears to have been explicitly stated and proved nowhere in the literature. We therefore give the complete proof of the lemma here.

Lemma 1.4 (The Second Parity Lemma) Let $\mathcal{P} = 2^{\star n} : N$ be a progenitor and let $id \neq \pi \in N$ be an involution such that $t_i^{\pi} = t_j$ or t_i. Let $w = w(t_i, t_j)$ be a word in the symmetric generators t_i and t_j. If the image of N in $\mathcal{P}/\pi w$ is faithful and the image $t_i \notin N$, then the length of w is odd if and only if $t_i^{\pi} = t_j$.

Proof. Suppose $t_i^\pi = t_j$ and that w has even length, then there exists an $r \in \mathbb{Z}^+$ such that $(t_i t_j)^r = \pi$. This is true if and only if $t_i(t_j t_i)^{r-1} = \pi t_j = t_i \pi$ which is true if and only if $(t_i t_j)^{r-1} = \pi$. Continuing inductively gives $id = \pi$. Similarly if w has odd length and $t_i^\pi = t_i$ then $t_j \in N$. □

Whilst these two lemmata are useful for determining the parity of the length of a relation to use, the actual length itself is still open. The following lemma tells us to avoid relations that are extremely short.

Lemma 1.5 (The Primitive Lemma) Let $G = \langle \mathcal{T} \rangle$, where $\mathcal{T} = \{t_0, \ldots, t_{n-1}\} \subseteq G$ is a set of involutions in G with $N = N_G(\mathcal{T})$ acting primitively on $\mathcal{T}$ by conjugation. (Thus G is a homomorphic image of the progenitor $2^{\star n} : N$.) If $t_0 t_i \in N$, $t_0 \notin N$ for some $i \neq 0$, then $|G| = 2|N|$.

The proof of this lemma may be found in Curtis [28, Lemma 3.4].

This lemma is often used when considering progenitors defined by primitive actions, and in particular is used to show that that the shortest 'interesting' relation a progenitor can be factored by is of length 3 or more. See for instance Curtis' strikingly natural construction of the sporadic Higman-Sims group in [24].

Finally we give some lemmata that help to explain why the techniques of symmetric generation are so well suited to furthering our understanding of the finite simple groups.

Lemma 1.6 If N is perfect and primitive, then $|\mathcal{P} : \mathcal{P}'|=2$ and $\mathcal{P}'' = \mathcal{P}'$.

Corollary 1.7 If N is perfect and primitive then any image of $\mathcal{P}$ possesses a perfect subgroup of index at most 2.

Lemma 1.8 Every finite simple group is an image of a progenitor of the form $2^{\star n} : N$.

For proofs of these three lemmata see Curtis [27, Section 2].

1.4 The Double Coset Enumerator

In Section 1.2 we noted that double coset enumeration is an important part of any study of symmetric generation. Bray and Curtis have produced a double coset enumeration program specially suited to this situation described in [11] in the MAGMA computer package [18]. The program uses an adaptation of the celebrated Todd-Coxeter algorithm first described in [58] and is an adaptation of an earlier program written by Sayed described in [53, Chapter 4] which worked well with relatively small groups, but could not be made to cope with groups of a larger index or rank [28, p.66]. (An account of the Todd-Coxeter algorithm more modern than [58] is given by Serres in [56, p.184].) Since we shall repeatedly make great use of this program in Chapters 2 and 3 we shall briefly describe how to use it here.

By way of example we shall illustrate its use by enumerating the double cosets of the form $\mathrm{L}_2(11)w\mathrm{L}_2(11)$ where w is a word in the symmetric generators for the (unpublished) symmetric presentation

$$\frac{2^{\star\binom{11}{2}} : \mathrm{L}_2(11)}{\pi_{2,3}t_{1,9}t_{4,8}t_{5,6}} \cong \mathrm{M}_{12} \qquad (\heartsuit)$$

discovered by the author. Here the progenitor is defined by the action of the group $\mathrm{L}_2(11)$ on the $\binom{11}{2} = 55$ pairs of points from a set of 11 points, $\pi_{2,3}$ denotes the permutation (2,3)(1,9)(4,8)(5,6)$\in \mathrm{L}_2(11)$ and $t_{1,2}$ denotes the double coset corresponding to the pair of points $\{1, 2\}$. (The reason for denoting this permutation $\pi_{2,3}$ centralizer of this permutation fixes the transposition (2,3) and transitively permutes the other three transpositions and for each pair of points there is a unique permutation in $\mathrm{L}_2(11)$ with this property.) For each of the 55 pairs of points there is a unique involution corresponding to that pair with this property). The symbol 'M_{12}' denotes the sporadic simple Mathieu group of order 95040. To verify this we shall use one of the degree 11 permutation representations given on the online ATLAS, [62]. We first define a copy of the control group acting in a

way that enables us to define the progenitor appearing in (♡).

```
/* www-ATLAS of Group Representations. L2(11) represented as
permutations on 11 points. */

G<x,y>:=PermutationGroup<11|\[ 1,10,4,3,9,7,6,8,5,2,11] ,\[
2,11,5,4,10,8,7,9,6,3,1]
>;
print "Group G is L2(11) < Sym(11)";

> s:=Stabilizer(G,{2,3});
> f,nn:=CosetAction(G,s);
```

Here we have defined the action our copy of $L_2(11)$, denoted `G`, on the cosets of the stabilizer of the pair of points $\{2,3\}$, denoted `s`, which is equivalent to the action of $L_2(11)$ on these pairs. The command `f,nn:=CosetAction(G,s)` makes the computer define `f` to be a homomorphism from our original copy of $L_2(11)$, acting on 11 points, to a copy that acts on the 55 pairs of points, denoted `nn`.

```
> T:=Transversal(G,s);
> for i in [1..#T] do
for> if {2,3}^T[i] eq {1,9} then
for|if> 1^f(T[i]);
for|if> end if;end for;
55
> for i in [1..#T] do
for> if {2,3}^T[i] eq {4,8} then
for|if> 1^f(T[i]);
for|if> end if; end for;
38
> for i in [1..#T] do
for> if {2,3}^T[i] eq {5,6} then
for|if> 1^f(T[i]);
for|if> end if; end for;
10
```

Here we have defined `T` to be a transversal for the cosets of `s` in `G`. The above code searches through this transversal for a permutation that sends the pair $\{2,3\}$, labeled '`1`'

by the computer, to the each of the pairs $\{1,9\}$, $\{4,8\}$ and $\{5,6\}$ labeled by the computer 55, 38 and 10 respectively.

```
> RR:=[<[55,38,10],f(G!(2,3)(4,8)(5,6)(1,9))>];
> CT:=DCEnum(nn,RR,nn:Print:=5,Grain:=100);

Index: 144 === Rank: 5 === Edges: 25 === Status: Early closed ===
Time: 3.870
```

Here we have entered the relation $\pi_{23}t_{1,9}t_{4,8}t_{5,6}$ into the machine as the sequence of symmetric generators followed by the permutation appearing in the relation. The symbol `CT` represents the output of the coset enumerator which is a sequence of various pieces of information related to the coset enumeration. In particular the program itself automatically tells us that the target group contains the image of our control group to index 144; that there are five double cosets in total; there are 25 distinct pairs of pairs of single cosets of the form $(wN, t_{i,j}wN)$, giving information on the Cayley graph corresponding to our symmetric generating set (we shall give no consideration to these graphs in this thesis); that the resulting group is finite (the numerator's status as '`Early closed`' tells us this) and that the machine took just 3·87 seconds to complete the enumeration. Other commonly used useful pieces information are as follows.

```
> CT[4];
[
    [],
    [ 1 ],
    [ 1, 5 ],
    [ 1, 23 ],
    [ 1, 5, 4 ]
]
> CT[7];
[ 1, 55, 66, 11, 11 ]
```

The fourth element of the output sequence, `CT[4]`, is a list of coset representatives for the double cosets themselves (again, the numbers are simply labels the computer has given to each of the symmetric generators). The seventh element of the output sequence, `CT[7]`, gives the indices of the coset stabilizing subgroups corresponding to these double cosets, so in particular we note that 1+55+66+11+11=144.

(We remark in passing that the above coset enumeration has verified that the target group obtained in the symmetric presentation (♡) contains the image of a copy of $L_2(11)$ to index 144 and therefore has order at most $144\times|L_2(11)|=95040$. To actually *prove* that the image is in fact M_{12} permutations generating a copy of M_{12} corresponding to the control group and the symmetric generators need to be found. It is straightforward to verify that that $t_{1,9} = (1,9)(2,3)(7,10)(11,12)$ and its conjugates under the action of the above copy of the control group will satisfy the additional relations. Combined with the above permutations generating $L_2(11)$ these generate a copy of M_{12}.)

1.5 Symmetric Generation II: Non-Involutory Generators

The cyclic group of order 2 has a trivial automorphism group. Consequently any control group in the involutory case has no choice but to simply permute the symmetric generators. Using groups that admit non-trivial outer automorphisms enables us to use more interesting actions and define more interesting progenitors. In this section we translate the basic definitions given in Section 1.2 to a more general setting and in particular we give definitions that are far more general than those appearing elsewhere in the literature. Several authors have found interesting symmetric presentations of groups by considering this more general setting. See for instance any of [8], [55], [63]. This more general situation will be the main subject of Chapter 4.

Let G be a group, and let $(A_i)_{i\in I}$ be a family of subgroups of G. Then G is said to

be the *free product* of the subgroups A_i if given any group H and any homomorphism $f_i\colon A_i \to H$ for each $i \in I$, there is a unique homomorphism $f\colon G \to H$ such that $f|_{A_i} = f_i$ for all $i \in I$. This may be shown to be well-defined and is unique upto isomorphism (see for instance Artin [3]).

In particular we shall consider the case where $A_i \cong A_j =: A$ for any i and j and I is finite. In this case we shall write $A^{\star n}$ where $n := |I|$ (so in particular if $A \cong 2$, then $A^{\star n}$ is the free group considered in Section 1.2).

If N is a permutation group that acts transitively on the collection $(A_i)_{i\in I}$ then we write $\mathcal{P} := A^{\star n} : N$ if the stabilizer of A_1 in N fixes all the elements of A_1, in other words if N simply permutes the A_is. If the stabilizer of A_1 in N does not fix all the elements of A_1 then we write $\mathcal{P} := A^{\star n} :_m N$ (the 'm' here standing for 'monomial' since it is monomial representations of the N that commonly allow us to define these progenitors). In either case we call $\mathcal{P}$ a *progenitor* and N the *control group* of $\mathcal{P}$. When we need to refer to progenitors of both kinds we shall write $A^{\star n} :_{(m)} N$.

Most commonly, A is taken to be a cyclic group of order greater than 2 (see for instance [9]), but more interesting groups can be used. For example, the sporadic Rudvalis group (a group that, at the time of writing, is not known to admit an elegant symmetric presentation) has been found by the author to be a homomorphic image of the progenitor $\mathrm{A}_5^{\star 1456}$:Suz(8) where A_5 denotes the alternating group of order 60; Suz(8) is the Suzuki group of order 29120 and the action defining the progenitor is the action of Suz(8) on the conjugates of the maximal subgroups isomorphic to 5:4. We shall meet several examples in Chapter 4 where the action defining the progenitor is not a permutation action of the control group and in particular we shall even meet examples where the symmetric generators are isomorphic to the Klein foursgroup 2^2.

The remaining definitions of Section 1.2 now carry through almost word for word, but we reiterate them here to emphasis the similarity.

We call elements of the generators of the group $A^{\star n}$ the *symmetric generators*. Elements of $\mathcal{P}$ can all be written in the form πw where $\pi \in N$ and w is a word in the symmetric generators. Consequently any finitely generated subgroup of $\mathcal{P}$ may be expressed as $H := \langle w_1\pi_1, \ldots, w_r\pi_r \rangle$ for some r where each w_i is a word in the symmetric generators and each π_i is an element of the control group. In particular if H is a normal subgroup of $\mathcal{P}$ then the factor group may be expressed as

$$\frac{A^{\star n} :_{(m)} N}{w_1\pi_1, \ldots, w_r\pi_r} := G. \qquad (\clubsuit)$$

We call G the *target group*. It is the opinion of the author that no confusion should arise from calling both an element $t \in A_i$ for some $i \in I$ and its image in G a symmetric generator.

Henceforth we shall slightly abuse notation by writing N both for the control group in $\mathcal{P}$ and for the homomorphic image of N in G.

Note that it is possible that the image of N in G is not faithful, particularly if N is soluble as it will be on several occasions in this thesis. We shall only consider presentations in which the image of N is faithful in this thesis.

The Double Coset Enumerator described in Section 1.4 can handle non-involutory symmetric generators, but it was written primarily with involutory symmetric generators in mind and in particular is much less efficient when the symmetric generators are non-involutory. Consequently we shall employ single coset enumeration when considering symmetric presentations defined by non-involutory symmetric generators. This is only made possible by the fact that the groups being considered are of relatively small size and thus the index of the control group in each case is sufficiently low for the number of single cosets to be not too great.

1.6 Conventional Presentations

Several authors have noted that symmetric presentations of the form (♠) and (♣) may be expressed as conventional presentations in terms of generators and relations. For instance see any of the accounts due to SW Bolt [6, p.8], JD Bradley [7, p.2], JN Bray [8, p.27], MS Mohammed [53, p.11], S Stanley [55, p.15] or S Whyte [63, p.8].

This is particularly straightforward in the involutory case. If the control group N has the presentation $\langle x_i | \mathcal{R} \rangle$ then this may be extended to the presentation for the progenitor $2^{\star n} : N$

$$2^{\star n} : N \cong \langle x_i, t | \mathcal{R}, t^2, [t, N_1] \rangle,$$

where N_1 denotes the stabilizer in N of the point 1. The homomorphic image of this progenitor obtained by factoring by the relations $\pi_1 w_1, \ldots, \pi_r w_r$ may then be expressed as the conventional presentation

$$\frac{2^{\star n} : N}{\pi_1 w_1, \ldots, \pi_r w_r} \cong \langle x_i, t | \mathcal{R}, t^2, [t, N_1], \pi_1 w_1, \ldots, \pi_r w_r \rangle.$$

Progenitors defined by either permutation or monomial actions with non-involutory symmetric generators can also be described in terms of conventional presentations, but a general statement about their form is impossible.

We will also sometimes express presentations in terms of *Coxeter-type* presentations, particularly in Chapter 3, that are defined as follows. A *Coxeter diagram* of a Coxeter-type presentation is a graph in which the vertices correspond to involutory generators and an edge is labeled with the order of the product of its two endpoints. Commuting vertices are not joined and an edge is left unlabeled if the corresponding product has order three. For most (labeled) graphs, the group defined by this presentation is infinite, indeed the graphs for which the corresponding group is finite were classified by Coxeter in

[21]. Sometimes, most notably in the Atlas [19], presentations of groups are expressed by drawing a graph that defines a group that is known to be infinite and a finite group is defined by giving additional relations between the generators alongside the graph.

1.7 The Aims of this Thesis

There are several different aims of this thesis.

In Chapter 2 we aim to find interesting symmetric presentations using progenitors defined using imprimitive actions.

In Chapter 3 we aim to show how the traditional Coxeter-Moser presentations associated with each of the finite simply laced Coxeter groups may be naturally derived using the techniques of symmetric generation.

In Chapter 4 we aim to find symmetric presentations defined using monomial representations of the groups $L_2(q)$.

Chapter 2

Symmetric Presentations Defined by Imprimitive Actions

2.1 Motivation

Let G be a group acting on a set X. Recall that a *block* of an action is a subset $B \subset X$ such that $|B| \neq 1$ or $|X|$ and for any $g \in G$ either $B^g \cap B = \emptyset$ or $B^g = B$. Recall also that an action is said to be *primitive* if there are no blocks and *imprimitive* otherwise. In this chapter we shall consider symmetric presentation defined by imprimitive actions. There are several motivations for this.

Natural Relations When investigating natural symmetric presentations of groups we seek the shortest relations possible. Often the Primitive Lemma is used to argue that whenever the action defining a progenitor is primitive the shortest relations, ie relations of length 2, can be disregarded.

We can, of course, turn this idea on its head and argue that if we would like the most natural relations possible, ie relations of length 2, then we need to consider a progenitor defined by an imprimitive action. Our main result in this direction is Theorem 2.3.

Transitive extensions Under certain circumstances a permutation group N that acts

k transitively on a set of n points can be a extended to a $k+1$ transitive permutation group acting on $n+1$ points M called a *transitive extension* of N. This can be used to extend a presentation defined by progenitor $2^{\star n} : N$ to a presentation of a related group defined by the progenitor $2^{\star(n+1)} : M$. This situation was investigated extensively by Bolt in [6, Chapter 2].

A notable example is the following. In [23] Curtis obtained a symmetric presentation for the sporadic first Janko group J_1 namely

$$\frac{2^{\star 11} : \mathrm{L}_2(11)}{(\sigma t_1)^5} \cong \mathrm{J}_1,$$

where the action defining this progenitor is the 2 transitive action of the group $\mathrm{L}_2(11)$ on the 11 point biplane and $\sigma \in \mathrm{L}_2(11)$ is some well chosen permutation. Using the fact that this action of the control group can be extended to a 3 transitive action of the sporadic simple Mathieu group M_{11} on 12 points [19, p.18], Curtis went on to show that the above symmetric presentation may be extended to a symmetric presentation for the sporadic simple group of O'Nan [19, p.132] thusly

$$\frac{2^{\star 12} : \mathrm{M}_{11}}{(s_\infty s_0)^4, (\sigma^3 s_\infty s_3)^5, (\sigma(s_\infty s_0)^2)^5} \cong \mathrm{O'N}.$$

The circumstances under which transitive extensions of permutation groups are possible are extremely restrictive and so it is rare to find such extensions possible. It is always possible, however, to extend a permutation representation to an imprimitive permutation representation on a larger number of points using wreath products. This makes extensions of symmetric presentations of smaller groups to symmetric presentations of larger groups much easier. Our main result in this direction is Theorem 2.4.

Coset Enumeration As noted in Section 1.2 to verify that a presentation holds it is often necessary to enumerate double cosets of the form NwN where N is the control

group and w is some word in the symmetric generators. Often, however, the index of the image of N inside the target group G is quite large making enumeration impractical. A common way around this is to enumerate double cosets of the form NwH where H is a proper subgroup of G defined by certain words in the symmetric generators that is larger than N and thus of a lower index in G than N. In particular, if the action defining the progenitor is imprimitive, then the symmetric generators in a particular block may be used to define such an H.

The best example of this is the symmetric presentation of the Conway group $\cdot 0$ discovered by Bray and Curtis in [12], namely

$$\frac{2^{\star\binom{24}{4}} : \mathrm{M}_{24}}{\pi t_{ab} t_{ac} t_{ad}} \cong \cdot 0,$$

where M_{24} denotes the largest of the sporadic simple Mathieu groups; a, b, c and d are pairs of points the union of which is a block of the $\mathcal{S}(5,8,24)$ Steiner system on which M_{24} naturally acts (see the Atlas, [19, p.94]); $\cdot 0$ is the full cover group of the largest sporadic simple Conway group (see the Atlas, [19, p.180]) and $\pi \in \mathrm{M}_{24}$ is the unique non-trivial permutation of M_{24} determined by the Famous Lemma. Here, the action defining the progenitor is imprimitive since the symmetric generators lie in blocks of size six known as sextets. The presentation is verified using the fact (proved by hand) that words of the form $t_{ab}t_{cd}$ all commute and thus generate an elementary abelian group of order 2^{12} normalized by the control group. Letting $H := 2^{12} : \mathrm{M}_{24}$ enabled Bray and Curtis to enumerate the double cosets of the form NwH and thus verify the symmetric presentation.

2.1.1 Some Preliminary Results

Here we give a couple of theorems that will be useful later in this thesis.

Theorem 2.1 (Dickson) The maximal subgroups of $L_2(q)$ are

- The group A_4 when $q \equiv \pm 3 \pmod 8$, with $5 \leqslant q$ prime;
- The group S_4 when $q \equiv \pm 1 \pmod 8$, with either q prime, or $q = p^2$ and $5 \leqslant p \equiv \pm 3 \pmod 8$;
- The groups A_5 when $q \equiv \pm 1 \pmod{10}$, with either q prime, or $q = p^2$ and $p \equiv \pm 3 \pmod{10}$;
- The dihedral groups of order $q - 1$ for $q \geqslant 13$ odd and $2(q - 1)$ for q even;
- The dihedral groups of order $q + 1$ for $q \neq 7$, 9 odd and $2(q + 1)$ for q even;
- The subfield subgroups: $L_2(q_0)$, where q is an odd prime power of q_0, for q odd, a prime power of q_0 for q even or; $PGL_2(q_0)$, where $q = q_0^2$, for q odd;
- The Frobenius group $p^r : (q - 1)/2$ for q odd and $p^r : (q - 1)$ for q even, recalling that in ATLAS notation, p^r denotes an elementary abelian group of order p^r.

The proof of this theorem and a very detailed discussion of the groups $L_2(q)$ and $PGL_2(q)$ may be found in Dickson, [34, Chapter XII]. (Dickson's own account is written in English that is now somewhat antiquated and thus difficult to follow. A more recent and readable discussion of these matters has been given by King in [48].)

We remark that what Dickson actually proved was a complete classification of all subgroups of the groups $L_2(q)$ and $PGL_2(q)$, but the above immediate corollary is sufficiently strong for our purposes.

We shall also need the following technical lemma of Galois theory when handling groups defined over a field of characteristic 2.

Lemma 2.2 The polynomial $P(x) = x^{2^r} + x + 1$ has a root in the field $\mathbb{F}_{2^{2r}}$ contained in no proper subfield.

Proof. We first note that since $D(P)(x) = 1 \neq 0$, where $D(P)$ denotes the formal derivative of P, P and P' have no common roots. We thus have by a standard result of Galois theory that P is separable and so has 2^r distinct roots (see Lang [50, Section V.8]). It is therefore sufficient to show that of the elements of the field $\mathbb{F}_{2^{2r}}$ that are contained in proper subfields, fewer than 2^r of them can be roots of P.

Let $i \in \mathbb{Z}^+$ such that $i|2r$ and $i < 2r$. Consider the unique subfield of $\mathbb{F}_{2^{2r}}$ of order 2^i. Call this $\mathbb{F}$.

If $i|r$ then any element of $\mathbb{F}$ will be contained in the unique subfield of order 2^r. No element of this subfield can be a root of P since any $a \in \mathbb{F}_{2^r}$ satisfies $a = a^{2^r}$ and so

$$P(a) = a^{2^r} + a + 1 = a + a + 1 = 1 \neq 0.$$

Now suppose i does not divide r. Then $i = 2k$ for some $k|r$. Half the elements of $\mathbb{F}$ will therefore be contained in a subfield of order 2^r, which cannot be roots of P by the previous paragraph. If n is the total number of elements of $\mathbb{F}_{2^{2r}}$ contained in a proper subfield other than the unique subfield of order 2^r we then have

$$n = \sum_{j|r, j<r} 2^j \leqslant \sum_{j=1}^{r-1} 2^j = 2^r - 1 < 2^r.$$

We thus have that of the elements of the field $\mathbb{F}_{2^{2r}}$ that are contained in proper subfields, fewer than 2^r of them can be roots of P. □

(We note in passing that the bounds used at the end of the proof of this lemma are extremely crude. In practice almost all of the roots of the polynomial P are not contained in proper subfields.)

2.2 A Brutal Relation

As an example of a natural relation that may be used to define a group we consider a natural example of an imprimitive action, namely the action of the dihedral group of order $4n$ on $2n$ points with n blocks of size 2. We will not consider dihedral groups of order $2n$ with $2 \not| n$ acting naturally on n points since the stabilizer of any two points in this case is trivial rendering the Famous Lemma useless.

Consider an even cycle with $2n$ vertices labeled $1, \ldots, 2n$ cyclically. If we fix the vertex 1 then the vertex diametrically opposed to it, $n+1$, will automatically be fixed too. Applying the the Famous Lemma we find that a word in the symmetric generators t_1 and t_{n+1} can only be equal to some member of a certain Klein foursgroup consisting of two involutions interchanging the vertices 1 and $n+1$ and one involution fixing them both. We consider possible words in these symmetric generators to factor the progenitor $2^{\star 2n} : D_{4n}$ by. Clearly a word of length 1 would map every symmetric generator to an element of the control group, so the shortest word we wish to consider is of length 2. Such a word cannot equal either of the 'interchanging' involutions by the Second Parity Lemma. We call the remaining involution π. Wanting the images of the symmetric generators to be distinct precludes us from using the relation $t_1 t_{n+1} = id$. We are thus naturally led to considering the factored progenitor

$$\frac{2^{\star 2n} : D_{4n}}{\pi t_1 t_{n+1}}. \qquad (\diamondsuit\diamondsuit)$$

2.2.1 The Main Theorem

Morally, a majority of finite simple groups are of the form $L_2(q)$ for some prime power q. By this we mean the following. Recall the statement of the Classification of the Finite Simple Groups. The cyclic groups of prime order are abelian and have no proper

non-trivial subgroups, so for many purposes may be largely disregarded. The order of the alternating group A_n is $n!/2$, so grows rapidly with n. There are only finitely many sporadic simple groups. The order of a group of Lie type is a polynomial in the order of the field over which it is defined whose degree is a polynomial function of the rank. Consequently, if we are given any positive integer N and we are asked which finite simple groups have order less than N we find that the low ranking groups of Lie type will account for a majority of them. In particular the groups $L_2(q)$ will account for a vast majority of the groups we find since their orders grow so slowly.

We thus wish to consider which of the groups $L_2(q)$ are homomorphic images of the factored progenitor $(\diamondsuit\diamondsuit)$.

Consider $n = 2$. By Dickson's Theorem any subgroup of $L_2(q)$ with structure D_8 must be contained either in one of th larger dihedral groups; a copy of S_4 or a subfield subgroup. There are only copies of S_4 in $L_2(q)$ if $q \equiv \pm 1 \pmod 8$. This holds for infinitely many prime powers, but also fails to happen for infinitely many. Furthermore, such a subgroup can only be contained in a dihedral group if $q \equiv \pm 1 \pmod 8$. It follows that copies of D_8 sit inside these groups in a rather complicated way making it difficult to prove any general result about them.

In contrast, copies of D_{12} are much more co-operative. By Dickson's Theorem copies of D_{12} lying in $\mathrm{L}_2(\mathrm{q})$ can only be contained in larger dihedral groups or subfield subgroups. Furthermore, if $p \neq 3$ then 3 does not divide q and so $q \equiv \pm 1 \pmod 3$ for any prime power q. If q is odd then $q \equiv \pm 1 \pmod 4$, so such dihedral subgroups almost always exist in larger dihedral groups making proving a result about them much easier. We proceed to prove the following.

Theorem 2.3 Consider the factored progenitor

$$\frac{2^{\star 6} : \mathrm{D}_{12}}{(26)(35)t_1t_4}. \qquad (\diamondsuit\spadesuit)$$

(a) The only groups of the form $L_2(2^r).d$ that are homomorphic images of ($\diamondsuit\spadesuit$) are the groups $L_2(2^{2r}).2$. In particular, the groups $L_2(2^r)$ are never images of ($\diamondsuit\spadesuit$).

(b) No group of the form $L_2(3^r).d$ is a homomorphic image of ($\diamondsuit\spadesuit$).

(c) Let $p \geqslant 5$ be a prime and

$$G := \begin{cases} PSL_2(p) & \text{p} \equiv \pm 1 \text{ (mod 24)}; \\ PGL_2(p) & \text{p} \not\equiv \pm 1 \text{ (mod 24)}. \end{cases}$$

Then G is a homomorphic image of ($\diamondsuit\spadesuit$).

Proof. (a) We first note that $L_2(2^{2r}).2$ is the only non-trivial split extension of $L_2(2^{2r})$ that can be an image of ($\diamondsuit\spadesuit$) since it contains all of the involutions of $P\Gamma L_2(2^{2r})$. Secondly, no split extension of a group of the form $L_2(2^{2r+1})$ can be an image, since they contain no copies of D_{12} as the only dihedral subgroups are either too small to contain a copy of D_{12} or do not have order divisible by 4. It remains to show that the groups $L_2(2^{2r}).2$ really are images. We do this by exhibiting explicit elements of $L_2(2^r)$ that satisfy the conventional presentation corresponding to ($\diamondsuit\spadesuit$) and that generate the whole of $L_2(2^r)$.

Consider the group elements

$$x = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \alpha, \qquad y = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad t = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$$

where α is the automorphism of $L_2(2^{2r})$ defined by the automorphism of the field $\mathbb{F}_{2^{2r}}$ given by the map $x \to x^{2^r}$. Since the matrix used to define x has order 3 and is invariant under the action of α, x will have order 6. Since the entries of y all lie in the prime subfield, and are therefore fixed by α, the elements x and y satisfy $(xy)^2 = id$ we so we have $\langle x, y\rangle \cong \mathrm{D}_{12}$. Moreover, for any $a \in \mathbb{F}_{2^{2r}}$, t will still satisfy the relations $t^2 = [t, y] = id$. To satisfy

the remaining relation we need to take a to be a root of the polynomial $x^{2^r}+x+1=0$ since

$$t^{x^3} = \begin{pmatrix} 1 & 0 \\ a^{2^r} & 1 \end{pmatrix} \text{ and } tt^{x^3} = \begin{pmatrix} 1 & 0 \\ a^{2^r}+a & 1 \end{pmatrix} \text{ thus } ytt^{x^3} = \begin{pmatrix} 1 & 0 \\ a^{2^r}+a+1 & 1 \end{pmatrix}.$$

By Dickson's Theorem the only subgroups of $L_2(2^{2r}).2$ that can contain our control group are either 'subfield subgroups' or dihedral groups. (Note that we have actually used an adaptation of Dickon's theorem that incorporates the field automorphism that easily deduced from the full statement of the Theorem. In particular if H is a subfield subgroup of $L_2(2^{2r}).2$ then the outer automorphism of $L_2(2^{2r}).2$ will wither become an automorphism of H or will commute with everything in H giving a copy of $2 \times H$. Similarly the field automorphism becomes an automorphism of the dihedral groups.) Now, we have that

$$x^2t = \begin{pmatrix} 1+a & 1 \\ 1 & 0 \end{pmatrix},$$

which clearly has trace $a+1$. If we can choose a so that it is not a member of a proper subfield, then $a+1$ will not be contained in a proper subfield. We can do this by Lemma 2.2. Our control group is therefore contained in a maximal dihedral group which is the full centralizer of x^3. Since t does not centralize x^3 we have that $\langle x, y, t\rangle \cong L_2(q).2$.

(b) None of the subgroups of $L_2(3^r)$ contain a copy of D_{12} since such a subgroup would have to be contained in either a subfield subgroup (which by induction will also contain no copies of D_{12}) or in a dihedral group of order $3^r \pm 1$, but the order of such dihedral groups is not divisible by three and so cannot contain a copy of D_{12}. Therefore the only groups that can be images of the unfactored progenitor are of the form $L_2(3^{2r}).2$ since this extension of $L_2(3^{2r})$ contains all of the involutions.

The additional relation, however, cannot hold in $L_2(3^{2r}).2$ either. Let π denote the

involution corresponding to the permutation (2,6)(3,5). If the additional relation did hold in $L_2(3^{2r}).2$ then there would be a copy of the Klein foursgroup in $L_2(3^{2r}).2$ containing t_1, t_4 and π. If all three of these lie in the derived subgroup of $L_2(3^{2r}).2$ then the control group would lie in the derived subgroup since π and its conjugates generate the whole of the control group which by the above cannot lie in the derived subgroup. Half of this Klein foursgroup must therefore lie outside the derived subgroup. Since t_1 and t_4 are conjugate and the identity belongs to the derived subgroup it follows that t_1 and t_4 must lie outside the derived subgroup. Again this forces π and thus the whole of the control group to be contained in the derived subgroup forcing a contradiction. A similar argument applies to the group $L_2(3^{2r}).2^2$. Therefore no group of the form $L_2(3^{2r}).d$ is an image of (♢♠).

(*c*) We prove this by exhibiting explicit matrices based on Bray's proof of a related result for the progenitor $2^{\star 3} : \mathrm{S}_3$ [8, p.85]. This makes use of the isomorphism $SO_3(q) \cong PGL_2(q)$ for any odd prime power q (see Cameron [17, p.67] for details). In particular we shall exhibit matrices generating the group and satisfying the conventional presentation

$$\langle x, y, t | x^6, y^2, (xy)^2, t^2, [t, y], ytt^{x^3} \rangle. \qquad (♢♡)$$

corresponding to the symmetric presentation (♢♠).

For any value $a \in \mathbb{F}_{p^n}$ the matrices

$$x = \begin{pmatrix} 1 & 1 & 0 \\ -1 & 0 & 0 \\ \frac{2a+1}{3} & \frac{a+2}{3} & 1 \end{pmatrix}, \qquad y = \begin{pmatrix} 1 & 0 & 0 \\ -1 & -1 & 0 \\ 1 & 0 & -1 \end{pmatrix} \quad \text{and} \quad t = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

satisfy the presentation $\langle x, y | x^6, y^2, (xy)^2 \rangle \cong \mathrm{D}_{12}$ and the relations $t^2, [t, y], ytt^{x^3}$. Further-

more these matrices all preserve the symmetric bilinear form defined by the matrix:

$$A = \begin{pmatrix} 2 & -1 & 1 \\ -1 & 2 & -a-1 \\ 1 & -a-1 & 2 \end{pmatrix}$$

which has determinant $2(1-a)(2+a)$ which is non-zero whenever $a \neq 1, -2$.

Consider $a = (p-1)/2$ with p prime. In this case we have the matrices

$$x = \begin{pmatrix} 1 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & \frac{1}{2} & 1 \end{pmatrix}, \qquad y = \begin{pmatrix} 1 & 0 & 0 \\ -1 & -1 & 0 \\ 1 & 0 & -1 \end{pmatrix} \text{ and } t = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

which satisfy all the relations of the presentation ($\diamondsuit\heartsuit$) and preserve the symmetric bilinear form defined by A. Furthermore, in this case A has determinant $(9-p^2)/2$. This is non-zero and well defined since we're assuming $p \geqslant 5$. We further note that by Dickson's Theorem the only proper subgroups of G (where G is as defined in part (c) of the statement of Theorem 2.3) containing our D_{12} must themselves be dihedral (there are no subfield subgroups here since we are only considering fields of prime order). In particular x^3 must be in the center of this maximal subgroup, which is the full centralizer of x^3. Since t does not centralize x^3 it cannot be contained in this subgroup, and must therefore generate the whole of G.

If $p \not\equiv \pm 1 \pmod{12}$ then $L_2(p)$ does not contain a copy of the control group. Furthermore if $p \equiv \pm 1 \pmod{12}$, but $p \not\equiv \pm 1 \pmod{24}$ then the additional relation tells us that $\langle x^3, t_1 \rangle$ is dihedral of order eight, which in the simple group cannot happen. The above matrices will therefore generate $PGL_2(p)$ rather than $L_2(p)$ whenever $p \not\equiv \pm 1(24)$.

Finally it remains to show that if $p \equiv \pm 1 \pmod{24}$ then $PGL_2(p)$ is not an image of ($\diamondsuit\spadesuit$). Again, the control group is contained in the simple group, so $PGL_2(p)$ could

only be an image if the symmetric generators lie outside the simple group. As before the additional relation tells us that $\langle x^3, t_1 \rangle$ is dihedral of order eight. This must lie entirely in the simple group since x^3 does and the only elements of order 4 in $\mathrm{PGL}_2(p)$ also lie in the simple group (see King [48]). This completes the proof. □

Case (c) of the above result does not easily generalize to higher prime powers. Powers of larger primes defining groups that are images of $(\diamondsuit\spadesuit)$ often need automorphisms defined by the Frobenius automorphisms of the underlying field, and seem to prefer $P\Gamma L_2(q)$ and not in a way that can be described by a simple pattern. Some of the smaller examples are listed in the below table.

power	decoration
5^2	$\mathrm{P\Sigma L}_2(5^2)$ and $\mathrm{P}\Gamma\mathrm{L}_2(5^2)$
5^3	none
5^4	$\mathrm{L}_2(5^4).2$ and $\mathrm{P\Sigma L}_2(5^4)$
7^2	$\mathrm{P\Sigma L}_2(7^2)$
7^3	none
11^2	$\mathrm{P\Sigma L}_2(11^2)$ and $\mathrm{P}\Gamma\mathrm{L}_2(11^2)$
13^2	$\mathrm{P\Sigma L}_2(13^2)$ and $\mathrm{P}\Gamma\mathrm{L}_2(13^2)$

2.2.2 Additional Relations

Perhaps unsurprisingly using a relation as short as the Brutal Relation ensures that few additional short relations are required to produce finite homomorphic images of the factored progenitor $(\diamondsuit\spadesuit)$. In several of the smaller cases to which Theorem 2.3 applies we can easily find additional relations required to completely determine the target group. In Table I we list additional relations of the form $(t_1(1,2)(3,6)(4,5))^a$ and $(t_1(1,3)(4,6))^b$ that completely determine the groups given. Following the conventions of [31] the numbers given in bold are sufficient to define the whole group stated in Table I.

a	b	Target
6	10	$2\times\mathrm{PGL}_2(5)$
6	**5**	$\mathrm{PGL}_2(5)$
7	**8**	$\mathrm{PGL}_2(7)$
10	**12**	$2\times\mathrm{PGL}_2(11)$
9	16	$\mathrm{PGL}_2(17)$
11	**11**	$\mathrm{L}_2(23)$
20	**9**	$\mathrm{PGL}_2(19)$
10	**17**	$\mathrm{L}_2(16).2$

Table I: Some additional relations defining homomorphic images of the factored progenitor (♢♠) related to Theorem 2.3.

We further note that additional relations of the form $(t_1(1,2)(3,6)(4,5))^a$ and $(t_1(1,3)(4,6))^b$ can also give finite homomorphic images of the factored progenitor (♢♠) whose existence is *not* alluded to by Theorem 2.3. We exhibit a selection of these in Table II.

a	b	Target
10	**13**	$\mathrm{P\Sigma L}_2(25)$
12	**10**	$2^6{:}\mathrm{S}_5$
13	**12**	$\mathrm{L}_3(3).2$
15	**10**	$\mathrm{U}_3(4).2$

Table II: Some additional relations defining homomorphic images of the factored progenitor (♢♠) not related to Theorem 2.3.

We remark that in addition to those given in the Tables I and II several soluble images can also easily be obtained using few additional relations of the above types.

2.2.3 Other Groups

Given the vast plethora of almost simple groups that Theorem 2.3 gives us it is natural to ask which other groups can also be expressed as homomorphic images of the factored progenitor (♢♠). To this end we make the following two conjectures.

Conjecture 1 The symmetric group S_n is a homomorphic image of the factored progenitor (♢♠) unless $n \in \{1, 2, 3, 4, 6, 7, 8, 11, 14\}$.

For $n \leqslant 4$, $\mathrm{D}_{12} \not\leqslant S_n$ and so clearly S_n cannot be an image even of the unfactored progenitor $2^{\star 6} : \mathrm{D}_{12}$.

This conjecture has been verified by computer for $n \leqslant 50$. In particular, for the 'sporadic' values of $n \leqslant 14$ for which S_n is an image of $(\diamondsuit\spadesuit)$ we can explicitly give permutations satisfying all the relations and generating the whole of S_n. We give these in full in Table III.

In each case it is straightforward to argue that S_n is indeed generated by the permutations given using information about the subgroup structure of S_n which for $n \leqslant 13$ is given in the ATLAS, [19]. For example in the case $n = 13$, whose maximal subgroups are listed in [19, p. 104], we have that $tt^{x^2} = (1,3,5,4,6,2,7,13,12,9,11,10,8)$, which has order 13, and $tt^{x^2}y = (1,4)(11,13)(2,9,12,7,10,8,6,5,3)$, which has order 9. The only maximal subgroups of S_{13} containing elements of order 13 are copies of the Frobenious group 13:12, which clearly contains no elements of order 9, and copies of the alternating group A_{13}. The permutation given for x is visibly odd and therefore cannot be contained in A_{13}. The permutations given in Table III must therefore generate the whole group.

n	x	y	t
5	(123)(45)	(23)(45)	(24)(35)
9	(123456)(789)	(16)(25)(34)(78)	(28)(34)(57)
10	(1,2,3,4,5,6)(7,8,9)	(1,6)(2,5)(3,4)(7,8)	(2,8)(3,4)(5,7)(9,10)
12	(1,2,3,4,5,6)	(2,6)(3,5)(8,12)(9,11)	(2,8)(6,12)
	(7,8,9,10,11,12)		(3,11)(5,9)(7,10)
13	(1,2,3,4,5,6)	(1,6)(2,5)(3,4)	(1,10)(2,7)(3,11)(7,9)
	(7,8,9)(10,11)(12,13)	(10,13)(11,12)	

Table III: Conjecture 1 for small values of n. In the above $\langle x, y\rangle \cong \mathrm{D}_{12}$ with $|x| = 6$ and $|y| = 2$.

We emphasise that the only real evidence for the above conjecture is computational. More heuristically, the number of elements of order 6 in S_n rapidly grows quite large (the group S_{15} has 29 classes of elements of order 6) and each of these is contained in several

different classes of dihedral groups of order 12, making it very likely that such a group is a homomorphic image of (♢♠).

In light of Conjecture 1 we make the following further conjecture.

Conjecture 2 The alternating group A_n is a homomorphic image of the factored progenitor (♢♠) unless $n \in \{3, \ldots, 13, 19, 20, 21, 23\}$.

For $n \leqslant 6$, $\mathrm{D}_{12} \not\leqslant A_n$ and so clearly A_n cannot be an image even of the unfactored progenitor $2^{\star 6} : \mathrm{D}_{12}$.

As with conjecture 1, this conjecture has been verified by computer for $n \leqslant 50$.

We emphasise that the only real evidence for the above conjecture is computational. More heuristically, the number of elements of order 6 in A_n rapidly grows quite large (the group A_{24} has 50 classes of elements of order 6) and each of these is contained in several different classes of dihedral groups of order 12, making it very likely that such a group is a homomorphic image of (♢♠).

We remark that proving Conjectures 1 and 2 is morally much more difficult than proving Theorem 2.3 for the following reason. To justify the assertion that a given collection of elements will generate the whole of a group G it is necessary to have a complete understanding of the subgroup structure of G and in particular in the maximal subgroups of G. In the case of $L_2(q)$ and $PGL_2(q)$ these are given by Dickson's Theorem, which 'morally' states that the maximal subgroups of these are "essentially the same for every q". The nearest analogue of this result for the symmetric and alternating groups is a well-known corollary of the O'Nan Scott Theorem (see for instance [16, p.107]). In stark contrast to Dickson's theorem, this result can only describe the maximal subgroups inductively, ie a full understanding of the maximal subgroups of S_n can only be obtained from an understanding of smaller groups and in particular of all almost simple permutation groups acting primitively on n points. In short, the approach used in the $L_2(q)$ case becomes

substantially harder in the S_n and A_n cases. It follows that radically different methods will need to be employed in these cases.

2.3 Wreathed Extensions

Our attention now turns to the problem of using imprimitive actions, specifically actions defined using wreathed products, to extend symmetric presentations of smaller groups to symmetric presentations of larger groups.

Let

$$\frac{2^{\star n} : N}{\mathcal{R}} \cong G$$

be a symmetric presentation of the group G defined by some set of relations $\mathcal{R}$. Let M be a transitive permutation group of degree m. We define a *wreathed extension* of the above symmetric presentation to be a symmetric presentation

$$\frac{2^{\star nm} : (N \wr M)}{\mathcal{R}'} \cong G^+$$

where the progenitor is defined by the natural action of $N \wr M$ on nm points; $\mathcal{R}'$ is a set of relations containing $\mathcal{R}$ and G^+ is a group that contains G as a subgroup. In this section we investigate this method of transitively extending symmetric generating sets for small groups to symmetric generating sets for larger groups.

Our main result is the following. In keeping with ATLAS notation we write $2^r + 1$ for the cyclic group of order $2^r + 1$ and write $U_3(2^r)$ where some authors would write $U_3(2^{2r})$.

Theorem 2.4 Let $r \geqslant 2$. (i) The group $(2^r+1) \times L_2(2^r)$ (and therefore the group $L_2(2^r)$) is a homomorphic image of the progenitor $2^{\star(2^r+1)} : (2^r + 1)$.

(ii) The group $SU_3(2^r)$ (and therefore the group $U_3(2^r)$) is a homomorphic image of the progenitor $2^{\star((2r+1)+(2r+1))} : ((2^r+1) \wr 2)$. Furthermore the symmetric generators in a block of the action defining this progenitor along with the subgroup $(2^r+1)^2 \leqslant (2^r+1) \wr 2$ generate

a maximal subgroup with structure $(2^r+1)\times L_2(2^r)$ that stabilizes a non-isotropic vector in the module naturally acted by $SU_3(2^r)$ (and so any symmetric presentation of $SU_3(2^r)$ as an image of this progenitor may be given as a wreathed extension of a symmetric presentation given in part (i)).

Proof. As in the proof of Theorem 2.3 we give explicit elements of the group that generate the group and satisfy the relations of the conventional presentation corresponding to the progenitors in question. Let $\alpha \in \mathbb{F}_{2^{2r}}$ be a generator of $\mathbb{F}_{2^{2r}}^{\times}$ and let V be the natural 3 dimensional $\mathbb{F}_{2^{2r}}$ module acted on by $SU_3(2^r)$. Consider the following matrices

$$x = \begin{pmatrix} \alpha^{2^r-1} & 0 & 0 \\ 0 & \alpha^{2^r-1} & 0 \\ 0 & 0 & \alpha^{2^{2r}-1-2(2^r-1)} \end{pmatrix} \quad y = \begin{pmatrix} 0 & 0 & 1 \\ \alpha^{2^r+1} & 1 & \alpha^{2^r+1} \\ 1 & 0 & 0 \end{pmatrix} \quad t = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

(i) We consider the group generated by the matrices t, x and $x^n x^y$ for some n. Since each of the matrices x and t has determinant 1, any words in these matrices will generate a subgroup of $SL_3(2^{2r})$. Now by direct calculation we have that

$$x^n x^y = \begin{pmatrix} \alpha^{2^{2r}-1-2(2^r-1)}\alpha^{(2^r-1)n} & 0 & 0 \\ \alpha^{2^{2r}-1-2(2^r-1)}\alpha^{(2^r-1)n}(\alpha^{2^{2r}-1-2(2^r-1)} - \alpha^{2^r-1}) & \alpha^{2^r-1}\alpha^{(2^r-1)n} & 0 \\ 0 & 0 & \alpha^{2^r-1}\alpha^{(2^{2r}-1-2(2^r-1))n} \end{pmatrix}.$$

Both this and the matrix t clearly stabilize the 1 dimensional subspace of V spanned by the vector (0,0,1). They thus generate a subgroup of $(2^r+1)\times L_2(2^r) =: T$, the stabilizer of this subspace. If n is chosen so that $\alpha^{2^r-1}\alpha^{(2^{2r}-1-2(2^r-1))n} = 1$ then $x^n x^y$ will belong to the derived subgroup of T and since t is an involution it will also belong to the derived subgroup of T since there are no elements of even order in the center of T. We therefore

have that $\langle x^n x^y, t\rangle \leqslant L_2(q)$. We claim that $\langle x^n x^y, t\rangle = L_2(q)$.

We now consider Dickson's theorem to show that there is no maximal subgroup containing both $x^n x^y$ and t.

First note that since x^n is central and $|x^n| = |x^y| = 2^r + 1$ we have that $(x^n x^y)^{(2^r+1)} = (x^n)^{(2^r+1)}(x^y)^{(2^r+1)} = id$, so $x^n x^y$ has order $2^r + 1$ since no power of x^y is central.

The element $x^n x^y$ is not contained in a subfield subgroup. Since $|x^n x^y|$ is a factor of $2^r + 1$, $x^n x^y$ is contained in neither a dihedral group of order $2(2^r - 1)$ nor a Froebenious group of structure $2^r : (2^r - 1)$. The two elements could only be contained in a dihedral group of order $2(2^r + 1)$ if t normalized the subgroup generated by $x^n x^y$. Since $x^n x^y$ is lower triangular all of its powers are lower triangular, so in particular all elements in the subgroup generated by $x^n x^y$ are lower triangular. By direct calculation $(x^n x^y)^t$ is upper triangular, so in particular it is not lower triangular, so $\langle x^n x^y, t\rangle$ cannot be dihedral. We thus have $\langle x^n x^y, t\rangle = L_2(q)$.

Clearly x commutes with both t and $x^n x^y$ and so generates a cyclic group commuting with the whole of our $L_2(2^r)$ and since $|x| = 2^r + 1$, $\langle t, x, x^y\rangle \cong (2^r + 1) \times L_2(2^r)$.

Finally, the progenitor in this case corresponds to the conventional presentation

$$\langle x, t | x^{2^r+1}, t^2\rangle$$

and the above matrices clearly satisfy these relations. Consequently $(2^r + 1) \times L_2(2^r)$ is an image of the progenitor $2^{\star(2^r+1)} : (2^r + 1)$ as required.

(ii) In this case we have the following conventional presentation for the progenitor

$$\langle x, y, t | x^{(2^r+1)}, y^2, [x, x^y], t^2, [t, x]\rangle.$$

We now observe that the matrices x, y and t given above satisfy the relations of this presentation. We further note that each of the above matrices have determinant 1 and

thus certainly generate a subgroup of $SL_3(2^r)$. Furthermore, if P is any of the above matrices then $P^T A P^\sigma = A$ where A is the matrix

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

P^T denotes the transpose of the matrix P and P^σ denotes the image of $P = (p_{ij})$ under the map $p_{ij} \mapsto p_{ij}^{2^r}$. Note that the determinant of A is $1 + \alpha^{2(2^r+1)}$ which is non-zero since, by the definition of α, we have $1 = \alpha^{2^{2r}-1} = (\alpha^{2^r+1})^{2^r-1}$ and $2^r - 1$ is odd. The matrices therefore preserve the non-singular Hermitian bilinear form defined by A and so are contained in the copy of $SU_3(2^r)$ preserving this form. We note further that the matrices x and t each fix the one dimensional subspace spanned by the vector (0,0,1), which is isotropic with respect to the above bilinear form. These matrices are therefore contained in the maximal subgroup of $SU_3(2^r)$ stabilizing the non-isotropic vector $(0, 0, 1)$. (The maximal subgroups of the groups $U_3(2^r)$ were determined by Hartley. See King, [48, p.7], for details.) Since y clearly maps the vector (0,0,1) to $(1, \alpha^{2^r+1}, 0) \neq (0, 0, 1)$ these three matrices must altogether generate the whole of the group $SU_3(2^r)$. □

We remark that this Theorem does not generalize well to characteristics other than 2. The group $\mathrm{U}_3(3)$ (and therefore the group $\mathrm{SU}_3(3)$) is not an image of the progenitor $2^{\star(4+4)} : (4 \wr 2)$ despite the stabilizer of of an non-isotropic vector having structure $4 \cdot \mathrm{S}_4$. The group $\mathrm{U}_3(5)$ hits similar problems.

2.4 $\mathrm{U}_3(4)$

One of our motivations for considering imprimitive actions was the hope that they may lead to natural and beautiful presentations of groups. The smallest case of Theorem 2.4 gives us an example of this. We first note that the in this case the symmetric generators

in a given block satisfy a classical presentation of the group A_5. For completeness we give this conventional presentation as a symmetric presentation and prove it in the traditional manner similar to that of other symmetric presentations.

Lemma 2.5

$$\frac{2^{\star 5}\colon 5}{(t_1(1,2,3,4,5))^3} \cong A_5$$

Proof. The permutations $t_1 = (2,3)(4,5)$ and $x = (1,2,3,4,5)$ satisfy the conventional presentation corresponding to this symmetric presentation, namely

$$\langle x, t | x^5, t^2, (tx)^3 \rangle.$$

These permutations generate a copy of A_5. (Alternatively we could use the isomorphism $A_5 \cong L_2(4)$ and observe that the matrices given in the proof of the Theorem 2.4 in this special case satisfy the additional relation.)

It remains to verify the order of the target group. We do this with a straightforward coset enumeration that is readily done by hand. We do this in Table IV.

Label $[w]$	Coset Stabilizing subgroup	$\lvert N : N^{(w)}\rvert$
$[\star]$	$N \cong 5$	1
$[t_1]$	$N^{(t_1)} \cong \langle e \rangle$	5
$[t_1t_2]$	As $t_1t_2 \sim t_1$	
$= [t_1]$		
$[t_1t_3]$	$N^{(t_1t_3)} \cong \langle e \rangle$	5
$[t_1t_3t_1]$	$N^{(t_1t_3t_1)} \cong 5$ as $t_1t_3t_1 = t_1t_3t_2^2t_1t_5^2 = t_1x^2t_1x^2t_5 \sim t_5t_3t_5$	1
	and $t_1t_3t_1 = t_1t_2^2t_3t_4^2t_1 = x^3t_3x^3t_4t_1 \sim t_1t_4t_1$	
$[t_1t_3t_2]$	as $t_1t_3t_2 = t_1x^2t_1 \sim t_3t_1$	
$= [t_1t_4]$		
$[t_1t_3t_4]$	as $t_1t_3t_4 = t_1t_2^2t_3t_4 \sim t_3x^3 \sim t_1$	
$= [t_1]$		
$[t_1t_3t_5]$	as $t_1t_3t_5 = t_1t_2^2t_3t_4^2t_5 = x^3t_3xt_1 = x^4t_4t_1$	
$= [t_1t_3]$		

Table IV: The Coset Enumeration for A_5. □

We remark that since the action defining the progenitor $2^{\star 5} : 5$ is primitive we can disregard factoring by relations of length 2 by the Primitive Lemma. The relation of Lemma 5.2 is therefore one of the shortest natural relations to consider.

We aim to extend the above presentation to a homomorphic image of $2^{\star(5+5)} : (5 \wr 2)$. The above Lemma gives an 'intra-block' relation that describes how symmetric generators lying in the same block relate to each other. We seek an 'inter-block' relation to define a symmetric presentation. Defining elements of our control group with the presentation $5 \wr 2 = \langle x, y | x^5, y^2, [x, x^y] \rangle$ an element that is natural to consider is the involution y. By the Second Parity Lemma the shortest relation involving y we can use is $(ty)^3$ since y interchanges the two blocks. Consequently we prove the following result.

Lemma 2.6 Let G be defined by the symmetric presentation

$$\frac{2^{\star(5+5)} : (5 \wr 2)}{(t_1 y)^3} =: \mathrm{G},$$

where our control group is defined by the presentation $\langle x, y | x^5, y^2, [x, x^y] \rangle$. Then $|G| \leqslant 750$ and is thus soluble.

Proof. First note that since $|5 \wr 2| = 50$ it is enough to show that the image of the control group has index at most 15. This is an easy coset enumeration given in Table V.

Label $[w]$	Coset Stabilizing subgroup	$\lvert N : N^{(w)} \rvert$
$[\star]$	$N \cong 5 \wr 2$	1
$[t_1]$	$N^{(t_1)} \cong 5$	10
$[t_1 t_2]$	$N^{(t_1 t_2)} \cong 5 \wr 2$	1
	as $t_1 t_2 = t_1 t_2 t_7^2 = t_1 y t_2 t_7 \sim t_6 t_2 t_7 \sim t_7 t_2 t_8 = y t_7 t_8$	
$[t_1 t_2 t_1]$	as $t_6^2 t_1 t_2 t_1 = t_6 y t_1 t_6 t_1 \sim t_1^2 t_2 t_1 = t_2 t_1$	
$= [t_1 t_2]$		
$[t_1 t_2 t_3]$	as $t_1 t_2 t_3 = t_1 t_7^2 t_2 t_3 \sim t_1 t_2 y t_3 \sim t_6 t_7 t_3 = t_6 t_3 y^{x^2} \sim t_2 t_7 \sim t_7$	
$= [t_1]$		
$[t_1 t_2 t_6]$	as $t_1 t_2 t_6 = t_1 y^x t_2 \sim t_{10} t_2$	
$= [t_{10} t_2]$		

Table V: The Coset Enumeration for a group of order 750. Since each case of the form $t_1 t_i$, $i \in \{2, \ldots 5\}$ is similar, we only give the calculations in the case $t_1 t_2$. Similarly for $t_1 t_i t_j$ we only give the cases $t_1 t_2 t_1$ and $t_1 t_2 t_6$.

No simple group of order at most 750 has order divisible by 25, by easy Sylow's Theorem arguments. Therefore a simple finite group containing a faithful image of the control group must have order greater than 750. Hence $|G| \leqslant 750$ implies G is soluble. □

Now by the Second Parity Lemma the next shortest relation involving y we can sensibly consider is $(ty)^5$ since y acts fixed point freely. We have thus been naturally led to the following result.

Lemma 2.7

$$\frac{2^{\star(5+5)} : (5 \wr 2)}{(t_1 x^2 x^y)^3, (t_1 y)^5} \cong \mathrm{U}_3(4). \qquad (\diamondsuit\clubsuit)$$

Proof. We first exhibit explicit matrices that generate the group $\mathrm{U}_3(4)$ and satisfy the conventional presentation corresponding to the symmetric presentation. As a conventional presentation for this symmetric presentation is given by

$$\langle x, y, t | x^5, y^2, [x, x^y], t^2, [t, x], (tx^3x^y)^3, (ty)^5 \rangle.$$

Recalling the matrices given in the proof of Theorem 2.4 we define the matrices

$$x = \begin{pmatrix} \alpha^3 & 0 & 0 \\ 0 & \alpha^3 & 0 \\ 0 & 0 & \alpha^9 \end{pmatrix} \qquad y = \begin{pmatrix} 0 & 0 & 1 \\ \alpha^5 & 1 & \alpha^5 \\ 1 & 0 & 0 \end{pmatrix} \qquad t = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

where α is a generator for $\mathbb{F}_{16}^{\times}$. Recall that if P is any of the above matrices then P has the property that $P^T A P^\sigma = A$ where A is the matrix

$$\begin{pmatrix} 1 & \alpha^5 & 0 \\ \alpha^5 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

P^T denotes the transpose of the matrix P and P^σ denotes the image of $P = (p_{ij})$ under the map $p_{ij} \mapsto p_{ij}^4$. Note further that A has determinant $1 + \alpha^{10}$ which is non-zero and therefore defines a non-singular Hermition bilinear form. With respect to this form

we observe that the vector (0,0,1) is nonisotropic. This vector is visibly stabilized by a subgroup of structure $U_2(4) \cong A_5$. Note further that y does not fix the vector (0,0,1) and is therefore contained in the stabilizer of an isotropic point - these matrices will therefore generate the whole of the group. We have therefore verified that $U_3(4)$ is a homomorphic image of the factored progenitor ($\diamondsuit\clubsuit$).

It remains to perform the coset enumeration to verify the order. Unfortunately the index here is too great to be performed by hand. We thus resort to using the Double Coset Enumerator as described in Section 1.4.

```
> G:=WreathProduct(CyclicGroup(5),Sym(2));
> RR:=[<[1],G!(1,2,3,4,5)(6,9,7,10,8),3>,
<[1],G!(1,6)(2,7)(3,8)(4,9)(5,10),5>];
```

Here we have defined `G` $\cong 5 \wr 2$ to be our control group and defined `RR` to be a sequence consisting of the defining relations of our presentation.

```
> CT:=DCEnum(nn,RR,HH:Print:=5,Grain:=100);
Index: 1248 = Rank: 34 = Edges: 254 = Status: Early closed = Time:
0.340
```

Here the computer has found that the target group has order $|5 \wr 2| \times 1248 = |U_3(4)|$. This completes the proof. □

2.5 Other Wreathed Extensions

To illustrate that the presentation of Lemma 2.7 is not just a 'one-off' we exhibit a number of other interesting symmetric presentations that are wreathed extensions discovered in the course of these investigations. Since the proofs of these results are entirely analogous to the proof of Lemma 2.7 we omit them.

Lemma 2.8 (i)

$$\frac{2^{\star 3} : \mathrm{S}_3}{(t_1(1,2))^3} \cong \mathrm{S}_4$$

(ii)

$$\frac{2^{\star(3+3)} : (\mathrm{S}_3 \wr 2)}{(t_1(1,2))^3, (2,3)(5,6)(t_1 t_4)^4} \cong 2 \times \mathrm{L}_3(7).2$$

where $\mathrm{S}_3 \wr 2 \cong \langle (1,2), (1,2,3), (1,4)(2,5)(3,6) \rangle$.

Part (i) of this Lemma is a special case of Theorem 3.1. The 'intra-block' relation can be naturally arrived at using the Special Lemma since shorter relations of this form define groups no larger than the control group. We further remark that in some sense this Lemma is simply a reinterpretation of an old result since a presentation given in the "Addenda and Corrigenda" section of the ATLAS [19, p.xxxiv] is the following Coxeter-type presentation (note that the Addenda and Corrigenda appear in the more recent corrected version of the ATLAS).

$$\langle \quad \overset{a}{\bullet}\!\!-\!\!\overset{b}{\bullet}\!\!-\!\!\overset{c}{\bullet}\ 8\ \overset{d}{\bullet}\!\!-\!\!\overset{e}{\bullet}\!\!-\!\!\overset{f}{\bullet} \quad \mid af = (cd)^4 \rangle$$

We can identify the generators in our symmetric presentation with the generators in the above presentation as follows.

ATLAS	$\langle N, t_i \rangle$
a	(2,3)
b	(1,2)
c	t_1
d	t_4
e	(4,5)
f	(5,6)

Our next lemma is an example of a wreathed extension that comes from an imprimitive action with more than two blocks. It also provides an example of a presentation defined by relations more complex than simply a pairing of an inter-block relation and an intra-block relation.

Lemma 2.9

$$\frac{2^{\star(4\times 2)} : (2 \wr \mathrm{S}_4)}{(t_1 t_2)^3, (t_1 \pi)^7} \cong 2 \times \mathrm{HS}{:}2$$

where $2 \wr \mathrm{S}_4 \cong \langle (1,2), (1,3)(2,4), (1,3,5,7)(2,4,6,8) \rangle$ and π is the permutation $(1,3,8,15,16,14,9,2)(4,10,12,11,13,7,6,5)$.

Viewing the action defining the progenitor as the action of $2 \wr \mathrm{S}_4$ on the sixteen vertices of the tesseract (so the blocks of this action may be viewed as 'opposite corners') the relations in the above lemma may be viewed as follows. The symmetric generators t_1 and t_2 are adjoined by an edge and π is permutation preserving an 8-cycle of the tesseract. The group HS is the sporadic Higman-Sims group (see Atlas [19, p.80]).

In this case the stabilizer of a block defines a soluble group of order 480.

Chapter 3

Symmetric Presentations of Finite Coxeter Groups

3.1 Introduction

Recall from Chapter 1 that a *Coxeter diagram* of a Coxeter-type presentation is a graph in which the vertices correspond to involutory generators and an edge is labeled with the order of the product of its two endpoints. Commuting vertices are not joined and an edge is left unlabeled if the corresponding product has order 3. A Coxeter diagram and its associated group are said to be *simply laced* if all the edges of the graph are unlabeled. In [26] Curtis notes that if such a diagram has a "tail" of length at least two, as in Figure I, then we see that the generator corresponding to the terminal vertex, a_r, commutes with the subgroup generated by the subgraph $\mathcal{G}_0$.

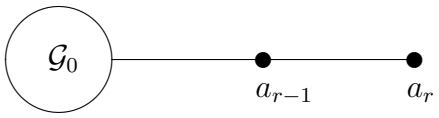


Figure I: A Coxeter diagram with a tail.

In this chapter we slightly generalize the notion of a "graph with a tail" and in doing so provide symmetric presentations for all the simply laced irreducible finite Coxeter groups

with the aid of little more than a single short relation. These in turn readily give rise to natural representations of these groups in both characteristics 0, 2 (and 5) among others.

The presentations given here, whilst not new, do provide an excellent example of how the techniques of symmetric generation may be used to arrive at very natural constructions of groups, and in seeing how these presentations may in turn lead to highly symmetric representations of these groups.

For the basic definitions and notation for Coxeter groups used throughout this chapter we refer the reader to Humphreys, [44]. The contents of this chapter is based heavily the author's paper [38] and extensions of these results to infinite Coxeter groups are at the time of writing being investigated jointly with Jürgen Müller in [40].

3.2 The Main Theorem

In this chapter we shall prove the following theorem.

Theorem 3.1 Let S_n be the symmetric group acting on n objects and $W(\Phi)$ denote the Weyl group of the root system Φ. Then:

1. $$\frac{2^{\star\binom{n}{1}} : S_n}{(t_1(1,2))^3} \cong W(A_n)$$

2. $$\frac{2^{\star\binom{n}{2}} : S_n}{(t_{1,2}(2,3))^3} \cong W(D_n) \text{ for } n \geqslant 4$$

3. $$\frac{2^{\star\binom{n}{3}} : S_n}{(t_{1,2,3}(3,4))^3} \cong W(E_n) \text{ for } n = 6, 7, 8.$$

In case (1) the action of S_n defining the progenitor is the natural action of S_n on $X := \{1, \ldots, n\}$; in case (2) the action of S_n defining the progenitor is the action of S_n on the 2-element subsets of X and in case (3) the action of S_n defining the progenitor is the action of S_n on the 3-element subsets of X.

We note that case (1) of this Theorem is an essentially 'classical' result and has been noted by several authors before, see for instance, Bradley [7, Example 1.2, p.7], Bray [8, Example 1.3.1, p.5], Curtis [28, Section 3.1, p.63] or Whyte [63, p.4]. We include it here for completeness as well as its usefulness in motivating the relations we use in the larger cases and in the 'near Coxeter' cases discussed in Section 3.8.

We further note that case (3) in the cases $n = 6$ and $n = 7$ are closely related to traditional presentations for these groups. The connection with symmetric generation in these cases was first investigated by Sayed [53, p.22]. Our result is, however, more uniform, better motivated and extends to both the case $n = 8$ and the other simply laced Coxeter groups more naturally.

More suggestively we can express these symmetric presentations as Coxeter diagrams as given in Figure II. (Notice that from the presentations given in this Theorem, without even drawing any Coxeter diagrams, the exceptional coincidences of D_3=A_3 and E_5=D_5 are immediate since $\binom{3}{2} = \binom{3}{1}$ and $\binom{5}{3} = \binom{5}{2}$).

We remark that the natural pattern of applying the relation $(t_{1,\ldots,k}(k, k+1))^3$ to the progenitor $2^{\star\binom{n}{k}} : S_n$ to produce a finite image does not extend further. In [14], Bray, Curtis, Parker and Wiedorn prove the symmetric presentation:

$$\frac{2^{\star\binom{n}{4}} : \mathrm{S}_8}{(t_{1,2,3,4}(45))^3, t_{1,2,3,4}t_{5,6,7,8}} \cong W(\mathrm{E}_7) \cong \mathrm{S}_6(2) \times 2.$$

The second relation, which simply identifies a 4-element subset with its compliment so that the symmetric generators correspond to partitions of the eight points into two fours,

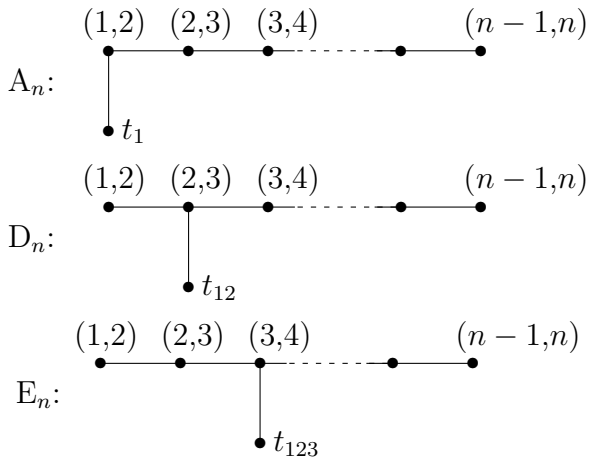


Figure II: Symmetric presentations as Coxeter diagrams.

is necessary for the coset enumeration to terminate; hence the pattern does not continue when the control group is the full symmetric group however using a control group smaller than the full symmetric group can resolve this problem. For instance in [60], Wiedorn proves by hand the symmetric presentation

$$\frac{2^{\star 5} : \mathrm{A}_5}{(t_1(1,2,3,4,5))^7} \cong \mathrm{J}_1$$

where J_1 is the sporadic first Janko group [19, p.36]. Since $\mathrm{S}_5 \not\leqslant \mathrm{J}_1$ using the full symmetric group as a control group instead cannot be used to define J_1. Indeed the image of the control group of the progenitor $2^{\star 5} : \mathrm{S}_5$ when factored by the above relation is not faithful.

3.3 Motivating the Relations

In this section we motivate the relations appearing in the statement of Theorem 3.1.

3.3.1 A_n

Motivated by the Famous Lemma we consider $Stab_{S_n}(1,2)$ for $n \geqslant 2$ and find that

$$Stab_{S_n}(1,2) = \begin{cases} \langle id \rangle & \text{if } n \in \{2,3\}; \\ \langle (3,4),(3,\ldots,n) \rangle & \text{if } n \geqslant 4. \end{cases}$$

We thus find that the corresponding centralizers are

$$C_{S_n}(Stab_{S_n}(1,2)) = \begin{cases} \langle (1,2) \rangle & \text{if } n = 2 \text{ or } n \geqslant 5; \\ \langle (1,2,3),(1,2) \rangle & \text{if } n = 3; \\ \langle (1,2),(3,4) \rangle & \text{if } n = 4. \end{cases}$$

The Famous Lemma now tells us that for generic n the only non-trivial element of S_n that may be expressed in terms of the symmetric generators t_1 and t_2 is the permutation $(1,2)$. The Second Parity Lemma now tells us that the shortest possible relation that we can factor the progenitor $2^{\star n}: S_n$ by to obtain a non-trivial homomorphic image is the relation $(t_1(1,2))^3$.

We shall return to the smaller exceptional cases in Section 3.8.

3.3.2 D_n

Given the relation we arrived at when considering the type A_n progenitors we shall consider subsets of size two that intersect in one point. Motivated by the Famous Lemma we consider $Stab_{S_n}(12,13)$ for $n \geqslant 4$ and find that

$$Stab_{S_n}(12,13) = \begin{cases} \langle id \rangle & \text{if } n = 4; \\ \langle (4,5),(4,\ldots,n) \rangle & \text{if } n \geqslant 5. \end{cases}$$

We thus find that the corresponding centralizers are

$$C_{S_n}(Stab_{S_n}(12,13)) = \begin{cases} \langle (1,2),(1,2,3,4)\rangle & \text{if } n = 4; \\ \langle (1,2),(1,2,3),(4,5)\rangle & \text{if } n = 5; \\ \langle (1,2),(1,2,3)\rangle & \text{if } n \geqslant 6. \end{cases}$$

The Famous Lemma now tells us that for generic n the only non-trivial element of S_n that may be expressed in terms of the symmetric generators $t_{1,2}$ and $t_{1,3}$ is any permutation from the group $\langle (1,2),(1,2,3)\rangle$. Given the relation that we arrived at when considering the type A_n progenitor we consider relations defined by the permutation (2,3). The Second Parity Lemma tells us that the shortest possible relation that we can factor the progenitor $2^{\star\binom{n}{2}} : S_n$ by to obtain a non-trivial homomorphic image is the relation $(t_{1,2}(2,3))^3$.

We shall return to the smaller exceptional cases in Section 3.8.

3.3.3 E_n

Given the relation we arrived at when considering the progenitors of type A_n and type D_n we shall consider subsets of size three that intersect in two points. Motivated by the Famous Lemma we consider $Stab_{S_n}(123,124)$ for $n \geqslant 6$ and find that

$$Stab_{S_n}(123,124) = \begin{cases} \langle (1,2),(5,6)\rangle & \text{if } n = 6; \\ \langle (1,2),(5,\ldots,n),(5,6)\rangle & \text{if } n \geqslant 7. \end{cases}$$

We thus find that the corresponding centralizers are

$$C_{S_n}(Stab_{S_n}(123,124)) = \begin{cases} \langle (1,2),(3,4),(5,6)\rangle & \text{if } n = 6; \\ \langle (1,2),(3,4)\rangle & \text{if } n \geqslant 7. \end{cases}$$

The Famous Lemma now tells us that for generic n the only non-trivial elements of S_n that may be expressed in terms of the symmetric generators $t_{1,2,3}$ and $t_{1,2,4}$ are per-

mutations from the group $\langle (1,2),(3,4),(5,\ldots,n)\rangle$. Given the relations that we arrived at when considering the progenitors type A_n and type D_n we consider relations defined by the permutation (3,4). The Second Parity Lemma tells us that the shortest possible relation that we can factor the progenitor $2^{\star\binom{n}{3}}: S_n$ by to obtain a non-trivial homomorphic image is the relation $(t_{1,2,3}(3,4))^3$.

We shall return to the small exceptional case in Section 3.8.

3.4 Double Coset Enumerations

Recall that S_n is the symmetric group acting on n objects. The high transitivity of the natural action of S_n on n objects enables us to form the progenitors $\mathcal{P}_1{:=}2^{\star\binom{n}{1}}: S_n$, $\mathcal{P}_2{:=}2^{\star\binom{n}{2}}: S_n$ and $\mathcal{P}_3{:=}2^{\star\binom{n}{3}}: S_n$.

To prove that the homomorphic images appearing in Theorem 3.1 are finite we shall perform a double coset enumeration in each case.

If we presuppose the result of Theorem 3.1 then there is a well developed theory of double cosets in Coxeter groups already in existence that may be used to perform the double coset enumerations (see [1, Section 2.3] for further details). Since the emphasis of this chapter is to derive the classical Coxeter-Moser presentations associated with all the finite simply laced Coxeter groups in a natural manner and with the barest minimum of technical machinery (and since we do not know that the groups defined by the symmetric presentations appearing in Theorem 3.1 are even Coxeter groups until the proof is complete), we will avoid this instead performing our double coset enumerations by hand as far as possible.

(As a 'nod' in the direction of the general theory, however, we note that that control group in each case is a parabolic subgroup for the following reasons. The derived subgroup of the progenitor $\mathcal{P}_i$ for $i = 1, 2, 3$ is given by

$$\mathcal{P}_i' = \{\pi w | \pi \text{ is an even permutation and } l(w) \text{ is even}\}.$$

Since the control group contains odd permutations in each case it cannot be contained in the derived subgroup of $\mathcal{P}_i$ and so the image of the control group cannot be contained in the image of the derived subgroup.

Now, in any matrix representation of any group a commutator will always have determinant 1. By definition, any reflection will have determinant -1 in the defining representation of any group containing it. Let G be a Coxeter group. Since any parabolic subgroup of G must contain reflections it follows that any parabolic subgroup of G cannot be contained in the derived subgroup of G. In each of the groups $W(E_n)$ with $n = 6, 7$ there are only two classes of subgroups isomorphic to S_n - one contained in the derived subgroup the other not, since they are contained in a maximal subgroup isomorphic to $2 \times S_n$ in each case (the list of maximal subgroups of each of the finite Weyl groups of type $W(E_n)$ may be deduced from the information found in the ATLAS [19, p.26, p.46, p.85]). The copy of S_n not contained in the derived subgroup must therefore be a parabolic subgroup and in particular must be our control group. In the derived subgroup of $W(\mathrm{E}_8)$ there are no copies of S_8 so similarly the control group is the parabolic subgroup. Similarly, in each of the cases $W(A_n)$ and $W(D_n)$ the control group is a parabolic subgroup.)

3.4.1 A_n

For $\mathcal{P}_1$ we enumerate the double cosets $S_n w S_n$ by hand. Since $t_i t_j = (i, j) t_i$ for $i, j \in \{1, \ldots, n\}$, $i \neq j$, any coset representative must have length at most 1. Since $S_n^{(t_1)} \cong S_{n-1}$, we have that $|S_n \colon S_n^{(t_1)}| = n$ and $|S_n \colon S_n^{(\star)}| = 1$, so the target group must contain the image of S_n to index at most $n + 1$.

3.4.2 D_n

We shall prove:

Lemma 3.2 The representatives for the double cosets $S_n w S_n$ with w a word in the symmetric generators are in one-to-one correspondence with the subsets of $\{1 \ldots n\}$ of

even cardinality. We thus have $|W(D_n) : S_n| = 2^{n-1}$.

We shall prove this by using the following two lemmata.

Lemma 3.3 Any coset representative of the form $t_{1,2} \dots t_{i,j} \dots t_{i,k} \dots t_{m,n}$ collapses to a representative of shorter length and so any coset representative containing a subword of this form will also shorten.

Proof. Clearly repetition cannot occur in words of length one. The relation immediately shortens words of length 2 of this form. We prove the result for words of length three, the argument for longer words being entirely analogous. By the high transitivity of the action of S_n on n points we may assume that our word has the form $t_{1,2}t_{3,4}t_{1,5}$ (if the repeated indices were in adjacent symmetric generators, the relation would immediately shorten it). Now,

$$t_{1,2}t_{3,4}t_{1,5} = t_{1,2}t_{3,4}t_{1,3}^2t_{1,5} = t_{1,2}((1,4)t_{3,4})((3,5)t_{1,3}) = (1,4)(3,5)t_{2,4}t_{4,5}t_{1,3} \sim t_{2,4}t_{1,3}.$$

□

Lemma 3.4 $t_{1,2}t_{3,4} \sim t_{1,3}t_{2,4}$
Proof.

$$t_{1,2}t_{3,4} = t_{1,2}t_{3,4}t_{2,4}^2 = t_{1,2}(2,3)t_{3,4}t_{2,4} = (2,3)t_{1,3}t_{3,4}t_{2,4} = (2,3)(1,4)t_{1,3}t_{2,4} \sim t_{1,3}t_{2,4}.$$

□

Proof of lemma 3.2 By Lemma 3.3 the indices appearing in any coset representative must be distinct. By Lemma 3.4 the indices appearing in a coset representative of length 2 may be reordered, noting that the permutation being pulled through the word of the symmetric generators in the proof of Lemma 3.4 does not affect indices other than those being reordered. Since the indices are all distinct it follows that the indices appearing in a coset representative of any length may be reordered. The double cosets must therefore be $[\star]$, $[t_{1,2}]$,...,$[t_{1,2} \dots t_{2k-1,2k}]$ where k is the largest integer such that $2k \leqslant n$. □

3.4.3 E_6

The coset enumeration in this case may also be performed by hand. We list the cosets in Table VI. Not every case is considered in this table, however all remaining cases may be deduced from them as follows. Since $t_{1,2,3}t_{1,4,5} \sim t_{1,2,4}t_{1,3,5}$ the S_4 permutating these indices ensures that for any three element subset $\{a,b,c\} \subset \{1,\ldots,6\}$ the word $t_{1,2,3}t_{1,4,5}t_{a,b,c}$ will shorten. Since the only non-collapsing word of length 3 is of the form $t_{1,2,3}t_{4,5,6}t_{1,2,3}$ and $t_{1,2,3}t_{4,5,6}t_{1,2,3} \sim t_{1,2,4}t_{3,5,6}t_{1,2,4}$ the S_6 permuting these indices ensures that for any three element subset $\{a,b,c\} \subset \{1,\ldots,6\}$ the word $t_{1,2,3}t_{4,5,6}t_{1,2,3}t_{a,b,c}$ will shorten and so all words of length 4 shorten.

From this double coset enumeration we see that $|W(\mathrm{E}_6) : \mathrm{S}_6| \leqslant 1{+}20{+}30{+}20{+}1 = 72$. Our target group must therefore have order at most $72 \times |\mathrm{S}_6| = 51840$.

Table VI: The coset enumeration for E_6

Label $[w]$	Coset Stabilising subgroup	Number of Cosets
$[\star]$	N	1
$[t_{1,2,3}]$	$N^{(t_{1,2,3})} \cong \mathrm{S}_3{\times}\mathrm{S}_3$	20
$[t_{1,2,3}t_{1,4,5}]$	$N^{(t_{1,2,3}t_{1,4,5})} \cong \mathrm{S}_4$ since	30
	$t_{1,2,3}t_{1,4,5} = t_{1,2,3}t_{1,2,4}^2t_{1,4,5} \sim t_{1,2,3}(2,5)t_{1,2,4} \sim t_{1,3,5}t_{1,2,4}$	
$[t_{1,2,3}t_{4,5,6}]$	$N^{(t_{1,2,3}t_{4,5,6})} \cong \mathrm{S}_3{\times}\mathrm{S}_3$ since	20
$[t_{1,2,3}t_{4,5,6}t_{1,2,4}]$	$t_{1,2,3}t_{4,5,6}t_{1,2,4} = t_{1,2,3}t_{4,5,6}t_{1,4,5}^2t_{1,2,4}$	
$=[t_{3,5,6}t_{2,4,5}]$	$= t_{1,2,3}(1,6)t_{4,5,6}(2,5)t_{1,4,5}$	
	$\sim t_{3,5,6}t_{2,4,5}t_{1,4,5}$	
	$\sim t_{3,5,6}t_{2,4,5}$	
$[t_{1,2,3}t_{4,5,6}t_{1,2,3}]$	$N^{(t_{1,2,3}t_{4,5,6}t_{1,2,3})} \cong \mathrm{S}_6$ since	1
	$t_{1,2,3}t_{4,5,6}t_{1,2,3} = t_{1,2,3}(3,4)t_{4,5,6}t_{3,5,6}t_{1,2,3}$	
	$\sim t_{1,2,3}(3,4)t_{4,5,6}t_{3,5,6}t_{2,3,5}^2t_{1,2,3}$	
	$= t_{1,2,4}t_{4,5,6}(2,6)t_{3,5,6}(1,5)t_{2,3,5}$	
	$= t_{4,5,6}t_{1,2,4}t_{1,3,6}t_{2,3,5}$	
	$= t_{4,5,6}t_{1,4,6}^2t_{1,2,4}t_{1,3,6}t_{2,3,5}$	
	$= (1,5)t_{4,5,6}(6,2)t_{1,4,6}t_{1,3,6}t_{2,3,5}$	
	$= t_{2,4,5}t_{1,4,6}t_{1,3,6}t_{2,3,5}$	
	$= t_{2,4,5}(3,4)t_{1,4,6}t_{2,3,5}$	
	$\sim t_{2,3,5}t_{1,4,6}t_{2,3,5}$	

3.4.4 $\mathbf{E}_7$

Unfortunately the index here is too large to enumerate the cosets manually. We therefore resort to using the Double Coset Enumerator as described in Section 1.4.

```
> S:=Sym(7);
> stab:=Stabilizer(S,{1,2,3});
> f,nn,k:=CosetAction(S,stab);
> 1^f(S!(3,4));
22
```

Here we have defined the group S_7 as a permutation group acting on the $\binom{7}{3}$ subsets of size 3. The computer has labeled the set $\{1,2,3\}$ with the number 1 and the set $\{1,2,4\}$ with the number 22.

```
> RR:=[<[1,22,1],f(S!(4,3))>]; HH:=[nn];
> CT:=DCEnum(nn,RR,HH:Print:=5,Grain:=100);

Index: 576 = Rank: 10 = Edges: 40 = Status: Early closed = Time:
0.150
```

The Double Coset Enumerator has found there there are at most ten distinct double cosets and that $|W(\mathrm{E}_7) : \mathrm{S}_7| \leqslant 576$. Our target group must therefore have order at most $576 \times |\mathrm{S}_7| = 2903040$.

3.4.5 $\mathbf{E}_8$

Again we use the computer to determine the index.

```
> S:=Sym(8);
> stab:=Stabilizer(S,{1,2,3});
> f,nn,k:=CosetAction(S,stab);
```

```
> 1^f(S!(3,4));
28
> RR:=[<[1,28,1],f(S!(4,3))>];
> CT:=DCEnum(nn,RR,nn:Print:=5,Grain:=100);
Index: 17280 = Rank: 35 = Edges: 256 = Status: Early closed = Time:
0.940
```

We see that $|W(\mathrm{E}_8) : \mathrm{S}_8| \leqslant 17280$. Our target group must therefore have order at most $17280 \times |\mathrm{S}_8| = 696729600$.

We remark that here we have established our symmetric presentations by the traditional method of enumerating double cosets. Since simply laced Coxeter groups are generated by a class of involutions whose products have order at most 3 (and are therefore Fischer groups), we could have employed the methods previously used by Bray, Curtis, Parker and Wierdorn to establish symmetric presentations of the sporadic Fischer groups (see [14, 15]). More specifically, Theorem 2.1 of [15] (itself a 'progenitor form' of a result due to to Virotte-Ducharme, [59]) enables us to count the number of involutions of our target groups and in doing so verify their orders.

3.5 Representations

In this section we use the symmetric presentations of Theorem 3.1 to construct representations of the target groups and in doing so verifying have the structures that we claim. In the A_n and D_n cases this is sufficient to show that the groups are what we expect them to be.

3.5.1 A_n

Since these groups are most naturally viewed as permutation groups we shall construct the natural permutation representation. The lowest degree of a permutation representation in which the control group, S_n, acts faithfully is n, so the lowest degree of a permutation representation in which the target group acts faithfully is n. Since the control group already

contains all possible permutations of n objects, the target group must be a permutation group acting on at least $n+1$ objects. A permutation corresponding to a symmetric generator must commute with the centralizer in the control group of a symmetric generator, namely a copy of S_{n-1}. There is only one permutation that satisfies this namely $t_i = (i, n+1)$. Since this has order 2 and satisfies the relation we must therefore have that our target group is isomorphic to S_{n+1}.

3.5.2 D_n

We shall use our symmetric generators to construct an elementary abelian 2-group lying outside our control group and thus verify that our target group has structure $2^{n-1} : \mathrm{S}_n$.

Lemma 3.5 $t_{1,2}t_{3,4} = t_{3,4}t_{1,2}$
Proof.

$$t_{1,2}t_{3,4}t_{1,2} = t_{1,2}t_{3,4}t_{1,3}^2t_{1,2} = t_{1,2}(14)t_{3,4}(23)t_{1,3} = (14)(23)t_{3,4}t_{2,4}t_{1,3} = (14)(t_{3,4}t_{2,4})t_{2,4}t_{1,3} = t_{3,4}$$

□

Lemma 3.6 The elements $e_{ij} := (i,j)t_{ij}$ generate an elementary abelian 2-group of order 2^{n-1}.

Proof. If $i, j \notin \{k, l\}$, $i \neq j$ and $k \neq l$ then by Lemma 3.2 $e_{i,j}e_{k,l} = e_{k,l}e_{i,j}$. Suppose $i = l$, then

$$\begin{aligned}
e_{i,j}e_{i,k}e_{i,j}e_{i,k} &= (i,j)t_{i,j}(i,k)t_{i,k}(i,j)t_{i,j}(i,k)t_{i,k} \\
&= (i,j)(i,k)(i,j)(i,k)t_{i,k}t_{i,j}t_{j,k}t_{i,k} \\
&= (i,j)(i,k)(i,j)(i,k)(j,k)t_{i,k}t_{j,k}t_{i,k} \\
&= (i,j)(i,k)(i,j)(i,k)(j,k)(i,j) \\
&= id
\end{aligned}$$

□

Since the $e_{i,j}$ generate an elementary abelian 2-group we represent the elements $e_{i,j}$ as diagonal matrices with -1 entries in the i and j positions. Using the natural n-dimensional representation of S_n as permutation matrices we thus have:

$$t_{1,2} = \begin{pmatrix} & -1 & & & \\ -1 & & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}.$$

We note that for each of the type D_n Coxeter groups, the root system traditionally associated with these groups may be readily recovered from here by observing that the -1 eigenvectors of the matrices obtained for the symmetric generators in each of these cases has the form $(1^2, 0^{n-2})$. Further noting that

$$\begin{array}{rccccc} & (1 & 1 & 0 & \dots & 0) \\ - & (1 & 0 & 1 & \dots & 0) \\ \hline & (0 & 1 & -1 & \dots & 0), \end{array}$$

allows us to obtain all the root vectors of the root system associated with the control group and thus gives us the whole root system of type D_n.

3.5.3 $\mathbf{E}_6$

In the case of the Weyl group of type E_6 we shall first construct a six dimensional ordinary representation in which the action of the control group is given by permutation matrices. In any representation of a symmetrically generated group, the matrix used to represent a symmetric generator is (helpfully) compelled to satisfy each of the following three conditions.

1. commute with the stabilizer of a symmetric generator;
2. have order 2;
3. satisfy the relation.

By condition 1 such a matrix must be of the form

$$t_{1,2,3} = \left(\begin{array}{c|c} aI_3 + bJ_3 & cJ_3 \\ \hline c'J_3 & a'I_3 + b'J_3 \end{array}\right)$$

where I_3 denotes the 3×3 identity matrix and J_3 denotes a 3×3 matrix all the entries of that equal 1. Now condition 2 tells us that

$$(aI_3 + bJ_3)^2 + 3cc'J_3 = (a'I_3 + b'J_3)^2 + 3cc'J_3 = I_3$$

and

$$c'J_3(aI_3 + bJ_3 + a'I_3 + b'J_3) = cJ_3(aI_3 + bJ_3 + a'I_3 + b'J_3) = 0_3$$

which together imply that

$$c(a + a' + 3b + 3b') = c'(a + a' + 3b + 3b') = 0 \qquad (\spadesuit\diamondsuit)$$

$$a^2 = a'^2 = 1 \qquad (\spadesuit\spadesuit)$$

and

$$2ab + 3b^2 + 3cc' = 2a'b' + 3b'^2 + 3cc' = 0. \qquad (\spadesuit\heartsuit)$$

If our control group acts as permutation matrices then condition 3 implies that the determinant of the matrix for the symmetric generators must be -1. Recall that if A, B, C

and D are $n \times n$ matrices then

$$det\left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right) = det(A)det(D) - det(B)det(C).$$

Combined with the fact that

$$\begin{vmatrix} a+b & b & b \\ b & a+b & b \\ b & b & a+b \end{vmatrix} = \begin{vmatrix} a+b & -a & -a \\ b & a & 0 \\ b & 0 & a \end{vmatrix}$$

which, when evaluated along the middle column, gives us

$$a\begin{vmatrix} b & 0 \\ b & a \end{vmatrix} - a\begin{vmatrix} a+b & -a \\ b & a \end{vmatrix} = a^2b + a(a(a+b)+ab) = a+3b$$

since $a^2 = 1$ and so

$$(a+3b)(a'+3b') = -1. \qquad (\spadesuit\clubsuit)$$

More specifically we find condition 3 tells us that the matrix for $t_{123}t_{124}$ and the matrix

$$(3,4)t_{1,2,3} = \begin{pmatrix} a+b & b & b & c & c & c \\ b & a+b & b & c & c & c \\ c' & c' & c' & a'+b' & b' & b' \\ b & b & a+b & c & c & c \\ c' & c' & c' & b' & a'+b' & b' \\ c' & c' & c' & b' & b' & a'+b' \end{pmatrix}$$

must be equal. This tells us that

$$(a+b)^2 + b^2 + bc' + bc + 2cc' = a + b \qquad (\heartsuit\diamondsuit)$$

$$2b(a+b) + bc' + bc + 2cc' = b. \qquad (\heartsuit\spadesuit)$$

and

$$c'(a + 2b + 2b' + c') + b(a' + b') = b. \qquad (\heartsuit\heartsuit)$$

Subtracting equation ($\heartsuit\spadesuit$) from ($\heartsuit\diamondsuit$) now gives us

$$(a+b)^2 + b^2 - 2b(a+b) = a \Rightarrow a^2 = a$$

and so $a = 1$ by equation ($\spadesuit\spadesuit$). Similarly we have $a' = 1$. A natural value of c' to consider, given the relation ($\spadesuit\diamondsuit$), is $c' = 0$. Substituting this into equation ($\heartsuit\diamondsuit$) now tells us that if $b \neq 0$ then $c = -2b - 1$ and substituting $c' = 0$ into equation ($\heartsuit\heartsuit$) tells us that $b(a' + b') = b$. Equation ($\spadesuit\clubsuit$), combined with the fact that $a = a' = 1$ tells us that we cannot have $b = b' = 0$ but from equation ($\spadesuit\heartsuit$), $\{b, b'\} \subset \{0, -2/3\}$. We shall use the value $b \neq 0$ implying that $b = -2/3$ and so $c = 1/3$. We have thus been naturally led to a matrix of the form

$$t_{1,2,3} = \left(\begin{array}{c|c} I_3 - \frac{2}{3}J_3 & \frac{1}{3}J_3 \\ \hline 0_3 & I_3 \end{array}\right)$$

where 0_3 denotes the 3×3 matrix all the entries of which are 0.

The representation of the control group we have used is not irreducible and splits into two irreducible representations namely the subspace spanned by the vector $v{:=}(1^6)$ and the subspace $v^\perp$. The above matrix does not respect this decomposition since it maps the v to a vector of the form $(0^3,1^3)$. Consequently, the above representation of $W(\mathrm{E}_6)$ is

irreducible.

3.5.4 E_7

Using arguments entirely analogous to those appearing in the previous section there is a 7 dimensional representation of $W(\mathrm{E}_7$ in which the control group acts as permutation matrices and we can represent the symmetric generators for $W(\mathrm{E}_7)$ with matrices of the form

$$t_{1,2,3} = \left(\begin{array}{c|c} I_3 - \frac{2}{3}J_3 & \frac{1}{3}J_{3\times 4} \\ \hline 0_{4\times 3} & I_4 \end{array}\right)$$

which again is irreducible.

3.5.5 E_8

Again using arguments entirely analogous to those used in the E_6 case, there is an 8 dimensional representation of $W(\mathrm{E}_8)$ in which the control group acts as permutation matrices and we can represent the symmetric generators for $W(\mathrm{E}_8$ with matrices of the form

$$t_{1,2,3} = \left(\begin{array}{c|c} I_3 - \frac{2}{3}J_3 & \frac{1}{3}J_{3\times 5} \\ \hline 0_{5\times 3} & I_5 \end{array}\right),$$

which again is irreducible.

We note that for each of the type E_n Coxeter groups, the root system traditionally associated with these groups may be readily recovered from here by observing that the -1 eigenvectors of the matrices obtained for the symmetric generators in each of these cases has the form $(1^3, 0^{n-3})$. Further noting that

$$\begin{array}{rcccccc} & (1 & 1 & 1 & 0 & \ldots & 0) \\ - & (1 & 1 & 0 & 1 & \ldots & 0) \\ \hline & (0 & 0 & 1 & \text{-}1 & \ldots & 0), \end{array}$$

allows us to obtain all the root vectors of the root system associated with the control group and thus gives us the whole root system of type E_n, recalling that when considering Coxeter groups we disregard the lengths of the vectors appearing in the root system (unlike many other contexts in which the lengths of the roots matter).

3.6 Some Modular Representations of the Groups $W(\mathbf{E}_6)$, $W(\mathbf{E}_7)$ and $W(\mathbf{E}_8)$

In this section we use the matrices obtained in Section 3.5 for representing E_6, E_7 and E_8 to exhibit representations of these groups over $\mathbb{F}_2$ and in doing so we identify the structure of the groups in question.

3.6.1 $\mathbf{E}_6$

Multiplying each of the matrices representing our symmetric generators found in the last section by 3 ($\equiv$1 (mod 2)) we find that these matrices, working over $\mathbb{F}_2$, are of the form:

$$t_{1,2,3} = \left(\begin{array}{c|c} I_3 & J_3 \\ \hline 0_3 & I_3 \end{array}\right).$$

These matrices still satisfy the relation and the representation is still irreducible for much the same reason as in the real case as is easily verified by Magma. (We note that the representations of the control groups used here are not irreducible as they are each the direct sum of the Specht modules corresponding to the partitions $(n) \vdash n$ and $(n-1,1) \vdash n$. As ever, in characteristic 0 these Specht modules are irreducible but since each of these partitions are 2-regular, these modules are also irreducible in characteristic 2. See James, [47], for details.) Consequently we see the isomorphism $W(\mathrm{E}_6) \cong \mathrm{O}_6^-(2)$:2 since all of our matrices preserve the non-singular quadratic form $\sum_{i \neq j} x_i x_j$.

3.6.2 $\mathbf{E}_7$

Similarly we obtain a representation of $2\times \mathrm{O}_7(2)$ in the E_7 case, accepting that the central involution must clearly act trivially here. In this case the matrices preserve the non-singular quadratic form defined by $\sum_{i\neq j} x_i x_j + \sum_i x_i^2$.

From the Atlas of Brauer Characters [46, p.110] we see that there is no irreducible $\mathbb{F}_2$ representation of $\mathrm{O}_7(2)$ in 7 dimensions and this is precisely what we find here. The matrices for the symmetric generators and the whole of the control group fix the vector $v := (1^7)$. The space $v^\perp$ thus gives us a 6 dimensional $\mathbb{F}_2$-module for this group to act on. It may be easily verified that this representation is irreducible either with the aid of Magma or by the observation that this module as a representation of the control group is isomorphic to the Specht module corresponding to the partition $(6,1) \vdash 7$ and is therefore an irreducible representation of the subgroup isomorphic to S_7.

Since the above form is symplectic when restricted to this subspace we immediately have that $\mathrm{O}_7(2) \cong \mathrm{S}_6(2)$.

(It is worth noting that in the E_6 and E_7 cases the symmetric generators may be interpreted as 'bifid maps' acting on the 27 lines of Schläfli's general cubic surface and Hesse's 28 bitangents to the plane quartic curve respectively. See the Atlas [19, p.26 and p.46] for details. These in turn have provided the symmetric generators of symmetric presentations before. More specifically

$$\frac{2^{\star\binom{8}{4}} : \mathrm{S}_8}{(t_{1,2,3,4}(4,5))^3, (1,2)(3,4)(5,6)(7,8)t_{1,2,3,4}t_{1,2,5,6}t_{1,2,7,8}} \cong \mathrm{S}_6(2).$$

Here we have written the symmetric generators using the more modern notation commonly used in symmetric presentations. Cayley's original notation indexed the bitangents with $\binom{8}{2} = 28$ pairs of points and is thus able to express the bifid maps as permutations on 28

points as follows

$$t_{a,b,c,d} \equiv \frac{a,b,c,d}{e,f,g,h} := (ab,cd)(ac,bd)(ad,bc)(ef,gh)(eg,fh)(eh,fg)$$

See [43] for details.)

3.6.3 E_8

Similarly we obtain a representation of $2\dot{}\mathrm{O}_8^+(2)$ in the E_8 case, again accepting that the central involution must clearly act trivially. Like the E_6 case the matrices preserve the non-singular quadratic form $\sum_{i\neq j} x_i x_j$.

Notice that working in an even number of dimensions removes the irreducibility problem encountered with E_7 since the image of (1^8) under the action of a symmetric generator is of the form $(0^3,1^5)$.

We note that instead of multiplying by $3(\equiv 1 \pmod 2)$ we could have multiplied by $6(\equiv 1 \pmod 5)$ obtaining representations over the field of five elements. In each case these representations are irreducible, but reveal less about the structure of the groups in question.

Finally we note that each of the 6 dimensional $\mathbb{F}_2$-modules of $W(\mathrm{E}_6)$ and $W(\mathrm{E}_7)$ along with the 8 dimensional $\mathbb{F}_2$-module of $W(\mathrm{E}_8)$ are all easily seen to be absolutely irreducible, that is, they do not become reducible if $\mathbb{F}_2$ is extended to a larger field. For instance, in the case of $W(\mathrm{E}_6)$, if the 6 dimensional module was not irreducible, then it would split into two 3 dimensional $\mathbb{F}_4$-modules or into three 2 dimensional $\mathbb{F}_8$-modules. Since $W(\mathrm{E}_6) \not\leqslant \mathrm{SL}_2(8)$ and $W(\mathrm{E}_6) \not\leqslant \mathrm{SL}_3(4)$ this cannot happen. Alternatively this may be seen by consulting the $\mathbb{F}_2$ Brauer character tables given in [46, p.60, p.110 and p.232]. Similarly the n dimensional $\mathbb{F}_5$-modules for $W(E_n)$ alluded to above are also absolutely irreducible.

3.7 Other Coxeter Groups

Here we focused our attention on the simply laced finite Coxeter groups and obtained symmetric presentations by using an 'end node' of the Coxeter diagram and the remaining nodes to generate the control group. Analogous results may be obtained for other Coxeter groups by using almost any node of any Coxeter diagram, though the representations produced would be of a much more cumbersome nature and require more than one relation to produce a finite homomorphic image making them much less natural and thus more difficult to motivate. For example:

$$\frac{2^{\star 2n} : W(B_{n-1})}{(t_1(12)(n+1,n+2))^3} \cong W(B_n)$$

$$\frac{2^{\star n} : S_n}{(t_1(12))^5} \cong W(H_n) \text{ for } n = 3, 4.$$

Furthermore, the author's recent work with Jürgen Müller extends these ideas to finding symmetric presentations for both finite and infinite Coxeter groups satisfying certain finiteness conditions in general. See [40] for details.

3.8 Some 'Near' Coxeter Groups

On a philosophical note, one view of the existence of the sporadic simple groups is that 'bad behaviour breeds bad behaviour'. The smaller members of the 'well behaved' infinite families of simple groups often lack the size necessary to behave as their larger brethren do. This often leads to unusual behaviour such as exceptional automorphism groups (as we find with A_6 for example); exceptional Schur multipliers (as we find with A_7 for example) or exceptional actions on an unusual number of points (as we find with $\mathrm{L}_2(11)$ for example). These examples of 'bad' behaviour give rise to the existence of sporadic groups. The smaller sporadic groups in turn giving rise to the larger ones. More intriguingly, we

find that the existence of sporadic groups in turn breeds bad behaviour among objects found elsewhere in mathematics, such as the exceptional Steiner systems related to the Mathieu groups; the exceptional sphere packing known as the Leech lattice related to the Conway groups or the mysterious 'Monster Moonshine' results related to the Monster.

It is for this reason that exceptional cases such as those appearing in the analysis of Section 3.3 demand further investigation, which we discuss in this section. Several of the symmetric presentations we shall encounter are not new, but previous considerations of them have tended to do little to motivate them quite as naturally as we have here.

3.8.1 $\mathbf{A}_2$

Recall from Section 3.3.1 $Stab_{\mathrm{S}_3}(1,2) = \langle id \rangle$, and so $C_{\mathrm{S}_3}(Stab_{\mathrm{S}_3}(1,2)) = \mathrm{S}_3$. Furthermore $Stab_{\mathrm{S}_3}(1,2)$ fixes all three points and so the Extended Famous Lemma tells us that equating any word in all three symmetric generators with any element of S_3 is a permissable relation to factor by. This situation was investigated thoroughly by Curtis, Hammas and Bray as part of their 'systematic approach' (see [31, 9]) and as a consequence numerous homomorphic images of the progenitor $2^{\star\binom{3}{1}} : \mathrm{S}_3$ may be found in [31, Table 3]. Consequently we shall say no more about this case here.

3.8.2 $\mathbf{A}_3$

Recall from Section 3.3.1 that $Stab_{\mathrm{S}_4}(1,2) = \langle (3,4) \rangle$ and so $C_{\mathrm{S}_4}(Stab_{\mathrm{S}_4}(1,2)) = \langle (1,2),(3,4) \rangle$. We therefore have three possibilities for a non-trivial relation: a word in t_1 and t_2 is equal to one of (1,2), (1,2)(3,4) or (3,4). The shortest relation defined by the first of these gives the Coxeter group $W(\mathrm{A}_3)$. For the second possibility we note that the action defining this progenitor is primitive and so the Primitive Lemma tells us that the shortest word we should consider has length 3. Unfortunately we are compelled to prove the following

Lemma 3.7 The image of the control group in the factored progenitor

$$\frac{2^{\star 4}\colon \mathrm{S}_4}{(t_1(1,2)(3,4))^3}$$

is not faithful.

Proof. From the relation, we have $t_1 = (12)(34)t_1t_2 = (13)(24)t_1t_3$, which implies that $(14)(23) = t_1t_3t_2t_1$. The relation also gives us that $t_1t_4t_1 = (14)(23)$ and so $t_1t_4t_1 = t_1t_3t_2t_1$. Cancelation gives

$$t_4 = t_3t_2 \qquad (\clubsuit\diamondsuit)$$

Now the relation also tells us that $t_2t_3t_2 = (1,4)(2,3)$ and so $t_3t_2 = t_2(1,4)(2,3)$. Equating with $(\clubsuit\diamondsuit)$ tells us that $(1,4)(2,3) = t_2t_4$. Since one side of this equation is fixed by the action of the permutation (1,3) we have that

$$(1,4)(2,3) = t_2t_4 = (t_2t_4)^{(1,3)} = (1,4)(2,3)^{(1,3)} = (1,3)(2,4),$$

and so $(1,2)(3,4) = id$. □

Now by the Second Parity Lemma the next shortest word to consider is $(t_1(1,2)(3,4))^5$. We have thus been naturally led to the symmetric presentation given in Curtis, [28, p.77],

$$\frac{2^{\star 4}\colon \mathrm{S}_4}{(t_1(1,2)(3,4))^5} \cong (3 \times \mathrm{L}_2(11)).2.$$

The final case to consider is the permutation (3,4). This time the parity Lemma forces us to consider words of even length and since the action defining the progenitor is primitive the Primitive Lemma naturally leads us to the relation $(t_1t_2)^2 = (3,4)$. Again the symmetric presentation this defines was met 'in passing' during the systematic approach

of Curtis, Bray and Hammas and may be found in [31, Table 5] namely

$$\frac{2^{\star 4}\colon \mathrm{S}_4}{(t_1t_2)^2 = (3,4)} \cong \mathrm{PGL}_2(7).$$

3.8.3 D_4

As with the A_2 case, $Stab_{\mathrm{S}_4}(12,13) = \langle id \rangle$, and so $C_{\mathrm{S}_4}(Stab_{\mathrm{S}_4}(12,13)) = \mathrm{S}_4$. Furthermore $Stab_{\mathrm{S}_4}(12,13)$ fixes all four points and thus all six symmetric generators. By the Extended Famous Lemma equating any word involving t_{12} and t_{13} (and possibly other generators too) with any element of S_4 is a permissable relation to factor by. (Note also that in this case the action defining the progenitor is not primitive, so words of length 2 are possible.)

It turns out that even after a systematic search for interesting homomorphic images, few images arise. Several interesting images in which the image of the control group is not faithful are possible as well as numerous soluble groups, but given our emphasis on faithful images we shall not list these here.

3.8.4 D_5

Recall from Section 3.3.2 that $Stab_{\mathrm{S}_5}(12,13) = \langle (4,5) \rangle$, and so $C_{\mathrm{S}_5}(Stab_{\mathrm{S}_5}(12,13)) = \langle (1,2),(1,2,3),(4,5) \rangle$. Given the presentations we were led to in the A_3 case it is natural to consider words in the symmetric generators $t_{1,2}$ and $t_{1,3}$ equal to the (again permissible) permutations (2,3), (4,5) and (2,3)(4,5). Again, the shortest relation defined by the first of these gives the Coxeter group $W(\mathrm{D}_5)$.

The action defining the progenitor $2^{\star\binom{5}{2}} : \mathrm{S}_5$ is primitive, thus by the Primitive Lemma the shortest word in the symmetric generators we should consider have length at least 3. Since the permutation (4,5) fixes both of the symmetric generators, the only words in the symmetric generators $t_{1,2}$ and $t_{1,3}$ that can equal (4,5) must have even length, naturally leading us to the relation $(4,5) = (t_{1,2}t_{1,3})^2$. Unfortunately, factoring by this relation alone

does not produce a finite group. Attempts to find additional relations that produce finite homomorphic images in this case have produced too few results to merit tabulation.

The final case to consider is the permutation (2,3)(4,5). Again the Parity Lemma tells us that the shortest relation to consider is $(t_{1,2}(2,3)(4,5))^3$. A result analogous to Lemma 3.7 that we used when considering A_3 (and with entirely analogous proof) is the following.

Lemma 3.8 The image of the control group in the factored progenitor

$$\frac{2^{\star\binom{5}{2}} : S_5}{(t_{1,2}(23)(45))^3}$$

is not faithful.

Proof. From the relation, we have $t_{1,2} = (2,3)(4,5)t_{1,2}t_{1,3} = (2,4)(3,5)t_{1,2}t_{1,4}$, which implies that $(2,5)(3,4) = t_{1,2}t_{1,4}t_{1,3}t_{1,2}$. The relation also gives us that $t_{1,2}t_{1,5}t_{1,2} = (2,5)(3,4)$ and so $t_{1,2}t_{1,5}t_{1,2} = t_{1,2}t_{1,4}t_{1,3}t_{1,2}$. Cancelation now gives

$$t_{1,5} = t_{1,4}t_{1,3} \qquad (\clubsuit\spadesuit)$$

Now the relation also tells us that $t_{1,3}t_{1,4}t_{1,3} = (2,5)(3,4)$ and so $t_{1,4}t_{1,3} = t_{1,3}(2,5)(3,4)$. Equating with $(\clubsuit\spadesuit)$ tells us that $(2,5)(3,4) = t_{1,5}t_{1,3}$. Since one side of this equation is fixed by the action of the permutation (2,4) we have that

$$(2,5)(3,4) = t_{1,5}t_{1,3} = (t_{1,5}t_{1,3})^{(2,4)} = (2,5)(3,4)^{(2,4)} = (2,3)(4,5),$$

and so $(2,4)(3,5) = id$. □

Now by the Second Parity Lemma the next shortest word to consider is $(t_{1,2}(2,3)(4,5))^5$. Unlike the A_3 case we find that the coset enumeration in this case appears to not terminate, telling us that either we have a symmetric presentation of a group in which there

are too many double cosets to easily enumerate or the group is still infinite and further relations are required to produce a finite group. We search for further relations.

Since the relation $(t_{1,2}(2,3)(4,5))^5$ gives a relationship between symmetric generators defined by pairs that intersect we consider the relationship between disjoint pairs. Applying the Famous Lemma to such a pair we find that $Stab_{\mathrm{S}_5}(12,34) = \langle (1,2),(3,4)\rangle$ and so $C_{\mathrm{S}_5}(Stab_{\mathrm{S}_5}(12,34)) = \langle (1,2),(3,4)\rangle$. We thus have that the only relations of the form $w(t_{1,2},t_{3,4}) = \pi$ that can we can sensibly factor by must have even length by the Second Parity Lemma, since π must fix both symmetric generators, whichever π we use. Again the action defining the progenitor is primitive and so a relation of length 2 cannot be used by the Primitive Lemma. The shortest additional relation we can sensibly consider is therefore of the form $(t_{1,2}t_{3,4})^2 = \pi \in \langle (1,2),(3,4)\rangle$. We first prove the following result.

Lemma 3.9 The image of the control group in the factored progenitor

$$\frac{2^{\star\binom{5}{2}} : \mathrm{S}_5}{(t_{1,2}t_{3,4})^2 = (1,2)}$$

is not faithful.

Proof. Observe that $(1,2) = (1,2)^{-1} = (t_{1,2}t_{3,4})^{-2} = ((t_{1,2}t_{3,4})^2)^{(1,3)(2,4)} = (1,2)^{(1,3)(2,4)} = (34)$, which implies that $(1,2)(3,4) = id$. □

Clearly there is an analogous result replacing the permutation (1,2) with the permutation (3,4) that also holds. We thus consider the relation $(t_{1,2}t_{3,4})^2 = (1,2)(3,4)$.

Lemma 3.10 The image of the control group in the factored progenitor

$$\frac{2^{\star\binom{5}{2}} : \mathrm{S}_5}{(t_{1,2}(2,3)(4,5))^5, (t_{1,2}t_{34})^2 = (1,2)(3,4)}$$

is not faithful.

Proof. Owing to the constraints of time we are alas only able to provide a single coset enumeration using MAGMA to show that the homomorphic image has order 2.

```
> G:=Group<x,y,t|x^5,y^2,(x*y)^4,(y*y^x)^3,
> t^2,(t,y*y^(x^2)*y^(x^3)),(t,y^(x^2)),
> (t*y^x*y^(x^3))^5,(t*t^(x^2))^2*y*y^(x^2)>;
> #G;
2
```

□

Now, since we already have a relation relating a word in the symmetric generators to an element of the control group there is nothing to stop us considering the relation $(t_{1,2}t_{3,4})^2 = id$. Sure enough in this case we find that a coset enumeration reveals that we have been naturally led to symmetric presentation of a (non-trivial) finite group. Once again, we employ the double coset enumerator

```
> S:=!Sym(5);
> stab:=Stabilizer(S,{1,2});
> f,nn,k:=CosetAction(S,stab);
> 1^f(S!(2,3));
4
> 1^f(S!(1,3)(2,4));
3
```

Here we have taken a copy of the symmetric group S_5 and defined an action of it on pairs of points from the set $\{1, \ldots, 5\}$. The computer has now named the group '`nn`'. We have then found that the computer has labeled the pair 12 with the number '1'; the pair 13 with the number 4 and the pair 34 with the number '3'. We proceed to enter the relations and the enumerate the double cosets.

```
> RR:=[<[1,4,1,4,1],f(S!(2,3)(4,5))>,<[1,3,1,3],Id(nn)>];
> CT:=DCEnum(nn,RR,nn:Print:=5,Grain:=100);
```

```
Index: 1584 = Rank: 27 = Edges: 156 = Status: Early closed = Time:
0.770
```

The computer has found that our target group contains the image of a copy of S_5 to index at most 1584 and therefore has order at most $|S_5| \times 1584 = |M_{12} : 2|$.

To identify permutations satisfying the presentation we note that this presentation is closely related to one of the first examples of symmetric presentations discovered namely

$$\frac{3^{\star 5} : A_5}{(3,4,5) = (t_2^{-1}t_1)^2} \cong 3 \times M_{12}.$$

To verify this presentation, the conjugation action of A_5 on its 5-cycles is considered. The 5-cycles fall into two conjugacy classes each of size 12 with the property that if a permutation π is in one class then π^2 is in the other. Permutations lying outside A_5 that give symmetric generators for the group $3\times M_{12}$ may be described in terms of this action on the 5-cycles proving the above presentation. These in turn can be related to the structure of the Dodecahedron giving a beautiful connection between the Mathieu groups and the Platonic solids. This is described in some detail by Curtis in [28, Part I and Section 5.5] (A full colour diagram showing the connection with the dodecahedron is on [28, p.8]).

This is also, more overtly, related to an involutory symmetric presentation first considered by Sayed [53, p.26] namely,

$$\frac{2^{\star\binom{5}{2}} : A_5}{((1,2,3,4,5)t_{1,2})^3} \cong L_2(11).$$

Whilst this presentation only requires a single short relation, it is much more poorly motivated.

In our present situation, to produce the natural permutation representation of M_{12}:2

label	Cycles		label
1	(12345)	(13524)	13
2	(15432)	(14253)	14
3	(12453)	(14325)	15
4	(13542)	(15234)	16
5	(12534)	(15423)	17
6	(14352)	(13245)	18
7	(13425)	(12354)	19
8	(15243)	(14532)	20
9	(15324)	(12543)	21
10	(14235)	(13452)	22
11	(14523)	(12435)	23
12	(13254)	(15342)	24

Table VI: Labels of the 5-cycles of S_5

on 24 points we define an action of our control group on 24 points. Since the point stabilizer in such an action has order 5 we must consider the conjugation action of S_5 on its 5-cycles. Again we resort to our tried and tested method of considering the stabilizer of a symmetric generator. Labeling the 5-cycles as we do in Table VI we are able to construct permutations on the 24 points the generate the centralizer of a symmetric generator.

Using this labelling we can translate generators for our control group into permutations of 24 points. Generators for the control group and the stabilizer of the point 1 and 2 are given in Table VII.

5 points	24 points
(1,2,3,4,5)	(3,10,5,11,7)(4,9,6,12,8)(15,21,17,24,19)(16,22,18,23,19)
(1,2)	(1,22)(2,21)(3,20)(4,19)(5,24)(6,23)(7,16)(8,15)(9,14)(10,13)(11,18)(12,17)
(3,4)	(1,23)(2,24)(3,19)(4,20)(5,21)(6,22)(7,15)(8,16)(9,17)(10,18)(11,13)(12,14)
(4,5)	(1,19)(2,20)(3,21)(4,22)(5,23)(6,24)(7,13)(8,14)(9,15)(10,16)(11,17)(12,18)

Table VII: Generators of a copy of S_5 acting on 24 points and a copy of $2\times S_3$.

Now, to obtain a permutation corresponding to the symmetric generator t_{12} we seek a permutation of order 2 on the twenty four points that commutes with the permutations in Table VII corresponding to the permutations (1,2), (3,4) and (4,5) that satisfy the

additional relations $(t_{1,2}t_{3,4})^2$ and $(t_{12}(2,3)(4,5))^5$. It turns out that the only permutations meeting all of these conditions are the permutations given in Table VIII.

(1,2)(3,4)(5,6)(7,12)(8,9)(10,11)(13,18)(14,15)(16,17)(19,20)(21,22)(23,24)
(1,2)(3,4)(5,6)(7,10)(8,11)(9,12)(13,16)(14,17)(15,18)(19,20)(21,22)(23,24)
(1,4)(2,5)(3,6)(7,8)(9,10)(11,12)(13,14)(15,16)(17,18)(19,22)(20,23)(21,24)
(1,6)(2,3)(4,5)(7,8)(9,10)(11,12)(13,14)(15,16)(17,18)(19,24)(20,21)(22,23)

Table VIII. Permutations corresponding to the symmetric generator t_{12}

When combined with the permutations of Table VII, any one of these generate a copy of $\mathrm{M}_{12} : 2$.

We have thus been naturally led to the following new symmetric presentation.

Lemma 3.11

$$\frac{2^{\star\binom{5}{2}} : \mathrm{S}_5}{(t_{1,2}(2,3)(4,5))^5, (t_{1,2}t_{3,4})^2} \cong \mathrm{M}_{12} : 2$$

We can define a graph on the symmetric generators as follows. The symmetric generators themselves form the vertex set. We adjoin the vertices t_{ij} and t_{kl} with an edge if and only if $\{i,j\} \cap \{k,l\} = \emptyset$. There should be little confusion in writing $t_{1,2}t_{3,4}$ to denote both a particular edge of the graph and a particular word in the symmetric generators. This graph is clearly a copy of the venerable Petersen graph, as pictured on the cover of this thesis. We have thus found a connection between the sporadic group M_{12} and one of the most exceptional graphs in the whole mathematics.

Furthermore we can relate much of the combinatorial structure of the Petersen graph to the subgroup structure of $\mathrm{M}_{12} : 2$. We give some examples of this (we shall assume that the reader is familiar with basic structural properties of the Petersen graph that are easily proven and simply state them when necessary).

Vertex Set The simple group M_{12} contains all of the symmetric generators and so is generated by the 'vertices' of the graph alone. (Note that from the first relation this group will also contain the whole of the derived subgroup of the control group.)

Vertex/6-cycle Recall that every vertex of the Petersen graph uniquely corresponds to a 6-cycle (the six vertices at distance two from it) and vice versa. The stabilizer of a single vertex corresponds to the centralizer of a symmetric generator (ie an involution of $M_{12} : 2$ of class 2A). The symmetric generator t_{12} is clearly centralized by the subgroup of the control group $\langle (1,2)(3,4),(4,5) \rangle$ and from the second relation this will also be centralized by the group $\langle (1,2)(3,4),(4,5),t_{34} \rangle$. The second relation now tells us that the centralizer will also contain elements of the form $t_{13}t_{12}t_{14}t_{15}(2,4)$. Altogether these generate the maximal subgroup of structure $(2^2 \times A_5) : 2$.

Maximal Independent Sets There are two classes of maximal subgroups of $M_{12}.2$ with isomorphism type $L_2(11).2$, each of order 1320. One can be generated as follows.

Recall that a set of vertices of a graph is *independent* if no two of the vertices are adjoined by an edge. See for instance Bollobás [5, p.4]. A *maxiaml independent set* is an independent set of maximal order. An independent set of the Petersen graph of maximal size contains four vertices. Any independent set of vertices in the Petersen graph is of form $\{t_{i,j} | j \in \{1,\ldots,5\} \backslash \{i\}\}$ for some fixed $i \in \{1,\ldots,5\}$. These four symmetric generators along with the copy of S_4 in the control group fixing this set generates a maximal copy of $L_2(11).2$.

(We remark that at the time of writing the author knows of no maximal subgroup of $M_{12} : 2$ naturally corresponding to a non-edge of the Petersen graph, but since the 'endpoints' of a non-edge are contained in a unique maximal independent set, it is the opinion of the author that there are none.)

"Minimal Maximal" Matchings Recall that a *matching* of a graph is a set of pairwise non-adjacent edges; that is, no two edges share a common vertex. A *maximal matching* is a matching M of a graph Γ with the property that if any edge of Γ not in M is added to M, it is no longer a matching, that is, M is maximal if it is not a proper subset of any other matching in the graph Γ. See for instance Bollobás [5, p.85]. We say a maximal

matching is a *minimal maximal matching* if it is a maximal matching with a minimal number of edges in it.

It is straightforward to check that any minimal maximal matching of the Petersen graph is of the form $\{t_{1,2}t_{3,4}, t_{1,3}t_{2,4}, t_{1,4}t_{2,3}\}$. The subgroup generated by these three words is a copy of S_3. The copy of S_4 stabilizing this collection of words will normalize the whole of this subgroup. Together these generate a copy of the maximal subgroup of $\mathrm{M}_{12} : 2$ of index 1320 with structure $\mathrm{S}_4 \times \mathrm{S}_3$.

Automorphism Group The control group of our symmetric presentation, which is a copy of S_5 is the full automorphism group of the Petersen graph. It is maximal in $\mathrm{M}_{12} : 2$.

A noticeable omission from the above list is 5-cycles. These most naturally correspond to copies of the (non-maximal) subgroups of structure $\mathrm{PGL}_2(9)$ defined by the easily verified symmetric presentation

$$\frac{2^{\star 5} : \mathrm{D}_{10}}{(tt^x)^2, (ty^x)^5} \cong \mathrm{PGL}_2(9)$$

where D_{10} is the dihedral group of order 10 and the elements x and y are defined by the presentation $\langle x, y | x^5, y^2, (xy)^2 \rangle$.

3.8.5 $\mathbf{E}_6$

Finally, recall from Section 3.3.3 that $Stab_{\mathrm{S}_6}(123, 124) = \langle (1,2), (5,6) \rangle$, and so $C_{\mathrm{S}_6}(Stab_{\mathrm{S}_6}(123, 124)) = \langle (1,2), (3,4), (5,6) \rangle$. Given the results obtained for the other exceptional cases, it seems likely that some exceptional behaviour is possible in this case. For instance, applying the Famous Lemma to the pair of subsets denoted 123 and 456 we find that

$$Stab_{\mathrm{S}_6}(123, 456) \cong \mathrm{S}_3 \times \mathrm{S}_3$$

and so

$$C_{\mathrm{S}_6}(Stab_{\mathrm{S}_6}(123, 456)) = id.$$

Since the action defining the progenitor is not primitive (there are twenty blocks of size two) we are led straight to the short relation $t_{1,2,3}t_{4,5,6} = id$. Using only this relation alone, the coset enumeration appears to not terminate. Given the symmetric presentations of the Coxeter groups given in the previous sections it is natural to consider the symmetric generators t_{123} and $t_{1,2,4}$. In Section 3.3.3, we found that the Famous Lemma told us that words in the symmetric generators t_{123} and $t_{4,5,6}$ belong to the group $\langle (1,2), (3,4), (5,6) \rangle$. Since there is a large number of elements in the subgroup we make no effort to eliminate all possible additional relations we could potentially use here. Instead we note the following. If we wish to equate the permutation (1,2)(5,6) to a word in $t_{1,2,3}$ and $t_{1,2,4}$ then by the Second Parity Lemma, such a word must have even length.

Lemma 3.12 The image of the control group in the factored progenitor

$$\frac{2^{\star\binom{6}{3}} : \mathrm{S}_6}{(1,2)(5,6)t_{1,2,3}t_{1,2,4}}$$

is not faithful.

Proof. $(1,2)(5,6) = t_{1,2,3}t_{1,2,4} = t_{1,2,3}t_{1,3,4}^2 t_{1,2,4} = (t_{1,2,3}t_{1,3,4})(t_{1,3,4}t_{1,2,4}) = (1,3)(5,6)(1,4)(5,6)$ which implies that $(1,2,4,3)(5,6) = id$, so the image of the control group is not faithful.□

We are thus forced to consider the relation $(1,2)(5,6)(t_{1,2,3}t_{1,2,4})^2$. Using the double coset enumerator it is straightforward to verify the following symmetric presentation.

Lemma 3.13

$$\frac{2^{\star\binom{6}{3}} : \mathrm{S}_6}{(1,2)(5,6)(t_{1,2,3}t_{1,2,4})^2, t_{1,2,3}t_{4,5,6}} \cong 2 \times 2\dot{\mathrm{L}}_3(4)$$

At the time of writing, the only other interesting image of the progenitor $2^{\star\binom{6}{3}} : \mathrm{S}_6$, apart from $W(\mathrm{E}_6)$ (which is much harder to naturally motivate) is the following.

Lemma 3.14

$$\frac{2^{\star\binom{6}{3}} : \mathrm{S}_6}{(1,2)(5,6)(t_{1,2,3}t_{1,2,4})^2, (t_{1,2,3}t_{4,5,6})^3, (2,3)(4,5)(t_{1,2,3}t_{1,4,5})^3} \cong \mathrm{L}_3(9).2^2.$$

Chapter 4

Irreducible Monomial Representations of Low Dimensional Linear Groups

Recall that a matrix is said to be *monomial* if every row and column has only one non-zero entry. Let G be a group. A representation of G $\rho\colon G \to GL(V)$ is said to be a *monomial representation* of G if there exists a basis of V with respect to which $\rho(g)$ is a monomial matrix for every $g \in G$.

Note in particular that since the elements of a finite group have finite order, the non-zero entries of such a matrix must be r^{th} roots of unity for some positive integer r. Such a representation in characteristic 0 is therefore writable over the cyclotomic field $\mathbb{Q}(\zeta_k)$ where ζ_k satisfies $\zeta_k^{k-1} + \zeta_k^{k-2} + \cdots + 1 = 0$. Note that since ζ_2=-1 we have $\mathbb{Q}(\zeta_2) = \mathbb{Q}$. (These representations may also be defined in non-zero characteristics, but we shall not be considering these representations here.)

Let p be a prime and $q = p^r$ for some positive integer r. In this chapter we shall classify the irreducible monomial representations of the groups $L_2(q)$ and their most natural decorations. More specifically, we prove the following.

Theorem 4.1 The only irreducible monomial representations of the groups $L_2(q)$ are the following.

- Any linear representation;
- Any representation of $\mathrm{L}_2(2)$ all of which are writable over $\mathbb{Q}$;
- Any representation of $\mathrm{L}_2(3)$, the non-trivial linear representations being writable over $\mathbb{Q}(\zeta_4)$ and the 3 dimensional representation being writable over $\mathbb{Q}$;
- The 7 dimensional representation of $\mathrm{L}_2(7)$, writable over $\mathbb{Q}$;
- Any irreducible $q+1$ dimensional representation of $L_2(q)$, writable over $\mathbb{Q}(\zeta_d)$ where d is some divisor of $q-1$ depending on the representation.

Recall that a representation is said to be *faithful* if the only element $g \in G$ with the property that $\rho(g)$ is the identity matrix is the identity element of G. Using the fact that linear characters of non abelian groups are never faithful along with the fact that $\mathrm{L}_n(\mathrm{q})$ is simple unless $n = 2$ and $q \leqslant 3$ and the fact that the kernel of a representation is a normal subgroup, we can easily deduce that following corollary.

Corollary 4.2 The only irreducible monomial representations of the groups $L_2(q)$ are the following.

- The irreducible q dimensional representation of $L_2(q)$ for $q \in \{2, 3, 5, 7\}$;
- Every irreducible $q+1$ dimensional representation of $L_2(q)$ for any q.

The only repetition appearing in this corollary stems from the exceptional isomorphism $\mathrm{L}_2(4) \cong \mathrm{L}_2(5)$.

Our motivation for wanting to consider the groups $L_2(q)$ is as follows. Recall from page 1 the Classification of the Finite Simple Groups. Since the cyclic groups of prime

order are abelian all of their representations are linear and therefore of little use in defining symmetric presentations. The irreducible monomial representations of the symmetric and alternating groups and their covers were classified by Curtis and Whyte. They then went on to classify the monomial representations of the sporadic simple groups and their covers [32, 33, 63]. This only leaves the groups of Lie Type. As noted earlier, by far the widest class of these are the groups $L_2(q)$. In the earlier cases it was found that exceptional monomial representations may be used to define symmetric presentations of the sporadic simple groups. If we are to make similar use of monomial representations of the groups of Lie type we need the groups in question to be sufficiently small to be contained in sporadic groups. Furthermore, for there to be a plentiful supply of monomial representations, a plentiful supply of groups is desirable. As noted earlier, by far the largest class of finite simple groups are the groups $L_2(q)$. It is for this reason that we consider the monomial representations of these groups here.

Monomial representations are computationally useful since they allow group elements to be represented as a permutation matrix multiplied by diagonal matrix. This makes calculating with group elements as well as the storage and transmission of group elements much easier. In particular an $n \times n$ matrix ordinarily requires a string of n^2 symbols to be recorded. Since monomial matrix can be stored as a permutation matrix multiplied by a diagonal matrix it is possible to represent each group element in a monomial representation with at most $2n$ symbols. (Whilst computers will always store permutations as a string of n symbols a human being will neglect fixed points of permutations, making representation of such an element with fewer than $2n$ points possible.)

For example the group $3\dot{}\mathrm{S}_7$ was found to have a 30 dimensional irreducible monomial representation writable over $\mathbb{Q}(\zeta_3)$ enabling group elements to be represented as a degree 30 permutation multiplied by a diagonal matrix. (Note that the lowest degree permutation representation of $3\dot{}\mathrm{S}_7$ has degree 63.) Since the cyclic group of order 7 admits (outer)

automorphisms of order 3 it follows that this enables us to form the progenitor $7^{\star(15+15)} :_m 3^{\cdot}\mathrm{S}_7$ (the degree 30 permutation permutation representation is imprimitive, preserving two blocks of 15 points).

As a specific example of how monomial representations can be used in this way, the progenitor $7^{\star(15+15)} :_m 3^{\cdot}\mathrm{S}_7$ has been used by Curtis to construct the sporadic Held group (see Atlas [19, p.104]) with a natural symmetric presentation. Factoring this progenitor by a single short and naturally motivated relation, the Held group is obtained as a homomorphic image. More specifically Curtis proved

$$\frac{7^{\star(15+15)} :_m 3^{\cdot}\mathrm{S}_7}{(st)^3} \cong \mathrm{He}$$

where He denotes the sporadic Held group; t is a certain element of $3^{\cdot}\mathrm{S}_7$ and s is a certain symmetric generator. See Curtis [28, p.278] or [25] for details. Similar results have been proved for other sporadic groups including several of the Mathieu groups [22, p.266 and p.271] and the Harada Norton group, [10], [28, p.284]. This justifies our emphasis on the low dimensional cases.

When necessary we shall denote elements of the group $L_2(q)$ by matrices of $SL_2(q)$ that are mapped onto the elements of $L_2(q)$ when the center of $SL_2(q)$ is factored out. To emphasise that we are dealing with an equivalence class of matrices rather than the matrices themselves we shall write these with square brackets rather than the usual round brackets.

Whilst recent (unpublished) work of Hiss and Magaard [51] has led to a more general result than what we prove here, their methods are much less elementary. In particular they use the celebrated theorem of Aschbacher on the maximal subgroups of finite classical groups [4]; Kleidman and Liebeck's detailed extension of this result [49] and, of course, the Classification of the Finite Simple Groups. We assume none of these results here.

The contents of this chapter are based heavily on the author's paper [39].

4.1 Preliminaries

The most convenient way to obtain non-linear monomial representations of a group is to induce them up from non-trivial linear representations of subgroups by the following theorem.

Theorem 4.3 Let H be a subgroup of G and let $\chi\colon H \to GL_1(\mathbb{C})$ be a representation of H. Then $\chi \uparrow_H^G$ is a monomial representation of G of dimension $|G : H|$.

See Isaacs [45, p.67] for details.

The above theorem tells us that to find monomial representations of $L_2(q)$ we need to understand the subgroup structure of $L_2(q)$. We shall therefore need Dickson's Theorem classifying the maximal subgroups of the groups $L_2(q)$ as given in Section 2.1.1.

Theorem 4.3 also tells us that to classify the irreducible monomial representations of $L_2(q)$ we need to know the character table of $L_2(q)$. Generic character tables for these groups are given in Adams [2] or alternatively in Fulton and Harris [41, Section 5.2]. Rather than reproduce the entire character tables here we shall simply state the characters we need when required.

Theorem 4.3 also tells us that knowing how to induce representations up from subgroups will be extremely important in what follows. We shall therefore require the standard formula for inducing characters as given in Isaacs [45, p.62].

Lemma 4.4 (Formula for Inducing Characters) Let G be a group and let $H \leqslant G$ be a subgroup. Let χ be a character of H and let $\dot{\chi} : G \mapsto \mathbb{C}$ be defined by the following formula.

$$\dot{\chi}(g) = \begin{cases} \chi(g) & \text{if } g \in H; \\ 0 & \text{if } g \notin H. \end{cases}$$

The values of the character $\chi \uparrow_H^G$ are given by the following formula.

$$\chi \uparrow_H^G (g) := \frac{1}{|H|} \sum_{y \in G} \dot{\chi}(y^{-1}gy).$$

Early work on the irreducible monomial representations of groups was conducted by Djoković and Malzan [35, 36] classifying the monomial representations of the symmetric and alternating groups. In particular they found the following representations.

- The group S_3 has an irreducible monomial representation in 2 dimensions.
- The group S_4 has an irreducible monomial representation in 2 dimensions.
- The group S_4 has two irreducible monomial representation in 3 dimensions.
- The group S_5 has an irreducible monomial representation in 6 dimensions.
- The group A_4 has an irreducible monomial representation in 3 dimensions.
- The group A_5 has an irreducible monomial representation in 5 dimensions.
- The group A_6 has an irreducible monomial representation in 10 dimensions.

The well-known exceptional isomorphisms $S_3 \cong L_2(2)$, $A_4 \cong L_2(3)$, $A_5 \cong L_2(4) \cong L_2(5)$ and $A_6 \cong L_2(9)$ ensure that whenever we encounter one of the above groups the above irreducible monomial representations are already known to exist and further calculation on our part is not required.

Note that we shall only do character calculations to ensure the existence of the representations alluded to in Theorem 4.1 and we shall not give explicit matrices in the general for all of these groups here.

4.2 The Proof of Theorem 4.1

We first prove two lemmata concerning the linear characters of a class of subgroups of $L_2(q)$.

Lemma 4.5 Let $q \geqslant 5$ be odd. The linear characters of the image in $L_2(q)$ of the subgroup of $SL_2(q)$ of upper triangular matrices are as follows.

$p^r : (q-1)/2$			
# of classes	1	$(q-1)/2-1$	2
$\lvert C_G(g)\rvert$	$q(q-1)/2$	$(q-1)/2$	q
rep	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} \alpha^j & 0 \\ 0 & \alpha^{-j} \end{bmatrix}$ $1 \leqslant j \lneq (q-1)/2$	$\begin{bmatrix} x & y \\ 0 & x^{-1} \end{bmatrix}$ $x, y \in \mathbb{F}_q^\times$
χ_k	1	α^{jk}	1

Here α is a primitive $(q-1)^{th}$ root of unity and k ranges over $0 \leqslant k \lneq (q-1)/2$.

Proof. The above class functions are characters since they are precisely the $(q-1)/2$ characters obtained by lifting the linear characters from the cyclic group of order $(q-1)/2$ - a homomorphic image obtained by factoring out the normal elementary abelian subgroup of order q.

These $(q-1)/2$ characters are the only linear characters of $p^r : (q-1)/2$ since there are only $(q-1)/2+2$ conjugacy classes and thus $(q-1)/2+2$ irreducible characters. There are therefore only two more irreducible characters and these cannot be linear since $2 \lneq q(q-1)/2-(q-1)/2$ for $q \geqslant 5$. □

The case of $q = 3$ is easily handled separately as $\mathrm{L}_2(3) \cong \mathrm{A}_4$.

Lemma 4.6 Let $q \geqslant 4$ be even. The linear characters of the image in $L_2(q)$ of the subgroup of $SL_2(q)$ of upper triangular matrices are as follows.

$p^r : (q-1)$			
# of classes	1	$q-2$	1
$\lvert C_G(g)\rvert$	$\lvert L_2(q)\rvert$	$q-1$	q
rep	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} \alpha^j & 0 \\ 0 & \alpha^{-j} \end{bmatrix}$ $1 \leqslant j \lneq q-1$	$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$
χ_k	1	α^{jk}	1

Here α is a primitive $(q-1)^{th}$ root of unity and k ranges over $0 \leqslant k \lneq q-1$.

Proof. The above class functions are characters since they are precisely the $(q-1)$ characters obtained by lifting the linear characters from the cyclic group of order $(q-1)$ - a homomorphic image obtained by factoring out the normal elementary abelian subgroup of order q.

These $q-1$ characters are the only linear characters of $p^r : (q-1)$ since there are only q conjugacy classes and thus q irreducible characters. There is therefore only one more irreducible character and this cannot be linear since $2 \lneq q(q-1) - (q-1)$. □

The case of $q = 2$ is easily handled separately as $\mathrm{L}_2(2) \cong \mathrm{S}_3$.

Proof of Theorem 4.1 Clearly any linear representation of $L_2(q)$ is monomial. By Theorem 4.3 any non linear monomial representation of $L_2(q)$ will be induced from a linear representation of a proper subgroup. From the character tables of the groups $L_2(q)$ the highest dimensional representations are $q+1$ dimensional (see Adams [2, p.12]).

We proceed to use Dickson's Theorem to show that most maximal subgroups, and therefore most subgroups, have index greater than $q+1$. Indeed it will turn out that,

for most values of q, only one class of subgroups have index equal to $q+1$ that can therefore be used to produce monomial representations and that (other than the finitely many exceptions) no other non-linear representation of $L_2(q)$ is monomial.

Recall that $|L_2(q)| = (q-1)q(q+1)/2$ when q is odd and $|L_2(q)| = (q-1)q(q+1)$ when q is even. We consider each class of maximal subgroups in turn.

- $\underline{\mathrm{A}_4}$: In this case q must be odd and we must have $(q-1)q \leqslant 24$. This implies that $q = 3$ or 5. Since $\mathrm{L}_2(3) \cong \mathrm{A}_4$, the group $\mathrm{L}_2(3)$ contains no copies of A_4 as proper subgroups. We also have $\mathrm{L}_2(5) \cong \mathrm{L}_2(4) \cong \mathrm{A}_5$ and A_5 is a group for which all monomial representations are known. In particular there is a 5 dimensional monomial representation over the field $\mathbb{Q}(\zeta_3)$ and since 3=4-1 and 5=4+1, this representation falls into the family of monomial representations mentioned in the final bullet point of Theorem 4.1. (Note that $\mathrm{A}_4 \cong 2^2 : 3$.)

- $\underline{\mathrm{S}_4}$: In this case q must be odd and we must have $(q-1)q \leqslant 48$. This implies that $q = 3, 5$ or 7. The group $\mathrm{L}_2(3)$ is too small to contain a copy of S_4. The group $\mathrm{L}_2(5) \cong \mathrm{A}_5$ contains no copies of S_4 leaving only the possibility that $\mathrm{L}_2(7)$ has a 7 dimensional irreducible monomial representation obtained by inducing up the 'sign character' of S_4. Calculating the induced character shows this to be a genuinely new irreducible monomial representation and explicit matrices for this representation are given in Section 4.3.

- $\underline{\mathrm{A}_5}$: There are no non-trivial linear characters that can be induced up. All proper subgroups of a copy of A_5 are contained in one of the other subgroups.

- $\underline{\text{Subfield subgroups:}}$ The index of a subfield subgroup is greater than $q+1$ for all q.

- $\underline{\text{Dihedral groups or order } (q-1) \text{ or } 2(q-1)\text{:}}$ These subgroups have index $q(q+1)/2$ in both the even and odd cases. We have that $q(q+1)/2 \leqslant (q+1)$ if and only if $q = 2$ and again all monomial representations of the group $\mathrm{L}_2(2)$ are known.

- Dihedral groups of order $(q+1)$ or $2(q+1)$: These subgroups have index $q(q-1)/2$ in both even and odd cases. We have that $q(q-1)/2 \leqslant (q+1)$ if and only if $q = 2$ or 3 and again all irreducible monomial representations of $\mathrm{L}_2(2) \cong \mathrm{S}_3$ and $\mathrm{L}_2(3) \cong \mathrm{A}_4$ are already known and matrices for these representations are given in Section 4.3.

This only leaves the subgroups isomorphic to $p^r : (q-1)/2$ when q is odd or $p^r : (q-1)$ when q is even, each of index $q+1$. We first consider the case when q is odd. This splits into the two cases $q \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$ since the character tables are different in these two cases. We first handle case $q \equiv 1 \pmod 4$. From the character tables given by Adams [2, p.12] we see that the only $q+1$ dimensional characters of $L_2(q)$ are as follows.

# of classes	1	2	$(q-5)/4$	1	$(q-1)/2$
$\lvert C_G(g)\rvert$	$\lvert L_2(q)\rvert$	q	$(q-1)/2$	$q-1$	$(q+1)/2$
rep	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} \pm 1 & x \\ 0 & \pm 1 \end{bmatrix}$	$\begin{bmatrix} x^j & 0 \\ 0 & x^{-j} \end{bmatrix}$	$\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$	$\begin{bmatrix} x & \Delta y \\ y & x \end{bmatrix}$
ρ	$q+1$	1	$\alpha(x^j) + \alpha(x^{-j})$	$2\alpha(i)$	0

Here we write $i = \sqrt{-1} \in \mathbb{F}_q$; α is an automorphism of the multiplicative group $\mathbb{F}_q^\times$; $\Delta \in \mathbb{F}_q^\times - \mathbb{F}_q^2$ where $\mathbb{F}_q^2 := \{x \in \mathbb{F}_q | x = y^2 \text{ for some } y \in \mathbb{F}_q\}$ and $x, y \in \mathbb{F}_q^\times$. In the sixth column the x and y are chosen precisely so that $x^2 - \Delta y^2 = \pm 1$. There are $(q-5)/2$ such characters.

Using the standard formula for computing induced characters given in lemma 4.4 we find that each of the characters $\chi_k \uparrow_H^G$, where χ_k is the character appearing in Lemma 4.5, has the above form and is thus irreducible. More explicitly, the character values in the first and last column are clear since the identity is fixed under the conjugation action

of any element and the elements in the last class lie entirely outside the subgroup. The classes corresponding to the second column do not fuse in the larger group. The classes in the third an fourth columns are fused in pairs by the element

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

giving the character values listed.

Moreover it is easy to see that each of the above characters arises in this way since the group $\mathbb{F}_q^\times$ is cyclic and therefore any automorphism will be of the form $x \mapsto x^k$ which is precisely the form of the character values appearing in lemma 4.5. This completes the proof in this case.

Now if $q \equiv 3 \pmod 4$, the character tables given in Adams [2, p.12] tell us that the only $q+1$ dimensional characters are as follows.

# of classes	1	2	$(q-7)/4$	$(q-3)/4$	1
$\lvert C_G(g)\rvert$	$\lvert L_2(q)\rvert$	q	$(q-1)/2$	$(q+1)/2$	$(q+1)$
rep	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} \pm 1 & x \\ 0 & \pm 1 \end{bmatrix}$	$\begin{bmatrix} x^j & 0 \\ 0 & x^{-j} \end{bmatrix}$ $1 \leqslant j \lneq (q-3)/4$	$\begin{bmatrix} x & \Delta y \\ y & x \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$
χ_k	$q+1$	1	$\alpha(x^j)+\alpha(x^{-j})$	0	0

All symbols appearing here are the same as the case $q \equiv 1 \pmod 4$. There are $(q-2)/2$ such characters. Again, using the standard formula for computing induced characters given in lemma 4.4 we find that each of the characters $\chi_k \uparrow_H^G$ has the above form and is thus irreducible. Moreover it is easy to see that each of the above characters arises in this way since the group $\mathbb{F}_q^\times$ is cyclic and therefore any automorphism will be of

the form $x \mapsto x^k$ which is precisely the form of the character values appearing in lemma 4.5.

Finally if q is even then again the character table of $L_2(q)$ is again given in Adams [2, p.10]. We find that the only $q+1$ dimensional characters are as follows.

# of classes	1	$(q-2)/2$	1	$q/2$
$\lvert C_G(g)\rvert$	$\lvert L_2(q)\rvert$	$q-1$	q	$q+1$
representative	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} x^j & 0 \\ 0 & x^{-j} \end{bmatrix}$ $1 \leqslant j \lneq (2^r-1)/2$	$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} x & \Delta y \\ y & x \end{bmatrix}$
ρ	$q+1$	$\alpha(x^j)+\alpha(x^{-j})$	1	0

All symbols used here are the same as the q odd cases. There are $(q-2)/2$ such characters. Again using the standard formula for computing induced characters given in lemma 4.4 we find that each of the characters $\chi_k \uparrow_H^G$, where χ_k is the character appearing in Lemma 4.6, has the above form and is thus irreducible. Moreover it is easy to see that each of the above characters arises in this way since the group $\mathbb{F}_q^\times$ is cyclic and therefore any automorphism will be of the form $x \mapsto x^k$ which is precisely the form of the character values appearing in lemma 4.6. $\square$

4.3 Some Matrices

To illustrate how explicit matrices for the monomial representations alluded to by Theorem 4.1 may be obtained we give the MAGMA code used to obtain them here. Since near identical code may be used for the other groups, we only give the full code in the case $L_2(2)$.

4.3.1 2 by 2 matrices generating $\mathbf{L}_2(2) \cong \mathbf{S}_3$

```
> G:=PSL(2,2);
> Order(G.1*G.2);
3
> H:=sub<G|G.1*G.2>;
> C<u>:=CyclotomicField(3);
> M:=MatrixAlgebra(C,1);
> HM:=GModule(H,[M![u]]);
> I:=Induction(HM,G);
> GP:=MatrixGroup(I);
> GP;
MatrixGroup(2, C) Generators:
    [0 1]
    [1 0]

    [     0 -u - 1]
    [     u      0]
```

4.3.2 3 by 3 matrices generating $\mathbf{L}_2(3) \cong \mathbf{A}_4$

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

4.3.3 7 by 7 matrices generating $\mathbf{L}_2(7) \cong \mathbf{L}_3(\mathbf{2})$

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

4.4 Natural Decorations of $L_2(q)$

In this section we discuss analogues of the Theorem 4.1 for the groups $SL_2(q)$, $PGL_2(q)$ and $GL_2(q)$. We note that again, the generic character tables may be found in Adams [2] or Fulton and Harris [41, Section 5.2] and that from these tables we see that the highest dimensional representation in each case is $q+1$ dimensional. (Note that we make no attempt to consider exceptional decorations such as the exceptional cover group of $\mathrm{L}_2(9) \cong \mathrm{A}_6$.)

4.4.1 $GL_2(q)$

Theorem 4.7 No irreducible representations of the groups $GL_2(q)$ are monomial apart from the following.

- Any linear representation;
- Any representation of $\mathrm{GL}_2(2)$ each of which are writable over $\mathbb{Q}$;
- The 3 dimensional representation of $\mathrm{GL}_2(3)$, writable over $\mathbb{Q}(\zeta_4)$; the 2 dimensional representation of $\mathrm{GL}_2(3)$ writable over $\mathbb{Q}(\zeta_3)$ induced up from the special linear group $\mathrm{SL}_2(3)$ and the linear representations, each of which are writable over $\mathbb{Q}$;
- Any irreducible $q+1$ dimensional representation of $GL_2(q)$, writable over $\mathbb{Q}(\zeta_d)$ where d is some divisor of $(q-1)^2$ for q depending on the representation.

We first note that if q is even then $GL_2(q) = Z(GL_2(q)) \times SL_2(q)$ and so the proof is easy.

The only nonlinear representations of $GL_2(q)$ have dimension $q-1$, q or $q+1$, see [2, p.8].

If H is a subgroup of $GL_2(q)$ containing $SL_2(q)$ then H will have index at most $q-1$. If the index $|GL_2(q) : H| < q-1$ then no monomial representation induced from H will

be irreducible. If $|GL_2(q) : H| = q - 1$ then $H = SL_2(q)$ and is thus perfect so there are no non-trivial linear representations to induce up to give a monomial representation. If H does not contain $SL_2(q)$, then $|GL_2(q) : H| \geqslant q+1$, since subgroups of $SL_2(q)$ all have index at least $q+1$. If $|GL_2(q) : H| = q+1$ then the monomial representations of $GL_2(q)$ induced from the non trivial linear representations of H are precisely those appearing in Theorem 4.7.

Note that if $2|q$ then $L_2(q) = SL_2(q) = PGL_2(q)$ so the natural analogues of theorem 4.1 are immediate in these cases. Therefore throughout the rest of this section we shall assume that q is odd.

4.4.2 $SL_2(q)$

Theorem 4.8 No irreducible representations of the groups $SL_2(q)$ are monomial apart from the following.

- Any linear representation.
- Any representation of $\mathrm{SL}_2(2)$ all of which are writable over $\mathbb{Q}$.
- The 3 dimensional representation of $\mathrm{SL}_2(3)$, writable over $\mathbb{Q}$ and the linear representations, each of which are writable over $\mathbb{Q}(\zeta_3)$.
- The 7 dimensional representation of $\mathrm{SL}_2(7)$, writable over $\mathbb{Q}$.
- Any irreducible $q+1$ dimensional representation of $SL_2(q)$, writable over $\mathbb{Q}(\zeta_d)$ where d is some divisor of $q-1$ depending on the representation.

Since the center of $SL_2(q)$ is contained in every maximal subgroup of $SL_2(q)$, all maximal subgroups may be lifted from those of $L_2(q)$ and will have therefore have the same index.

Note that the 7 dimensional representation of $\mathrm{SL}_2(7)$ is not faithful since the center is contained in the derived subgroup of the index 7 subgroups of structure $2^{\cdot}\mathrm{S}_4$. Similarly the 3 dimensional representation of $\mathrm{SL}_2(3)$ is not faithful.

4.4.3 $PGL_2(q)$

Theorem 4.9 No irreducible representations of the groups $PGL_2(q)$ are monomial apart from the following.

- Any linear representation;
- Any representation of $\mathrm{PGL}_2(2)$ all of which are writable over $\mathbb{Q}$;
- The 2 dimensional representation of $\mathrm{PGL}_2(3)$, writable over $\mathbb{Q}(\zeta_3)$; the 3 dimensional representations, writable over $\mathbb{Q}(\zeta_4)$ and the linear representations, writable over $\mathbb{Q}$;
- The 5 dimensional representation of $\mathrm{PGL}_2(5)$, writable over $\mathbb{Q}$;
- Any irreducible $q+1$ dimensional representation of $PGL_2(q)$, writable over $\mathbb{Q}(\zeta_d)$ where d is some divisor of $q-1$ depending on the representation.

Here the maximal subgroups may be deduced as a corollary of Dickson's theorem since $PGL_2(q)$ lies inside $L_2(q^2)$.

Note that the isomorphisms $\mathrm{PGL}_2(3) \cong \mathrm{S}_4$ and $\mathrm{PGL}_2(5) \cong \mathrm{S}_5$ make the exceptional cases above special cases of the result of Djoković and Malzan [35].

4.5 Higher Dimensions

For the groups $L_3(q)$ we have a result analogous to Theorem 4.1 which states the following.

Theorem 4.10 The irreducible monomial representations of the groups $L_3(q)$ are the following.

- The trivial representations.

- Every irreducible q^2+q+1 dimensional representation, writable over $\mathbb{Q}$ for q odd or $q=2$.

The proof of this theorem is similar to the proof of Theorem 4.1; the differences are that in this case the maximal subgroups are those determined by Mitchell and Hartley ([42, 52]) and are again listed in King [48, p.6]. The generic character tables were determined by Simpson and Frame [54]. From these data we see that in this case it is sufficient to show that each maximal subgroup (and therefore every subgroup) either has an index greater than $(q+1)(q^2+q+1)/hcf(3,q-1)$, where $hcf(3,q-1)$ denotes the highest common factor of 3 and $q-1$, or is is a subgroup of this index whose derived subgroup has index 2 (these are the subgroups isomorphic to $p^{2r}:PGL_2(q)$, leading to the distinction between even and odd since $PGL_2(2^r)=L_2(2^r)$ and unless $r=1$ this group is simple). Again, as in the $L_2(q)$ case, variations of this result exist for the various decorations of $\mathrm{L_3(q)}$.

Note that the exceptional isomorphism $\mathrm{L_2(7)\cong L_3(2)}$ predicts that $\mathrm{L_2(7)}$ should have a $2^2+2+1=7$ dimensional representation, as seen in theorem 4.1.

Note the distinction between the cases $n=2$ and $n\geqslant 3$ stems from the fact that the $(q^n-1)/(q-1)$ dimensional representations are induced up from a subgroups of structure $p^{r(n-1)}:PGL_{n-1}(q)$ which is has a derived subgroup of index 2 when $n\geqslant 3$. In the case $n=2$, $PGL_1(q)$ is cyclic producing a greater index. Note that if $n=3$ and $q=2$ or 3 then these cases also have index 2, despite $PGL_2(q)$ being soluble. The other exceptional behaviour at $n=2$ stems from the exceptional isomorphisms $\mathrm{L_2(2)\cong S_3}$ and $\mathrm{L_2(3)\cong A_4}$.

4.6 Some Progenitors and Their Images

Returning to our philosophy of 'bad behaviour breeds bad behaviour', we use the monomial representations found in Theorem 4.1 to form progenitors and investigate their images. Several monomial progenitors closely related to these were investigated by Stanley [55]. Whilst several interesting images were found there, no particularly systematic ap-

proach was taken.

We shall use the notation that is used in the systematic approach of Bray, Curtis and Hammas [31, 9]. More specifically we shall write the order of a relation that is sufficient to define the group in bold, so a particular group may occur several times, being defined by different subsets of the set of relations. In each case we list the homomorphic images found in ascending order of order.

Whilst the Double Coset Enumerator is capable of handling symmetric generators of order greater than 2, and even non cyclic symmetric generators, it not very efficient at doing this. Furthermore, with such small control groups it is noticeably easier to use single coset enumeration. It is for these reasons that in this section we shall employ single coset enumeration to verify presentations. Since there are inevitably more single cosets than double cosets, this naturally limits the possible images we can find. Despite this, several interesting images are found.

4.6.1 $(2^2)^{\star 2} :_m \mathbf{L}_2(2)$

Since the 2 dimensional irreducible representation of $\mathrm{L}_2(2)$ is writable over $\mathbb{Q}(\zeta_3)$ we seek groups admitting an outer automorphism of order 3 to form a progenitor with. The smallest group with an outer automorphism of order 3 is the Klein foursgroup 2^2. This has been useful in defining symmetric presentations before. As noted in [26, p.52] John Bray has previously proved that

$$\frac{(2^2)^{\star 6} :_m 3^{\cdot}\mathrm{A}_6}{(\pi t)^6} \cong \mathrm{HJ}$$

where the central element of the control group fixes each of the six foursgroups while cycling their nontrivial elements; the natural action of A_6 simply permutes the foursgroups; π is a permutation in $3^{\cdot}\mathrm{A}_6$ that acts on the foursgroups like the permutation (1,2,3,4)(5,6) and t is an involution from the foursgroup labeled '1'.

Whilst the progenitor $(2^2)^{\star 2} :_m \mathrm{S}_3$ is mentioned by Curtis in [26] only the group A_5 is mentioned as being an image. We proceed to discuss a systematic approach to finding images of this progenitor.

Starting with the presentation

$$(2^2)^{\star 2} :_m \mathrm{L}_2(2) \cong \langle x, y, t, s | x^3, y^2, (xy)^2, t^2, s^2, (ts)^2, t^x s, s^x st, (st)^x t \rangle$$

we factor by the relations $(yt)^a$, $(xtt^y)^b$ and $(ytt^{xy})^c$ (using either of the related relations $(xts^y)^b$ and $(xt(st)^y)^b$ in place of the second of these relations gives the same result). Since the relation $(xt)^3$ always holds, the first of these relations is the only one using a word of the symmetric generators of length one worth considering. (Bray and Curtis refer to such relations as *first order parameters*.) We give some images of this progenitor below.

a	b	c	G
2	3	4	S_4
3	5	5	A_5
10	**2**	6	$\mathrm{A}_5 \times 2$
6	**4**	8	$\mathrm{PGL}_2(7)$
6	**7**	**6**	$\mathrm{PGL}_2(7)$
8	**7**	**6**	$\mathrm{PGL}_2(7)$
6	12	**6**	$(3\times\mathrm{L}_2(7)):2$
6	**5**	10	$2^5 :\mathrm{A}_5$
5	**10**	15	$\mathrm{A}_5\times\mathrm{A}_5$
5	20	30	$2^{\cdot}(\mathrm{A}_5\times\mathrm{A}_5)$
6	**6**	28	$\mathrm{S}_4\times\mathrm{L}_2(13)$
6	**7**	78	$\mathrm{PGL}_2(7)\times\mathrm{L}_2(13)$
11	**4**	11	$\mathrm{L}_2(23)$
12	**4**	**11**	$\mathrm{L}_2(23)$
13	**5**	**6**	$\mathrm{L}_2(25)$
6	**12**	**13**	$\mathrm{L}_2(25)$
8	**4**	22	$\mathrm{PGL}_2(23)$
7	**5**	14	$\mathrm{L}_2(29)$
7	**6**	**10**	J_1
13	**4**	26	$\mathrm{L}_2(103)$
8	**6**	**10**	$5\times\mathrm{HJ}$

We note that in addition to those listed above several finite soluble groups were also found to be images.

4.6.2 $7^{\star 2} :_m \mathbf{L}_2(2)$

It is more conventional to consider symmetric generators that are cyclic groups and the smallest cyclic group admitting an outer automorphism of order 3 has order 7. We shall therefore consider the progenitor $7^{\star 2} :_m \mathrm{L}_2(2)$.

Starting with the presentation

$$7^{\star 2} :_m \mathrm{L}_2(2) \cong \langle x, y, t | x^3, y^2, (xy)^2, t^7, t^x t^{-2} \rangle$$

we factor by the relations of the form $(yt)^a$ and $(xt(t^2)^y)^b$, $(xt(t^3)^y)^c$, $(xt(t^4)^y)^d$, $(xt(t^5)^y)^e$, $(xt(t^6)^y)^f$. Some interesting images of this progenitor are given below.

a	b	c	d	e	f	G
3	7	2	7	4	3	$\mathrm{L}_2(7)$
7	**4**	4	7	3	2	$\mathrm{L}_2(7)$
4	**7**	3	4	2	4	$\mathrm{PGL}_2(7)$
8	**2**	4	3	7	7	$\mathrm{PGL}_2(7)$
4	21	3	12	6	12	$(\mathrm{L}_2(7) \times 3) : 2$
8	6	12	**3**	21	21	$(\mathrm{L}_2(7) \times 3) : 2$
7	8	8	7	3	**2**	$2^3\mathrm{L}_3(2)$
6	7	**2**	7	8	3	$2 \times 2^3\mathrm{L}_3(2)$
14	8	8	7	3	**2**	$2 \times 2^3\mathrm{L}_3(2)$
5	**5**	5	7	4	4	A_7
5	5	5	7	**4**	4	A_7
6	**4**	**7**	5	5	6	S_7
6	**4**	7	5	**5**	6	S_7
6	**4**	21	5	15	6	$3\dot{}\mathrm{S}_7$
6	**5**	6	**4**	21	15	$3\dot{}\mathrm{S}_7$
6	21	21	6	**3**	12	$(3 \times \mathrm{U}_3(3)) : 2$
5	10	5	**6**	6	7	J_1

We note that in addition to those listed above several finite soluble groups were also found to be images.

4.6.3 $3^{\star 3} :_m \mathbf{L_2(3)}$

Since the 3 dimensional irreducible representation of $\mathrm{L}_2(3)$ is writable over $\mathbb{Q}(= \mathbb{Q}(\zeta_2))$ we seek groups admitting an outer automorphism of order 2 to form a progenitor with. The smallest group with an outer automorphism of order 2 is the cyclic group of order 3. We therefore form the progenitor $3^{\star 3} :_m \mathrm{L}_2(3)$. Curiously, this progenitor is not included in the Bray and Curtis non-involutory 'systematic approach' [9], mainly due to the fact that they also consider the progenitor $3^{\star 3} :_m \mathrm{S}_4$ ($\mathrm{L}_2(3) \cong \mathrm{A}_4 \leqslant \mathrm{S}_4$). Since the progenitor $3^{\star 3} :_m \mathrm{L}_2(3)$ may have images that the progenitor $3^{\star 3} :_m \mathrm{S}_4$ does not possess we proceed to investigate further.

Starting with the presentation

$$3^{\star 3} :_m \mathrm{L}_2(3) \cong \langle x, y, t | x^3, y^2, (yx)^3, t^3, t^y t, (t^x)^y t^x \rangle$$

we factor by the relations of the form $(xt)^a$, $(xt(t^x))^b$ and $(xt^y t^x)^c$ since the element y only inverts symmetric generators and so the relation $(yt)^2$ always holds. Some images of this progenitor are given below.

a	b	c	G
5	**11**	6	$\mathrm{L}_2(11)$
5	11	**6**	$\mathrm{L}_2(11)$
7	**3**	**7**	$\mathrm{L}_2(13)$
7	3	**7**	$\mathrm{L}_2(13)$
7	**3**	7	$\mathrm{L}_2(13)$
6	**7**	7	$\mathrm{L}_2(13)$
6	7	**7**	$\mathrm{L}_2(13)$
7	**7**	6	A_7
7	21	**6**	$3\dot{}\mathrm{A}_7$
25	25	**4**	$\mathrm{L}_2(49)$
25	**25**	**4**	$\mathrm{L}_2(49)$
12	**4**	7	HJ

We note that in addition to those listed above several finite soluble groups were also

found to be images.

4.6.4 $3^{\star 7} :_m \mathbf{L}_2(7)$

The only remaining exceptional action is the action of $\mathrm{L}_2(7)$ on seven points, writable over $\mathbb{Q}$. Again this leads to symmetric generators of order 3 and the progenitor $3^{\star 7} :_m \mathrm{L}_2(7)$. As noted earlier, this action is somewhat less exceptional than our other exceptions since the isomorphism $\mathrm{L}_2(7) \cong \mathrm{L}_3(2)$ combined with lemma 4.10 predicts that this group should have a $2^2 + 2 + 1 = 7$ dimensional representation writable over $\mathbb{Q}$. All other exceptional actions stemmed from isomorphisms with symmetric or alternating groups and were therefore completely different in nature.

It is therefore perhaps unsurprising that when Bray and Curtis considered images of this progenitor in the systematic approach [9, Section 9] they listed very few images stating that

> ...Certain of our progenitors possess too few known images to warrant separate tables, although the images they do have are of great interest ... the progenitor $3^{\star 7} :_m \mathrm{L}_3(2)$ maps onto the alternating group A_7 the image being realised by, for example, the single relator $[(1,\bar{1})(0,3,\bar{0},\bar{3})(2,6,\bar{4},\bar{5})t_2]^3$.

Here, t_2 is a symmetric generator that generates a cyclic subgroup corresponding to the point 2 and in the permutation $(1,\bar{1})(0,3,\bar{0},\bar{3})(2,6,\bar{4},\bar{5})$ the bars denote mapping a symmetric generator to its square (so for instance the symmetric generator labeled '0' is mapped to the square of the generator denoted '3'). We mention in passing that Bray and Curtis also found some interesting images of the progenitor $3^{\star 7} : \mathrm{L}_3(2)$ defined by the permutation action of $\mathrm{L}_3(2)$ on seven points including the groups HJ and $2^{\cdot}$HJ. Again, there were too few images to merit tabulation of these results.

Appendix A

Potential Future Work

In this appendix we describe some aspects of the work that remains to be done as part of the 'Symmetric Generation' research programme, which in the opinion of the author are worthy of future work.

- Symmetric Presentations of the Large Sporadic Simple Groups

  Given the usefulness of a symmetric presentation of a group and how effective the techniques of symmetric generation have proved to be in providing elementary constructions for the smaller sporadic simple groups it would be of great interest to exhibit elegant symmetric presentations of some of the larger sporadic simple groups. Most notably, at the time of writing, the following conjectured symmetric presentations for the Monster group $\mathbb{M}$ have yet to be verified.

  Conjecture A.1

  $$\frac{7^{\star(\frac{f}{2h}+\frac{f}{2h})} : 3^{\cdot}Fi_{24}}{(\pi t_1)^3} \cong \mathbb{M}$$

  where $f := |Fi'_{24}|$, the order of the largest sporadic simple Fischer group, $h := |He|$ the order of the sporadic simple Held group and the remaining notation as well as a description of the action defining the progenitor are explained in [26, p.56].

Conjecture A.2

$$\frac{5^{\star\frac{b}{2r}} : 2\cdot\mathbb{B}}{(\pi t_1)^3, (\sigma t_1)^3} \cong \mathbb{M}$$

where $2\cdot\mathbb{B}$ denotes the double cover of the Baby Monster group, $b := |\mathbb{B}|$, $r := |HN|$ the order of the sporadic simple group of Harada and Norton and again the remaining details may found in [26, p.56].

Furthermore, at the time of writing, no symmetric presentation is known for either the Baby Monster $\mathbb{B}$ or the Thompson group Th.

There are several other sporadic groups for which the only known symmetric presentations are unwieldy and difficult to motivate. Notable cases in point are the symmetric presentation of the Lyons group Ly due to Bray [8, Chapter 10] (whose defining relation is devoid of motivation and whose verification employs the high-powered theory of amalgams) and the symmetric presentation of the O'Nan group O'N given by Curtis [26, p.48] (which requires three extremely long relations).

Another notable 'thorn in the side' of symmetric generation is the sporadic Rudvalis group Ru - a group that has largely resisted all attempts to exhibit an elegant symmetric presentation of it, despite being a permutation group on just 4060 point and having a matrix representation in as few as 28 dimensions! To date the most fruitful investigations have been Curtis and Malik's approaches using the progenitors $2^{\star 7}$: $\mathrm{L}_3(2)$ and $2^{\star\binom{8}{2}} : (2^3{:}\mathrm{L}_3(2))$ and the author's approaches using the progenitor $2^{\star 300}{:}\mathrm{P}\Gamma\mathrm{L}_2(25)$ and progenitors closely related to the progenitor $\mathrm{A}_5^{\star 1456}{:}\mathrm{Sz}(8)$.

- Symmetric Representation of Group Elements

  One of the more significant applications of the techniques of symmetric generation is their use in the succinct representation of an element of a sporadic simple group as an

element of the control group followed by short words in the symmetric generators. This often results in a substantial saving in memory compared with representing elements in more traditional ways such as permutations or matrices. Of course, a representation of the elements of a group is useless unless the elements represented may be multiplied together and so the development of procedures and programs for doing this is of great interest. Whilst the most notable success in this direction was Curtis and the author's recent use of a symmetric presentation of the Conway group $\cdot 0$ to represent the elements of $\cdot 0$ in an extremely succinct manner [29], there is still great potential for producing similar programs for other, larger groups. In particular, other sporadic groups stand to benefit from this treatment.

A notable case in point is the Janko group J_4. Compared to the order of $\cdot 0$, the order of J_4 is only about 10 times bigger, but the group fares substantially worse with respect to conventional methods of representing its elements - the lowest degree permutation representation of J_4 is on 173067389 points and the lowest dimensional representation of this group is in 112 dimensions working over the field of two elements (ie representing an element of J_4 as a matrix requires a string of $112^2 = 12544$ symbols).

An elegant symmetric presentation for this group was first exhibited by Bolt [6] using the action of the Mathieu group M_{24} on the 3795 triads (see either the ATLAS [19, p.96] or Conway and Slone [20, Chapter 11] for the definition of a triad). This symmetric presentation makes it possible to represent elements of J_4 as a string of at most $86(=24+12+(5+5)\times 5)$ symbols and more typically as a string of as few as $65(=23+12+(5+5)\times 3)$ symbols. It would be of great interest to see a program that would be able to take elements of J_4 represented in this manner and exhibit their product in the same manner. Such a program would have to work very differently from the $\cdot 0$ program (since the $\cdot 0$ program made great use of the

geometry of the Leech lattice) and probably more closely resemble the workings of the programs used to represent the elements of the Janko group J_1 [30]. Such a program would inevitably be more difficult to produce than the J_1 programs owing to the difficulty in representing the symmetric generators themselves (which is done most succinctly by representing a triad by any of the 5+5 points from any pair of the octads contained in the triad) and by the fact that the presentation for J_4 is defined by two relations whilst the presentation for J_1 is defined by just one.

- A Non-Involutory Double Coset Enumerator

  In several places throughout this thesis we have seen the examples of the involutory Double Coset Enumerator of Bray and Curtis described in [11] at work. This program is extremely effective at performing coset enumerations inside large groups that would not be possible by hand.

  The program was, however, written with involutory symmetric generators in mind and whilst it is capable handling symmetric generators of higher order, it is not very efficient at doing this.

  A coset enumerator tailor made for non-involutory generators would be extremely desirable for exhibiting symmetric presentations of large groups, especially in light of conjectures A.1 and A.2. For such a program to work an adaptation of the procedure employed by the involutory symmetric generator will have to be developed. At present it is not clear if such a procedure could be developed to handle both progenitors defined by permutation actions and progenitors defined using monomial actions too. Furthermore, the possibility of non-cyclic symmetric generators may be of interest, especially given the possibility of exhibiting a symmetric presentation of the sporadic Rudvalis group using an image of the progenitor $A_5^{\star 1456}$:Sz(8), as noted in Chapter 1.

- Further Examples of Wreathed Extensions

  In Chapter 2 we saw a construction, the 'wreathed extension', that made it possible to extend a symmetric generating set of a small group to a symmetric generating set of a much larger one. Much of the point of wreathed extensions was that the construction could be used to extend a generating set no matter what action is being used to define it. In principal there should therefore be a whole plethora of examples of this construction at work.

  Alas, to date, essentially the only known examples are those given in Chapter 2. Additional examples, and in particular examples in which any member of an infinite family may be symmetrically generated in a generic way like the $SU_3(2^r)$ example from Theorem 2.4, would be of great interest. The most obvious analogue of Theorem 2.4 for the low dimensional symplectic groups is false.

  Since there is nothing about wreathed products that stops us from applying such a construction to non-involutory symmetric generators, it seems likely that further examples may have to be obtained using symmetric generators of higher order.

- Complex Reflection Groups

  In Chapter 3 we saw how the traditional Coxeter-Moser presentations for each of the finite simply laced Coxeter groups may be naturally arrived at purely by considering very natural actions of the symmetric groups. The author's work with Müller [40] later extended this result to a wider class of reflection groups meeting certain finiteness conditions. In particular this provided several families of infinite reflection groups with symmetric presentations, giving the first instance of an interesting infinite group being symmetrically generated.

  All of this work, however, applies solely to the reflection groups generated by involutory reflections. An attempt to extend these results to non-involtory reflections,

ie complex reflections, would be of great interest. Any attempt to make this generalization immediately hits the question of which action defines the progenitor - using higher order generators opens up the possibilities of using monomial representations to define progenitors. A naïve use of the classification of the finite complex reflection groups (first proved by Sheppard and Todd in [57]) to determine precisely which nodes of which diagrams require a permutation action or a monomial action (or perhaps even both) to define the corresponding progenitor would be of little interest in practice.

What would be of much greater interest would be some form of general easy-to-use condition telling us precisely when a particular node of a particular diagram defines what kind of progenitor and when we can obtain a symmetric presentation for the whole group from it. In particular if such a condition could be found that readily applied to not just finite complex reflection groups but infinite ones too then a substantial generalization of the results of Chapter 3 would become possible.

List of References

[1] P Abramenko and KS Brown "Buildings: Theory and Applications (Graduate Texts in Mathematics)" Springer (2008)

[2] J Adams "Character Tables for GL(2), SL(2), PGL(2) and PSL(2) over a Finite Field", preprint, University of Maryland (2002), available at `http://www.math.umd.edu/~jda/characters/characters.pdf`

[3] E Artin "The Free Product of Groups" American Journal of Mathematics, Vol. 69, No. 1 (1947), p.1-4

[4] M Aschbacher "On the Maximal Subgroups of the Finite Classical Groups" Inventiones Mathematicae 76 (1984), p.469-514

[5] B Bollobás "Modern Graph Theory (Graduate Texts in Mathematics, 184)", Springer-Verlag New York Inc. (1998)

[6] SW Bolt "Some Applications of Symmetric Generation" PhD, Birmingham, (2002)

[7] JD Bradley "Symmetric Presentations of Sporadic Groups" PhD, Birmingham, (2004)

[8] JN Bray "Symmetric Generation of Sporadic Groups and Related Topics" PhD, Birmingham, (1997)

[9] JN Bray and RT Curtis "A Systematic Approach to Symmetric Presentations. II. Generators of Order 3" Mathematical Proceedings of the Cambridge Philosophical Society 128 no. 1, (2000), p.1-20

[10] JN Bray and RT Curtis "Monomial Modular Representations and Symmetric Generation of the Harada-Norton Group", Journal of Algebra, 268 (2003), p.723-743

[11] JN Bray and RT Curtis "Double Coset Enumeration of Symmetrically Generated Groups" Journal of Group Theory 7 (2004), p.167-185

[12] JN Bray and RT Curtis "The Leech Lattice, Λ and the Conway Group $\cdot 0$ Revisited" accepted by the Transactions of the AMS

[13] JN Bray, RT Curtis and AMA Hammas "A Systematic Approach to Symmetric Presentations. I. Involutory Generators" Mathematical Proceedings of the Cambridge Philosophical Society 119 (1996), p.23-34

[14] JN Bray, RT Curtis, CW Parker and CB Wiedorn "Symmetric Presentations for the Fischer Groups I: the Classical Groups $Sp_6(2)$, $Sp_8(2)$, and $3^{\cdot}O_7(3)$" Journal of Algebra 265 (2003), p.171-199

[15] JN Bray, RT Curtis, CW Parker and CB Wiedorn "Symmetric Generation for the Fischer Groups II: the Sporadic Groups" Geometriae Dedicata 112 (2005), p.1-23

[16] PJ Cameron "Permutation Groups, London Mathematical Society Student Texts, 45", Cambridge University Press (1999)

[17] PJ Cameron "Notes on Classical Groups" available at `http://www.maths.qmul.ac.uk/~pjc/class_gps/`

[18] JJ Cannon *et al.* "The MAGMA Programming Language (various versions upto Version 2.8)" School of Mathematics and Statistics, University of Sydney (1993-2001)

[19] JH Conway, RT Curtis, SP Norton, RA Parker and RA Wilson "An ATLAS of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups", Oxford University Press (1985)

[20] JH Conway and NJA Sloane "Sphere Packing, Lattices and Groups" third edition Springer-Verlag, New York, (1998).

[21] HSM Coxeter "Discrete Groups Generated by Reflections" Annals of Mathematics (2) 35 no. 3, (1934), p.588-621

[22] RT Curtis "Symmetric Presentations I: Introduction with Particular Reference to the Mathieu Groups M_{12} and M_{24}" in 'Proceedings of the LMS Durham conference on 'Groups and Combinatorics" (1990)

[23] RT Curtis "Symmetric Presentations II: The Janko Group J_1" Journal of the London Mathematical Society (2) 47 (1993), p.294-308

[24] RT Curtis "Symmetric Generation of the Higman-Sims Group" Journal of Algebra 171 (1995) p.567-586

[25] RT Curtis "Monomial Modular Representations and Construction of the Held Group." Journal of Algebra 184 (3) (1996) p.1205-1227

[26] RT Curtis "A Survey of Symmetric Generation of Sporadic Simple Groups" in 'The Atlas of Finite Groups: Ten Years On.' (Birmingham, 1995), London Math. Soc. Lecture Note Ser., vol. 249, Cambridge University Press, (1998), p.39-57

[27] RT Curtis "Symmetric Generation and Existence of the Janko Group J_1" Journal of Group Theory 2 (1999), p.355-366

[28] RT Curtis "Symmetric Generation of Groups with Applications to many of the Sporadic Finite Simple Groups", Encyclopedia of Mathematics and Its Applications 111, Cambridge University Press (2007)

[29] RT Curtis and BT Fairbairn "Symmetric Representation of the Elements of the Conway Group ·0" accepted by Journal of Symbolic Computation

[30] RT Curtis and Z Hasan "Symmetric Representation of Elements of the Janko Group J_1" Journal of Symbolic Computation 22 (1996), p.201-214

[31] RT Curtis, AMA Hammas and JN Bray "A Systematic Approach to Symmetric Presentations. I. Involutory Generators" Mathematical Proceedings of the Cambridge Philosophical Society 119 (1996), p.23-34

[32] RT Curtis and S Whyte "The Irreducible Monomial Representations of the Covers of the Symmetric and Alternating Groups" preprint, Birmingham (2007)

[33] RT Curtis and S Whyte "Irreducible monomial representations of the sporadic simple groups and their covers", Birmingham (2007)

[34] LE Dickson "Linear Groups with an Exposition of the Galois Field Theory", Leipzig (1901), reprinted Dover (1958)

[35] DŽ Djoković and J Malzan "Monomial Irreducible Characters of the Symmetric and Alternating Groups.", Journal of Algebra, 35, (1975) p.153-158

[36] DŽ Djoković and J Malzan "Imprimitive, Irreducible Complex Characters of the Alternating Groups.", Canadian Journal of Mathematics, 28 (6), (1976) p.1199-1204

[37] BT Fairbairn "Computing in the Conway Group ·0" MPhil (qual), Birmingham, (2007)

[38] BT Fairbairn "Symmetric Presentations of Coxeter Groups" submitted to Proceedings of the Edinburgh Mathematical Society

[39] BT Fairbairn "A Note on Monomial Representations of Linear Groups" accepted by Communications in Algebra

[40] BT Fairbairn and J Müller "Symmetric Generation of Coxeter Groups" accepted by Archiv der Mathematik

[41] W Fulton and J Harris "Representation Theory, A First Course", Springer-Verlag (1991)

[42] RW Hartley "Determination of the Ternary Collineation Groups Whose Coefficients lie in the GF(2^n)", Annals of Mathematics 27 (1925/26), p.140-158

[43] H Hilton "Plane Algebraic Curves" Oxford University Press (1920)

[44] JE Humphreys "Reflection Groups and Coxeter Groups (Cambridge Studies in Advanced Mathematics)" Cambridge studies in advanced mathematics, Cambridge University Press (1997)

[45] IM Isaacs "Character Theory of Finite Groups (Dover books on advanced mathematics)", Dover Publications Inc (1994)

[46] C Jansen, K Lux, R Parker and R Wilson "An Atlas of Brauer Characters", Oxford University Press (1995)

[47] GD James "The Representation Theory of the Symmetric Group (Lecture Notes in Mathematics; 682)" Springer-Verlag (1978)

[48] OH King "The Subgroup Structure of Finite Classical Groups in Terms of Geometric Configurations", in 'Survey in Combinatorics, 2005' (ed BS Webb) Cambridge University Press 2006. Also available at `http://www.staff.ncl.ac.uk/o.h.king/KingBCC05.pdf`

[49] P Kleidman and M Liebeck "The Subgroup Structure of the Finite Classical Groups" London Mathematical Society Lecture Note Series, 129. Cambridge University Press (1990)

[50] S Lang "Algebra", Addison-Wesley (1965)

[51] K Magaard, personal correspondence

[52] HH Mitchell "Determination of the Ordinary and Modular Ternary Linear Groups", Transactions of the American Mathematical Society 12 (1911), p.207-242

[53] MS Mohamed "Computational Methods in Symmetric Generation of Groups" Phd thesis, Birmingham (1998)

[54] WA Simpson and J Sutherland-Frame "The Character Tables for SL(3,q), SU(3,q), PSL(3,q), PSU(3,q)" Canadian Journal of Mathematics, Vol. XXV, 3 (1973), p.486-494

[55] S Stanley "Monomial Representations and Symmetric Presentations" PhD, Birmingham, (1998)

[56] A Serres "Permutation Group Algorithms" Cambridge University Press (2003)

[57] GC Shephard and JA Todd "Finite unitary reflection groups" Canadian Journal of Mathematics 6, (1954) p.274-304

[58] JA Todd and HSM Coxeter "A Practical Method for Enumerating Cosets of Finite Abstract Groups" Proceedings of the Edinburgh Mathematical Society 5 (1936), p.26-34

[59] MM Virotte-Ducharme "Présentations des Groupes de Fischer. I" Geometriae Dedicata 41 (1992), p.275-335

[60] C Wiedorn "A Symmetric Presentation for J_1" Communications in Algebra, 31 (3) (2003) p.1329-1357

[61] RA Wilson "Standard Generators for the Sporadic Simple Groups" Bulletin of the London Mathematical Society 25 (1993), p.431-437

[62] RA Wilson *et al* "ATLAS of Finite Group Representations - Version 3" available at `http://brauer.maths.qmul.ac.uk/Atlas/v3/`

[63] S Whyte "Symmetric Generation: Permutation Images and Irreducible Monomial Representations" PhD, Birmingham, (2006)