SOME LINEAR CODES, GRAPHS AND DESIGNS FROM MATHIEU GROUPS M_{24} AND M_{23}

Vincent Nyongesa Marani

A Thesis submitted in fulfillment for the requirements of the award of the degree of Doctor of Philosophy in Pure Mathematics of Kibabii University.

May 2019.

Declaration

The research reported in this thesis was done under the supervision of Dr. Lucy Walingo Chikamai, Mathematics Department, Kibabii University and Prof. Shem Aywa, Mathematics Department, Kibabii University and it is the authors original work except where otherwise, due reference has been made . It has not been submitted before for any other degree or to any other institution.

Signature.. Date ....

Marani Vincent Nyongesa.

PHD/MAT/003/2014.

Declaration and Approval

We the undersigned certify that we have read and hereby recommend for acceptance of Kibabii University a thesis entitled," Some Linear Codes , Designs and Graphs from Mathieu Group M_{24} and M_{23}."

Signature... Date........................

Dr. Lucy Chikamai.

Department of Mathematics

Kibabii University.

Signature... Date.......................

Prof. Shem Aywa.

Department of Mathematics.

Kibabii University.

Copyright

Dedication

I dedicate this thesis to my daughters Joy Nakhumicha , Celia Nekoye and Ivy Naswa.

Acknowledgment

I would like to acknowledge my supervisors Dr. Lucy Chikamai and Prof. Shem Aywa for their guidance, patience and innumerable suggestions without which I would not have completed this thesis. I humbly appreciate the Kibabii University for offering me a chance to pursue my dreams in the institution and providing us with lecturers who are committed to their work. I also thank the University employees for their contributions towards my entire course and study work. Moreover, my thanks extend to the chairman of Mathematics Department Dr. Bonface Kwach , chairman of faculty board of science Prof. Donald Siamba and dean of school of Graduate Studies Prof.Stanely Mutsotso for advice in the entire study.

I also acknowledge my classmate Lydia for her moral support when writing this thesis. I thank my colleagues at work Mr. Mulati, Mr. Biwott, Mr. Magero, Mr. Mulambula, Mr. Sirengo and Mr. Kololi for their great support. Last but not least, I extend my sincere gratitude to my family especially my loving wife Jane Wanjala for her encouragement, understanding and support in the phases of academic endeavours.

Abstract

In this thesis, we have used four steps to determine G-invariant codes from primitive permutation representations of Mathieu groups M_{24} and M_{23} . We constructed all G-invariant codes from primitive representations of degree 24, 276, 759, and 1288 from the simple group M_{24}. We found one self dual [24, 12, 8] code, three irreducible codes; [276,11,128], [759,11,352] and [1288,11,648]. There were several decomposable, self orthogonal and projective linear binary codes. There were two strongly regular graphs from a representation of degree 276 and 759. These graphs are known. We determined designs from some binary codes using codewords of minimum weight. All the designs constructed were primitive. We constructed symmetric 1-designs from the primitive permutation representations of degree 24, 276, 759, 1771, 2024 and 3795 defined by the action of a group G on a set $\Omega = G/G_\alpha$. In most cases the full automorphism group of the design was M_{24} while in some cases the full automorphism group of the design was either S_{24} or S_{276}. We also constructed all G-invariant codes from primitive representations of degree 23, 253, and 253 from the simple group M_{23}. There was no self dual linear code. There were four irreducible codes [23,11,8], [253,11,112],[253,44] and [253,11,112] . There were several decomposable, self orthogonal and projective linear binary codes. There was no strongly regular graph from the three representations. We determined designs from some binary codes using codewords of minimum weight. All the designs constructed were primitive. We constructed symmetric 1-designs from the primitive permutation representations of degree 23, 253 and 253 defined by the action of a group G on a set $\Omega = G/G_\alpha$. In most cases the full automorphism group of the design was M_{23} while in some cases the full automorphism group of the design was either S_{23}, S_{253} or S_{506}

Symbols and abbreviations

$\mathbb{N}$	Set of Natural numbers
$\mathbb{Z}$	Set of Integers
$\mathbb{R}$	Set of Real numbers
$\mathbb{C}$	Set of Complex numbers
Ω	A finite set
$\mathbf{1}$	The all ones vector
S_n	the symmetric group on n symbols
V	Vector space
$\mathbb{F}$	A finite field
$\mathbb{F}_q$	A finite field of q elements
Char($\mathbb{F}$)	Characteristic of a field $\mathbb{F}$
Aut(G)	Automorphism group of group G
I_G	The identity element of G
K $<$ G	K is a subgroup of G
K $\lhd$ G	K is a normal subgroup of G
$\|G\|$	Order of a group G
H $\cong$ G	H is Isomorphic to G
$[n, k, d]_q$	A q-ary code of length n, dimension k and minimum distance d
C	A linear code
(P, B)	An incidence structure with P points and B blocks
Γ	Graph
PG(V)	The projectile geometry
FG	Group algebra
$\mathbb{F}\Omega$	$\mathbb{F}$G -module
GL$_n$(q)	General linear group of dimension n over F$_q$
#	Number of Orbits

Table of Contents

Declaration **ii**

Declaration and Approval **ii**

Copyright **iii**

Dedication **iv**

Acknowledgments **v**

Abstract **vi**

Symbols and abbreviations **vii**

Table of Contents **viii**

1 Introduction **1**

2 Basic Concepts **5**

2.1 Groups 5

2.2 Rank-3 Primitive permutation groups 7

2.3 Representations 7

2.4 $\mathbb{F}G$ - modules 8

2.5 Binary Linear Codes 9

2.6 Designs 12

2.7 Graphs 13

3 Constructions of Combinatorial Structures **15**

3.1 Codes from primitive groups 15

3.2 Designs from primitives groups 16

3.3 Construction of G-invariant codes 17

3.4 Strongly Regular Graphs from Two Weight Codes 17

4 Mathieu Group M_{24} **20**

4.1 The Representation of Degree 24 21
4.2 The Representation of Degree 276 25
4.3 The Representation of Degree 759 32
4.4 The Representation of Degree 1288 39
4.5 Representation of Degree 1771 46
4.6 The Representation of Degree 2024 50
4.7 The Representation of Degree 3795 54
4.8 Conclusion 58

5 Mathieu Group M_{23} **59**

5.1 The Representation of Degree 23 60
5.2 The 1^{st} Representation of Degree 253 65
5.3 The 2nd Representation of Degree 253 71
5.4 The Representation of degree 506 77
5.5 Conclusion 84

References **86**

Appendices **90**

Chapter 1

Introduction

This thesis is a study of linear codes obtained from primitive permutation representations of Mathieu Groups M_{24} and M_{23}. Many communication channels are subject to channel noise, and thus errors may be introduced during transmission from the source to a receiver. Codes are used to detect and correct errors that occur when data is transmitted across some noisy channel. We Construct and Enumerate G-invariant codes from M_{24} and M_{23}. We Classify some G invariant codes and determine properties of some binary codes. We establish the linkages between some linear codes and designs, graphs and finite geometries from primitive groups.

Given a permutation group G acting on a set Ω of n points, a binary code $C(G, \Omega) = \langle Fix(\sigma) | \sigma \in I(G) i^{\perp} \rangle$ was constructed in [27] , where $I(G)$ is the set of involutions of G and Fix$(\sigma) = \{\omega \in \Omega | \omega^{\sigma} = \omega\}$ is the set of fixed points of the permutation ω, i.e., $C(G, \Omega)$ is the code generated by the sets of fixed points of involutions of the group. They used representation theoretic methods to obtain the permutation representation of G on the cosets of a subgroup H of G. They treated Ω as the set G/H where H was chosen such that $|G : H| = n.$. The code obtained was very useful in the search for self-dual codes which were invariant under the action of the group G. Further, every self-dual code C was such that $C(G,\Omega)^{\perp} \subset C \subset C(G,)$. This provided a good starting point for the search of G-invariant self-dual codes. Using libraries of groups in the computer algebra packages GAP and MAGMA , they constructed codes invariant under some sporadic simple and almost simple groups of degree ≤ 2000.

In [9], the authors constructed G-invariant codes as outlined. Given a finite field of $q = p^k$ elements, where p is a prime and $k \in \mathbb{Z}$, and G a finite group acting primitively on the set Ω, then $V = \mathbb{F}\Omega$ is a vector base over $\mathbb{F}$ of all linear combinations of $\sum \lambda_i \alpha$, $\lambda_i \in \mathbb{F}$, $\alpha \in \Omega$. Considering the action of the elements of G on the basis elements of V defined by $\rho : G \to GL(V)$ where $\rho(g)(x) = g(x)$ with $g \in G$ and $x \in V$ and extending linearly the induced action of V makes V into an $\mathbb{F}\Omega$-module called the permutation module over $\mathbb{F}G$. The submodules of this permutation module are all the p-codes invariant under the group G.

In chapter 2, we have discussed the basic terms from the theory of finite groups, group representations, FG-modules and the combinatorial structures; codes, designs and graphs. In Chapter 3 we have discussed the construction of Codes from primitive groups. In this construction we find the permutation module from the primitive group. For this we decompose the permutation module into all submodules. These constitute the building blocks for the construction of a lattice of submodules. The chapter also describes the construction of designs from primitive groups using orbits of the point stabilizer.

In Chapter 4, we have constructed all G-invariant codes from primitive representations of degree 24, 276, 759, and 1288 from the simple group M_{24}. The computations were carried recursively in Magma with a built-in component of Meat-Axe. We constructed some linear binary codes with minimum distance of small dimensions due to computer limitations and found one self dual [24, 12, 8] code, three irreducible codes; [276,11,128], [759,11,352] and [1288,11,648]. There were several decomposable, self orthogonal and projective linear binary codes. There were two strongly regular graphs from a representation of degree 276 and 759. These graphs are known. We determined designs from some binary codes using codewords of minimum weight. All the designs constructed were primitive. We constructed symmetric 1-designs from the primitive permutation representations of degree 24, 276, 759, 1771, 2024 and 3795 defined by the action of a group G on a set $\Omega = G/G_\alpha$. In most cases the full automorphism group of the design was M_{24} while in some cases the full automorphism group of the design was either S_{24} or S_{276}

In Chapter 5, we have constructed all G-invariant codes from primitive representations of degree 23, 253, and 253 from the simple group M_{23}. There was no self dual linear code. There were four irreducible codes [23,11,8], [253,11,112],[253,44] and [253,11,112] . There were several decomposable, self orthogonal and projective linear binary codes. There was no strongly regular graph from the three representations. We determined designs from some binary codes using codewords of minimum weight. All the designs constructed were primitive. We constructed symmetric 1-designs from the primitive permutation representations of degree 23, 253 and 253 defined by the action of a group G on a set $\Omega = G/G_{\alpha}$. In most cases the full automorphism group of the design was M_{23} while in some cases the full automorphism group of the design was either S_{23}, S_{253} or S_{506}

Chapter 2

Basic Concepts

In this chapter we select some standard results from the theory of groups, designs, codes and graphs which will be required in the subsequent chapters. For a more detailed account and additional information the reader is advised to consult [1,2,3,7,9, 16 ,23,24].

2.1 Groups

The symmetric group on a set Ω is the group S_Ω of all permutations of Ω. A permutation group G on a set Ω is a subgroup of S_Ω, and G is said to be transitive on Ω if, for all $\alpha, \beta \in \Omega$, there exists an element $g \in G$ such that the image α^g of α under g is equal to β.

Definition 2.1.1. *Suppose G is a group and Ω is a set. An a group G action on Ω is a function which relates to every $\alpha \in \Omega$ and $g \in G$ an element $g\alpha$ of Ω such that, for all $\alpha \in \Omega$ and all g, $h \in G$, $\alpha^1 = \alpha, h\Big(g\alpha\Big) = (gh)\alpha$.*

In natural way , an action defines a permutation representation of G on Ω which is a homomorphism ψ from G into S_Ω. Conversely a permutation representation naturally defines an action of G on Ω.

Theorem 2.1.2. *A transitive action of a group G on a subgroup H is equivalent to the action of G on a set of coset G/H and is a quotient group if $H \lhd G$.*

Definition 2.1.3. *Suppose G acts on a set Ω. Suppose $\Omega = n$ and k are positive integers. G is k-transitive on Ω if every two ordered k-tuples.*

$(\alpha_1, \alpha_2, \cdots \alpha_k)$ and $(\beta_1, \beta_2, \cdots \beta_k)$ with $\alpha_i \neq \alpha_j$ for $i \neq j$ there exist $g \in G$ such that $\alpha_i^g = \beta_i$ for $i = 1, 2, \cdots, k$.

Lemma 2.1.4. *Suppose G is a transitive group on a set $\Omega||\Omega| = n \geq 2$. If G_α is $(k-1)$ transitive on Ω for any $\alpha \in \Omega$ then G is k-transitive on Ω.*

Definition 2.1.5. *The automorphism group $Aut(G)$ of a group G, is the set of all automorphisms of G .*

Definition 2.1.6. *Suppose g is an element of G. We define $\phi_g : G \to G$ by $\phi_g(x) = gxg^{-1}$ for any $x \in G$. Then ϕ_g is an automorphism of G , known as an* ***Inner automorphism*** *of G.*

Definition 2.1.7. *A permutation group G is* ***primitive*** *on Ω if G is transitive on Ω and the only G-invariant partitions of Ω are the trivial partitions. Also G is* ***imprimitive*** *on Ω if G preserves some non-trivial partition on Ω.*

Theorem 2.1.8. *For every n , the symmetric group S_n acts n-transitively on $\Omega = \{1, 2, \cdots, n\}$,*

Theorem 2.1.9. *Every k-transitive group G (with $k \geq 2$) acting on a set Ω, is primitive.*

Theorem 2.1.10. *(Characterization of primitive permutation groups) Let G be a transitive permutation group on a set Ω. Then G is primitive if and only if for each $\alpha \in \omega$, the stabilizer G_α is a maximal subgroup of G.*

2.2 Rank-3 Primitive permutation groups

Suppose G is a transitive permutation group on Ω, then the number of orbits of the point stabilizer G_α is independent of the particular $\alpha \in \Omega$ and is the rank of G. If G is a transitive permutation group on Ω of rank-3 then G is a rank-3 permutation group. In this case G_α has exactly three orbits $\alpha, \Delta(\alpha)$ and $\Gamma(\alpha)$. For more information on rank-3 permutation groups the reader should consult [6,8,12,17, 18,20,21].

2.3 Representations

Definition 2.3.1. *Suppose G is a finite group and V is a vector space of dimension n over the field $\mathbb{F}$. Then a homomorphism $\rho : G \to GL(n, \mathbb{F})$ is a matrix representation of G of degree n over the field $\mathbb{F}$.*

Definition 2.3.2. *Suppose $\rho : G \to GL(n, \mathbb{F})$ is a representation of G on a vector space $V = \mathbb{F}^n$. Suppose W is a subspace of V of dimension m such that $\rho_p(W) \subsetneq W$ for all $g \in G$, then the map $\rho : G \to GL(m, \mathbb{F})$ is a representation of G called a* ***subrepresentation*** *of ρ. The subspace W is said to be G-invariant.*

Definition 2.3.3. *A representation $\rho : G \to GL(n, \mathbb{F})$ of G with representation module V is called reducible if there exists a proper non-zero G-subspace U of V and it is irreducible if the only G-subspaces of V are the trivial ones.*

The $\rho-$ invariant subspaces of a representation module V are called submodules of V .

Definition 2.3.4. *Suppose $\rho : G \to GL(V)$ is a representation of G on a vector space V. If there exists G-invariant subspaces U and W such that $V = U \bigoplus W$ then is called decomposable.*

Definition 2.3.5. *A representation ρ is e completely reducible if it is the direct sum of irreducible representations.*

2.4 $\mathbb{F}G$ - modules

The results of $\mathbb{F}G$-modules carry over from representations.There is a 1-to-1 correspondence between representations of G and $\mathbb{F}G$ - modules.

Definition 2.4.1. *Suppose G is a finite group and $\mathbb{F}$ is a field. Then a group ring of G over $\mathbb{F}$ is the set of all sums of the form*

$\Sigma_{g \in G} \lambda_g g, \lambda_g \in \mathbb{F}$

with componentwise addition and multiplication.

Theorem 2.4.2. *Suppose $\mathbb{F}$ is a field and G is a finite group, then there is a bijective correspondence between finitely generated $\mathbb{F}G$-modules and representations of G on finite-dimensional $\mathbb{F}$-vector spaces.*

The definitions that follow have their equivalent stated in representation theory in section 2.3.

Definition 2.4.3. *Suppose V is an $\mathbb{F}G$-module, a subspace W of V is called an $\mathbb{F}G$-submodule of V i.e.,$gw \in W$, for all $w \in W$.*

Definition 2.4.4. *An $\mathbb{F}G$-module V is called simple or irreducible if it has no other submodules apart from the trivial submodules. A module which is not irreducible is called reducible.*

Definition 2.4.5. *Let V be an $\mathbb{F}G$-module. We say V is decomposable if it can be written as a direct sum of two $\mathbb{F}G$-submodules. i.e., there exist submodules U and W of V such that$V = U \bigoplus V$. If V can be written as a direct sum of irreducible submodules then it is called completely reducible.*

Definition 2.4.6. *Suppose V and W are $\mathbb{F}G$-modules. Then a function $\tau : V \to W$ is an $\mathbb{F}G$-homomorphism if τ is a linear transformation and for any $v \in V, g \in G$, $\tau(gv) = g\tau(v)$. A bijective homomorphism is called an isomorphism.*

Theorem 2.4.7. *Two $\mathbb{F}G$-modules are isomorphic if and only if they have equivalent representations.*

Definition 2.4.8. ***A composition series** for an $\mathbb{F}G$-module V is a series of submodules of the form $V = V_0 \supseteq V_1 \supseteq ... \supseteq V_t = 0$.*

2.5 Binary Linear Codes

Definition 2.5.1. *A linear binary code C is a subspace of $\mathbb{F}_2^n$. It is denoted as (n, k)-code. **Codewords** are the vectors of C .*

Definition 2.5.2. *Suppose $x \in V$ and $X = \{i_1, i_2, \cdots, i_k\} \subseteq \{1, \cdots, n\}$ are the nonzero coordinates of x . Then $x = (1000011) = e_1 + e_6 + e_7$ is represented as $X = \{1, 6, 7\}$.*

Definition 2.5.3. *The **Humming distance** $d(u, v)$ between vectors $u, v \in C$ is the number of coordinates in which they differ .*

Lemma 2.5.4. *The Hamming distance between any vectors is a metric on $\mathbb{F}_2^n$.*

Proof. See [9] $\square$

Definition 2.5.5. *The Hamming Weight $wt(v)$ of a vector is the number of nonzero components it possesses.*

Lemma 2.5.6. *We have $d(u, v) = wt(u - v)$ for all $u, v \in \mathbb{F}_{\not=}^{\ltimes}$,.*

Proof. See [16] $\square$

Definition 2.5.7. *An (n, k)-code of minimum weight d of its nonzero codewords is known as an (n, k, d)-code.*

Definition 2.5.8. *Suppose C is a code , and A_k is the number of codewords of weight k. Then the weight numerator of C is the polynomial*

$$\sum_{k=0}^{n} A_k x^{n-k} y^k.$$

Definition 2.5.9. *Suppose C is a code in V , then $C^\perp$ is the dual code or orthogonal code of C.*

Theorem 2.5.10. *Suppose C is an (n, k)-code, then $C^\perp$ is referred to as an $(n, n-k)$ code.*

Definition 2.5.11. *A binary code is is referred to as **even** if the weight of all its codewords is divisible by 2.*

Lemma 2.5.12. *a binary self-orthogonal code C is even.*

Proof. see [16] $\square$

Definition 2.5.13. *A binary code is **doubly even** if the weight of all its codewords are divisible by 4.*

Lemma 2.5.14. *A double even code is self-orthogonal.*

Proof. see [16] $\square$

Theorem 2.5.15. *Suppose C is a binary (n, k)-code. Suppose the weight of vectors of a generating set S are divisible by 4 and are pairwise orthogonal. Then C is doubly even .*

Proof. see [16] $\square$

Definition 2.5.16. *An (n, k)-code is self-dual if $C = C^{\perp}$*

Theorem 2.5.17. *If C is a self-dual (n, k)-code , then $k = n/2$.*

Proof. see [9,16] $\square$

Definition 2.5.18. *Let C be a binary (n, k)-code. An **automorphism** of C is an element of S_n that sends codewords to codewords. The **automorphism group** of C is*

$$Aut(C) = \{\pi \in S_n | c\pi \in C for\ all c \in C$$

Definition 2.5.19. *A code with its dual distance at least 3 is called projective .*

2.6 Designs

Definition 2.6.1. ***An incidence structure*** *is a set $I = (\rho, \beta, I)$, where ρ is the point set, β is the block set and I is an incidence relation between ρ and β. The elements of I are called flags.*

Definition 2.6.2. *A $t-$ design or more a $t-(v,k,\lambda)$ design is an incidence structure $D = (\rho, \beta, I)$ such that $\mid \rho \mid= v,$, $B \in \beta$ is incident with k points and t distinct points are together incident with λ blocks. A symmetric design is a design with the same number of points and blocks.*

Theorem 2.6.3. *Suppose D is a $t-(v,k,\lambda)$ design and for 1$\leq s \leq t$,. Then D is a $s-(v,k,\lambda)$ design where*

$$\lambda_s = \lambda \frac{(v-s)(v-s-1)\cdots(v-t+1)}{(k-s)(k-s-1)\cdots(k-t+1)}.$$

Definition 2.6.4. *Suppose $D = (P, \beta, I)$ is a design in which $P = \{p_1, p_2, \cdots p_v\}$ and $B = \{B_1, B_2 \cdots B_i\}$. Then the* ***incidence matrix*** *of D is $ab \times v$ matrix $A = (a_{ij}$ such that*

$$a_{ij} = \begin{cases} 1, & \text{if} \quad (p_i, B_j) \in I \\ 0, & \text{if} \quad (p_i, B_j) \notin I \end{cases}$$

Definition 2.6.5. *A* ***Steiner system*** *is a $t-(v,k,1)$ design for integers $1 < k < v$. [9].*

Definition 2.6.6. *Two designs $D' = (P', B', I')$ and $D = ((P, B, I)$ are said to be isomorphic if there exist a bijection $\emptyset$ from P' to P . A bijection from a design D to itself is referred to as an automorphism. $aut(D)$ denotes the group of all automorphism .*

Definition 2.6.7. *An automorphism group of a design is said to be **flag-transitive** if it is transitive on the flags .*

Definition 2.6.8. *An automorphism group of a design is **t-flag-transtive** if it is transtive on the blocks and a block stabilizer is t-transitive on the point of that block.*

2.7 Graphs

We are concerned with strongly regular graphs whose definition reflects the symmetry inherent in t-designs.

Definition 2.7.1. *A **graph** is a double $\Gamma = (V, E)$, where V is a finite set of vertices and E is a set of edges .*

If x is a vertex for a graph Γ, the **valency** of x is the number of edges containing x. If all vertices have the same valency, the graph is called regular, and the common valency is the valency of the graph. Thus an arbitrary graph is a 0-design, with block size $k = 2$. A regular graph is a 1-design.

Definition 2.7.2. *A **strongly regular graph** (n, k, λ, μ) is a graph Γ with n vertices, k edges, common number of vertices λ from adjacent edges and common number n of vertices from non-adjacent edges respectively.*

Let G be a rank-3 group of even order and let O_1, and O_2 be two orbitals other than the diagonal. Then G contains an involution τ. Some pair x, y of distinct points are interchanged by an element of G. Suppose that $(x, y) \in O_1$, then every pair in O_1 is interchanged by an element of G. So we can take the set of unordered pairs x, y for which $(x, y) \in O_1$ as the edge of a graph Γ on V. The fact that O_1 and O_2 are orbitals implies that the number of common neighbours of two adjacent vertices, or two non-adjacent vertices, is constant; and the transitivity of G shows that Γ is regular. So Γ is a rank-3 strongly regular graph.

We have established a relationship between groups, designs, modules and codes. The interplay between these combinatorial structures will become evident in Chapter 3.

Chapter 3

Constructions of Combinatorial Structures

This chapter provides the techniques that are used throughout this work to construct codes, designs and graphs . Section 3.1 describes how to construct codes from primitive groups. Section 3.2 describes how to construct designs from primitive groups. Section 3.3 describes how to construct codes from combinatorial designs and finally Section 3.4 describes how to construct strongly regular graphs from two weight codes. From these four methods we extract algorithms that were implemented with the software package MAGMA. For a more detailed account and additional information the reader is advised to consult [1,2,3,4,5,7, 9 ,16, 19].

3.1 Codes from primitive groups

The construction requires that we find the permutation module. For this we decompose the permutation module into all submodules. These constitutes the building blocks for the construction of a lattice of submodules , thus attaining an answer to the enumeration problem. With the characterization of these codes we respond to the problem of classification of the codes.

Decomposition of the modules into submodules depends on the field. Maschkes Theorem gives a characterization of decomposition over a field whose characteristic is 0 or relatively prime to the order of the group. In this case the permutation module is completely reducible and can be written as a direct sum of its irreducible submodules. When the characteristic p of the field divides the order of the group i.e., $p||G|$, we apply Krull-Schmidts Theorem which shows that any module with finite length can be written as a direct sum of indecomposable submodules. In addition to Krull-Schmidt theorem, we have the composition series of the module which provides a way of breaking the module into simple components. These concepts have been used to develop different methods to construct submodules hence codes invariant under a group.

For each primitive representation of a given permutation group G, we use Meat-Axe recursively and Magma [17] to construct the associated permutation module over $\mathbb{F}_2$ and subsequently a chain of its maximal submodules. Each maximal submodule contains a binary code that is invariant under G. The G-invariant subspaces of the permutation module give all the p-ary codes invariant under G.

3.2 Designs from primitives groups

This section describes how to construct designs from primitive groups more precisely;

Theorem 3.2.1. { *Key-Moori Method 1*} *Suppose G is a finite primitive permutation group acting on set X of size n. Suppose $x \in X$, and $\Delta \neq \{x\}$ is an orbit of G_x, the stabilizer of x. If $B = \{\Delta^g : g \in G\}$, then $D = (X, B)$ is a symmetric 1-$(n, |\Delta|, |\Delta|)$ design, with G acting as an automorphism group, primitive on blocks and points of the design.*

Proof. see [19] □

Theorem 3.2.2. *The blocks of any symmetric 1-design with an automorphism group G acting primitively on points can be constructed as a union of orbits of the G-stabilizer.*

Proof. see [19] □

3.3 Construction of G-invariant codes

Given a permutation group G acting on a finite set Ω, and $\rho : G \cong GL(V)$ where $\rho(g)(x) = g(x)$ with $g \in G$ and$x \in V$,we can find all codes with a group G acting as an automorphism group. The steps are as follows:

1 . Recognize $\mathbb{F}_2\Omega$ as a permutation module;

2 .Using Meat-Axe find all non-isomorphic$\mathbb{F}_2G$ -submodules

3 .By Lemma 6.19 [9] the submodules are the G-invariant codes;

4 . Determine where possible the lattice structure of the permutation module;

The steps in this thesis show that we can get the non-isomorphic $\mathbb{F}_2G$-submodules using Meat-Axe without necessarily finding all the maximal $\mathbb{F}_2G$-submodules, testing equivalence and filtering isomorphic copies.

3.4 Strongly Regular Graphs from Two Weight Codes

A linear code C is called a two weight code if it has only two non-zero weights w_1 and w_2 and any two of its coordinates are linearly independent ,[1,4,5,12,18].

Strong connections exist between projective two weight codes and strongly regular graphs which we shall briefly discuss. Every projective two-weight code over a finite field has a strongly regular graph. This was first established by Delsarte ([12], Theorem 2) who then gave the connection between them .

Theorem 3.4.1. *([5], Theorem 2). Suppose w_1 and w_2 (where $w_1 < w_2$) is the weights of a q-ary projective two-weight code C of length n and dimension k. To C we associate a graph $\Gamma(C)$ as follows. The vertices of the graph are identified with the $v = q^k$ codewords and two vertices corresponding to x and y are adjacent iff $d(x, y) = w_1$. Then $\Gamma(C)$ is a strongly regular.*

Proof: See [5] Corollary 3.7

Calderbank [5] gave another construction of the strongly regular graph from projective two weight code and further determined the graphs parameters from the parameters of the code. The parameters (N, K, λ, μ) of a strongly regular are determined in ([5] where;

$$N = q^k$$

$$K = n(q-1)$$

$$\lambda = K^2 + 3K - q(w_1 + w_2) - Kq(w_1 + w_2) + q^2 w_1 w_2$$

$$\mu = \frac{q^2 w_1 w_2}{q^k} = K^2 + K - Kq(w_1 + w_2) + q^2 w_1 w_2$$

In chapters 4 and 5 we shall see how a combination of these techniques outlined in sections (3.1, 3.2, 3.3, 3.4, 3.5, 3.6) help determine and classify a number of interesting codes invariant under the simple Mathieu groups M_{24} and M_{23}.

Chapter 4

Mathieu Group M_{24}

Mathieu group M_{24} is described as the automorphism group of a Steiner system $S(5, 8, 24)$ on 24 objects. It is a 5-transitive permutation group . Mathieu groups are related to Conway groups because the Leech lattice and the binary Golay code are both found in spaces of length 24. [16].

Mathieu group M_{24} has seven primitive permutation representations of degree 24, 276, 759, 1288, 1771, 2024 and 3795 respectively as indicated in the Atlas [26]. The seven primitive permutation representations are as shown in the table 4.1, where the first column gives the structure of the maximal subgroups; the second gives the degree (the number of cosets of the point stabilizer); the third gives the order of the maximal subgroups; the fourth gives the number of orbits of the point-stabilizer, and the fifty,sixty and seventh column give the dimension of the orbits.

The primitive representations are described as the action of the group G on duad, octad, duum, sextet,triad and trio geometrical objects respectively. The elements of each degree generate a permutation module over $\mathbb{F}_2$. We determine orbits of the point stabilizer through cosset action of G on the maximal subgroups.

Table 4.1: Maximal Subgroups of M_{24} .

Max.sub	Degree	Order	#	Length	Length	Length	Length
M_{23}	24	10200960	2	23			
$M_{22} : 2$	276	887040	3	44	231		
2^4: A_8	759	322560	4	30	280	448	
$M_{12} : 2$	1288	190080	3	495	792		
$2^6 : 3.S_6$	1771	138240	4	252	483	1035	
$L_3(4) : S_3$	2024	120960	5	23	252	483	1265
$2^6 : (L_3(2) : S_3)$	3795	64512	5	252	483	1035	2024

4.1 The Representation of Degree 24

For a permutation group G acting on a finite set Ω, of degree 24 we construct a 24-dimensional permutation module invariant under G. We take the permutation module to be our working module and recursively find all submodules . The recursion stops as soon as we obtain all submodules. We find that permutation module breaks into submodules of dimension 1, 12 and 23. This submodules are the building blocks for the construction of a submodule lattice as shown in Figure 4.1

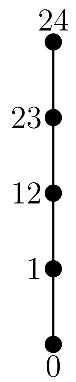


Figure 4.1: Submodule lattice of the 24 dimensional permutation module

The lattice diagram shows that there is only one irreducible submodule of dimension 1.

The authors in [9] used slightly different approach to the one described above. They split the permutation module into maximal submodules. They took the permutation submodule to be the working module and recursively found all maximal submodules of each module. The recursion terminated as soon as it reached an irreducible maximal submodule. In so doing they determined all codes associated with the permutation module invariant under G. This approach is cumbersome since it involves every time testing equivalence and filtering out isomorphic copies. Our approach has the advantage that the permutation module show up as non isomorphic submodules. In this case we produce the submodules more directly.

We obtain only one non trivial submodule of dimension 12. The binary linear code with minimum distance from this representation is [24,12,8]. We shall denote the code $C_{24,1}$ and its dual $C_{24,1}^{\perp}$ Table 4.2 shows the weight distribution of these codes

.

Table 4.2: Weight distribution of codes of length 24

name	dim	0	8	12	16	24
$C_{24,1}$	12	1	759	1256	759	1
$C_{24,1}^{\perp}$	12	1	759	1256	759	1

We make some observations about the properties of these codes in Proposition 4.1.1.

Proposition 4.1.1. *Let G be a primitive group of degree 24 of the Mathieu group M_{24} and $C_{24,1}$ a binary code of dimension 12 . Then $C_{24,1}$ is self dual, doubly even and projective $[24, 12, 8]_2$ code of weight 8 with 759 words. Furthermore Aut($C_{24,1}$) $\cong S_{24}$.*

Proof

From weight distribution, we deduce that codewords have weights divisible by 4. Since the weights of this codewords are divisible by 4, $C_{24,1}$ is doubly even. Since the dimension of $C_{24,1}$ is half its length $C_{24,1}$ is self dual. The code $C_{24,1}^{\perp}$ is of weight 8. Hence $C_{24,1}$ is projective. For the structure of the automorphism group, let $\overline{G} \cong C_{24,1}$. $\overline{G}$ has only one composition factor M_{24} . We conclude that $\overline{G} \cong M_{24}$ □

Deigns of codewords of minimum weight in $C_{24,1}$

We determine designs held by the support of codewords of minimum weight w_m in $C_{24,1}$. In Table 4.3 columns one, two, three and four respectively represents the code $C_{24,1}$ of weight m , the parameters of the 5-designs D_{w_m} , the number of blocks of D_{w_m}, and tests whether or not a design D_{w_m} is primitive under the action of Aut(C).

Table 4.3: Deigns of codewords of minimum weight in $C_{24,1}$

weight m	D_{w_m}	No of Blocks	primitivity
8	5-(24, 8, 1)	759	yes

Remark 4.1.2. *From the results in table 4.3 we observe that D_{w_m} is primitive.*

Symmetric 1- designs

Using the orbits of the point stabilizers in theorem 3.1 and theorem 3.2 we construct symmetric 1 - designs from the simple Mathieu group M_{24}. We examine symmetric 1-design invariant under G constructed from orbits of the rank - 2 permutation representation of degree 24. The first column in Table 4.4 represents the 1-design D_k of orbit length k, the orbit length in the second column , the parameters of the symmetric 1-design D_k in the third column and the automorphism group of the design the last column .

Table 4.4: symmetric 1-Design

Design	orbit length	parameters	Automorphism Group
D_{23}	23	1-(24,23,23)	S_{24}

Proposition 4.1.3. *Let G be the primitive group of degree 24 of the mathieu group M_{24}. Let $\beta = \{\triangle^g \colon g \in G\}$ and $D_k = (\Omega, \beta)$. Then the Aut(D_k) $\cong S_{24}$*

Proof

The composition factors of D_k are $\mathbf{Z}_2$ and A_{24}. This implies that Aut$D_{23} \cong S_{24}$ □

Theorem 4.1.4. *Let G be the primitive group of degree 24 of M_{24} and C a linear code admitting G as an automorphism group . Then the following holds:*

(a) There exist a self dual doubly even projective code.

(b) There exist a Primitive Design related to M_{24}.

(c) $AutD_{23} \cong S_{24}$ *for primitive symmetric 1-design*

Proof

(a) See proposition 4.1.1

(b) See table 4.3

(c) See table 4.4

4.2 The Representation of Degree 276

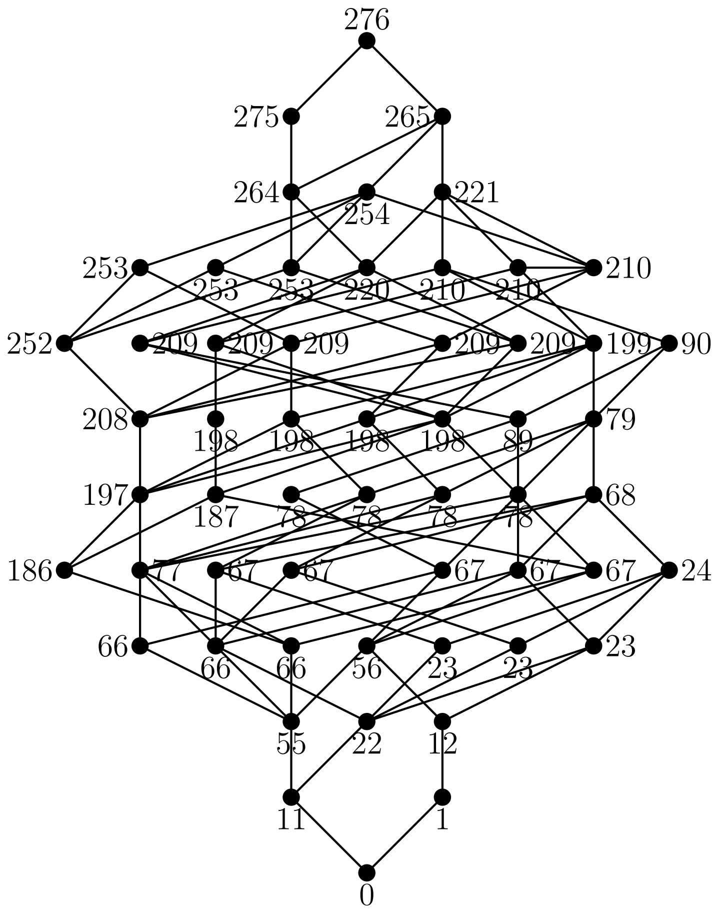
We construct a 276-dimensional permutation module invariant under permutation group G acting on a finite set Ω, of degree 276. We take the permutation module to be our working module and recursively find all submodules . The permutation module splits into 56 submodules. The submodules are the dimensions of the codes related to permutation module. The permutation module breaks into six completely irreducible parts of dimensions 1, 11,11, 44, 44 and 120 with multiplicities 2, 3, 3, 1, 1, and 1 respectively. The submodules are shown in Table 4.2. Column k represents the dimension of the submodule and # the number of the submodules of each dimension.

This submodules are the building blocks for the construction of a submodule lattice as shown in Figure 4.2

Table 4.5: submodules from 276 permutation module

k	#	k	#	k	#	k	#	k	#
0	1	55	1	79	1	208	1	254	1
1	1	56	1	89	1	209	5	264	1
11	1	66	3	90	1	210	3	265	1
12	1	67	5	186	1	220	1	275	1
22	1	68	1	187	2	221	1	276	1
23	3	77	4	198	4	252	1		
24	1	78	4	199	1	253	3		

Figure 4.2: Submodule lattice of the 276 dimensional permutation module



From the lattice diagram, we see that the submodules of dimension 1 and dimension 11 are irreducible .

We discuss five non trivial submodules of small dimensions 11, 12, 22, 23 and 24 .

The binary linear codes of these submodules are represented in table 4.6.

Table 4.6: codes of small dimension

Name	Dimension	parameters	Name	Dimension	Parameters
$C_{276,1}$	11	$[276,11,128]_2$	$C_{276,5}$	23	$[276\ ,23,44]_2$
$C_{276,2}$	12	$[276,12,128]_2$	$C_{276,6}$	23	$[276,23,44]_2$
$C_{276,3}$	22	$[276,22,44]_2$	$C_{276,7}$	24	$[276,24,23]_2$
$C_{276,4}$	23	$[276,23,23]_2$			

We make some observations about the codes. These properties are examined with certain detail in Proposition 4.2.1.

Proposition 4.2.1. *Let G be a primitive group of degree 276 of the Mathieu group M_{24} and $C_{276,1}$, $C_{276,2}$, $C_{276,3}$, $C_{276,6}$,$C_{276,7}$ be binary codes of dimension 11, 12, 22, 23, 24 respectively .Then the following holds;*

i $C_{276,1}$ *is self orthogonal, doubly even and projective [276, 11,128] binary code . [276, 265, 3] is the dual of* $C_{276,1}$ *. Furthermore* $C_{276,1}$ *is irreducible and* $Aut(C_{276,1}) \cong M_{24}$

ii $C_{276,2}$ *is self orthogonal, doubly even and projective [276, 12,128] binary code . [276, 264, 4] is the dual of* C_{12} *. Furthermore* $Aut(C_{276,2}) \cong M_{24}$

iii $C_{276,3}$ *is self orthogonal, doubly even and projective [276, 22, 44] binary code . [276, 254, 3] is the dual of* $C_{276,3}$ *. Further more* $Aut(C_{276,3}) \cong S_{24}$

iv $C_{276,6}$ *is self orthogonal, doubly even and projective [276, 23,44] binary code . [276, 253, 4] is the dual of* $C_{276,6}$ *. Further more* $C_{276,6}$ *is decomposable and* $Aut(C_{276,6}) \cong S_{24}$

proof

i The polynomial of $C_{276,1}$ is $W(x) = 1 + 759x^{128} + 1288x^{144}$. From weight enumerator we observe that the weights of the two codewords are divisible by 4. Hence $C_{276,1}$ is self orthogonal. $C^{\perp}_{276,1}$ has a minimum weight of 3. Hence $C_{276,1}$ is projective. It follows that $C^{\perp}_{276,1}$ is a 1-error-correcting code. Hence $C^{\perp}_{276,1}$ is uniformly packed since $C_{276,1}$ is a two-weight code. $C_{276,1}$ has no other submodule apart from the trivial submodule hence it is irreducible. Since $\mathrm{Aut}(C_{276,1})$ has only one composition factor M_{24} , then it follows that $\mathrm{Aut}(C_{276,1}) \cong M_{24}$.

ii The polynomial of $C_{276,2}$ is $W(x) = 1 + 759x^{128} + 1288x^{132} + 1288x^{144} + 759x^{148} + x^{276}$. Accordingly from the weight enumerator of $C_{276,2}$ we observe that all codewords of $C_{276,2}$ have weights divisible by 4. Since the weights of this codewords are divisible by 4, $C_{276,2}$ is doubly even. Hence $C_{276,2}$ is self orthogonal. The minimum weight of $C^{\perp}_{276,2}$ code is 4. Hence $C_{276,2}$ is projective. Since $\mathrm{Aut}(C_{276,1})$ has only one composition factor M_{24} , it follows that $\mathrm{Aut}(C_{276,2}) \cong M_{24}$.

iii The polynomial of $C_{276,3}$ is $W(x) = 1 + 276x^{44} + 10626x^{80} + 134596x^{108} + 735471x^{128} + 1961256x^{140} + 1352078x^{144}$. Accordingly the weight enumerator shows that the weight of all codewords of $C_{276,3}$ is divisible by 4. Hence 4, $C_{276,3}$ is doubly even. Doubly even codes are self orthogonal, hence $C_{276,3}$ is self orthogonal. $C^{\perp}_{276,3}$ code has a minimum weight of 3.

iv The polynomial of $C_{276,6}$ is $W(x) = 1 + 276x^{44} + 10626x^{80} + 134596x^{108} + 735471x^{128} + 1961256x^{140} + 1352078x^{144} + 735471x^{148} + 134596x^{168} + 10626x^{196} + 276x^{232} + 1x^{276}$. .Accordingly Since all codewords of $C_{276,6}$ are divisible by 4, $C_{276,6}$ is doubly even. The minimum weight of $C^{\perp}_{276,6}$ code is 4.

v The minimum weight of $C^{\perp}_{276,7}$ code is 4. Hence $C_{276,7}$ is projective. $\square$

Weight distribution of $C_{276,1}$ shows that $C_{276,1}$ is a two weight code hence $C_{276,1}$ can be linked to a strongly regular graphs. We obtain a strongly regular graph $T(C_{276,1})$ related with $C_{276,1}$ whose properties are given in the proposition 4.3.2

Proposition 4.2.2. *$T(C_{276,1}$) is a strongly regular $[2048, 276, 44, 36]$ graph with spectrum* $[276]^1$,$[20]^{759}$,$[-12]^{1288}$.

Remark 4.2.3. *These examples have been studied from a point of view similar to Calderbank [5].*

The Designs of Minimum Weight in $C_{276,i}$

We determine the designs of codewords of minimum weight w_m in $C_{276,i}$ where i = 1, 2, 3, 4,5,6,7 as shown in Table 4.7. Column one represents the code C_i of weight m and column two gives the parameters of the 1-designs D_{w_m} . In column three we list the number of blocks of D_{w_m}, column four tests whether or not a design D_{w_m} is primitive.

Table 4.7: Deigns of codewords of minimum weight in $C_{276,i}$

m	D_{w_m}	No of Blocks	prim
128_1	1-(276, 128, 352)	759	yes
128_2	1-(276, 128, 352)	759	yes
44_3	1-(276, 44, 44)	276	yes
44_4	1-(276, 44, 44)	276	yes
23_5	1-(276, 23, 2)	24	yes
44_6	1-(276, 44, 44)	276	yes
23_7	1-(276, 23, 2)	24	yes

Remark 4.2.4. *From table 4.7 we observe that D_{w_m} is primitive for each m.*

Symmetric 1-Design

Using the orbits of the point stabilizers in theorem 3.1 and theorem 3.2 we construct symmetric 1 - designs. We take G to be the Mathieu group M_{24} and examine symmetric 1-design invariant under G constructed from orbits of the rank - 3 permutation representation of degree 276. We consider the p - element subsets $\{i_1, i_2, i_3\}$ of the set$\{1, 2, 3\}$ to form $\begin{pmatrix} 3 \\ p \end{pmatrix}$ distinct unions of suborbits Ω_i. We take the images of these unions under the action of G and form the 1 - designs D_k whose properties we examine . Observe that $k = \left| \bigcup_{i=1}^{p} \Omega_{i_j} \right|$ where $1 \leqslant p \leqslant 3$ and $1 \leqslant k \leqslant 275$.
Table 4.5 shows Designs from primitive group of degree 276. Column one shows the 1-design D_k of orbit length k, column two gives the orbit length, column three gives the parameters of the 1-designs D_k and column four represents the automorphism group of the design.

Proposition 4.2.5. *Let G be the primitive group of degree 276 of mathieu group*

Table 4.8: Designs from primitive group of degree 276

Design	orbit length	parameters	Automorphism Group
D_{44}	44	1-(276,44,44)	S_{24}
D_{231}	231	1-(276,231,231)	S_{24}
D_{45}	45	1-(276,45,45)	S_{24}
D_{232}	232	1-(276,232,232)	S_{24}
D_{275}	275	1-(276,275,275)	S_{276}

M_{24}. Let $\beta = \{\triangle^g \colon g \in G\}$ and $D_k = (\Omega, \beta)$. Define the sets M and N such that $M = \{44, 231, 45, 232\}$ and $N = \{275\}$. If $k \in M$ then Aut(D_k) $\cong S_{24}$.

Proof We consider the case when k $\in$M. The composition factors of Aut(D_k) are $\mathbb{Z}_2$ and A_{24}. This implies that Aut(D)$_k \cong S_{24}$ □

Theorem 4.2.6. *Let G be the primitive group of degree 276 of M_{24} and C a linear code . Then the following holds:*

(a) There exist a set of self orthogonal doubly even projective codes.

(b) There exist a strongly regular graphs related to two weight codes.

(c) There exist a set of Primitive Designs related to M_{24}.

(d) If $k \in M$ then Aut(D_k) $\cong S_{24}$

Proof

(a) See proposition 4.2.1

(b) See proposition 4.2.2

(c) See table 4.7

(d) See proposition 4.2.5

4.3 The Representation of Degree 759

We construct a 759-dimensional permutation module invariant under a permutation group G acting on a finite set Ω, of degree 759. We take the permutation module to be our working module and recursively find all submodules . The permutation module splits into 224 submodules. The submodules are the dimensions of the codes related to permutation module . The module splits into seven completely irreducible parts of length 1, 11,11, 44, 44,120 and 252 with multiplicities 3, 4, 4, 2, 2,2 and 1 respectively. Table 4.9 shows the 1st 112 submodules with dimension k from this permutation module.

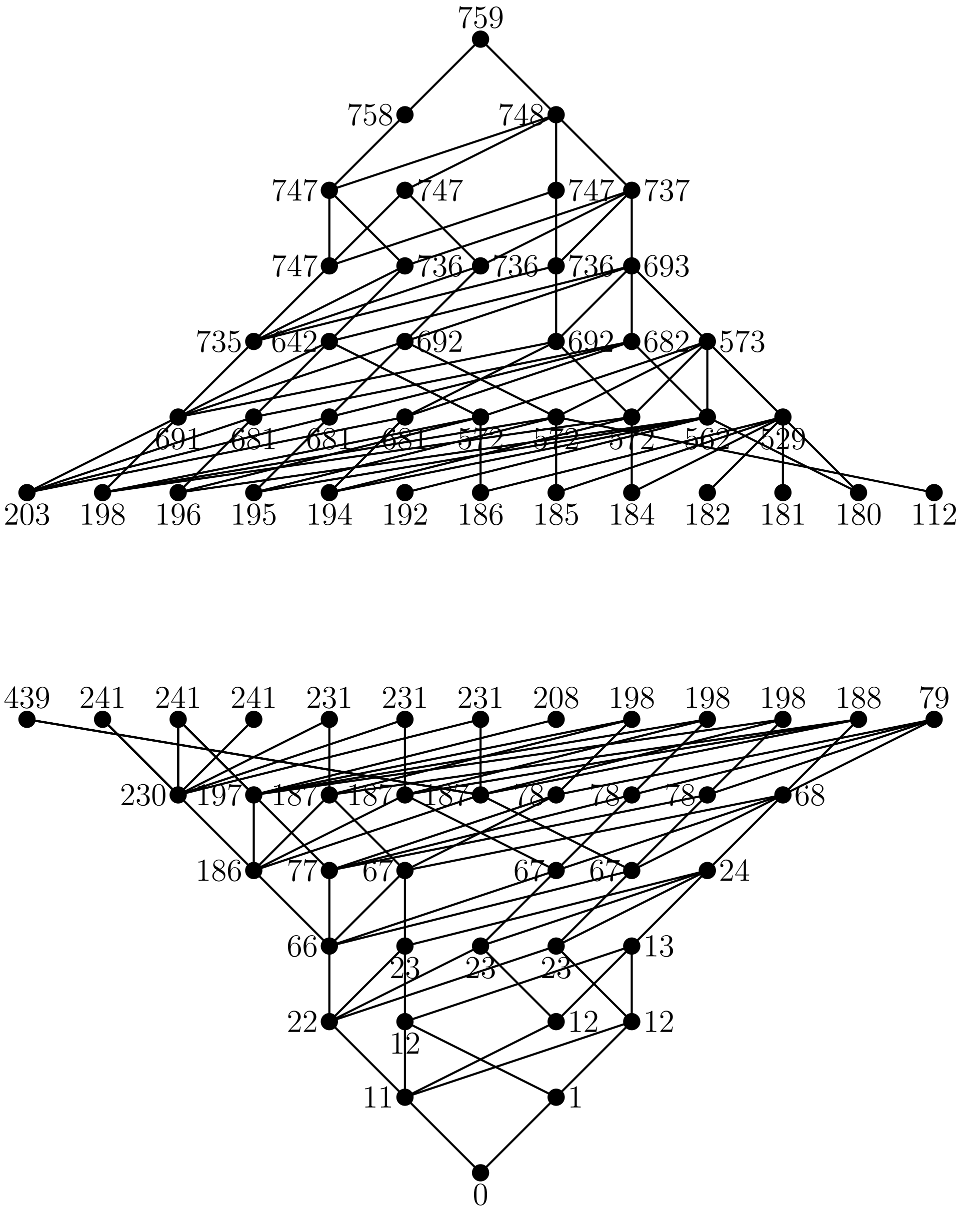
Table 4.9: Submodules from 759 Permutation Module

k	#	k	#	k	#	k	#
0	1	79	1	241	3	297	3
1	1	186	1	242	9	298	1
11	1	187	3	243	3	307	1
12	3	188	1	252	4	308	3
13	1	197	1	253	12	309	1
22	1	198	3	254	4	318	1
23	3	199	1	263	3	319	3
24	1	208	1	264	9	320	1
66	1	209	3	265	3		
67	3	210	1	274	1		
68	1	230	1	275	1		
77	1	231	3	276	1		
78	3	232	1	296	1		

The remaining submodules are of dimension $n - k$.

Partial submodule lattice is as shown in Figure 4.3

Figure 4.3: Partial Submodule lattice of degree 759



From the lattice structure the submodules of dimension 1 and dimension 11 are irreducible. We discuss ten non trivial submodules of small dimensions 11, 12, 12, 12, 13, 22, 23, 23, 23 and 24 . The binary linear codes of these submodules are represented in table 4.10.

Table 4.10: Codes of Small Dimensions

Name	Dimension	Parameters	Name	Dimension	Parameters
$C_{759,1}$	11	$[759,11,352]_2$	$C_{759,6}$	22	$[759,22,264]_2$
$C_{759,2}$	12	$[759,12,253]_2$	$C_{759,7}$	23	$[759,23,253]_2$
$C_{759,3}$	12	$[759,12,352]_2$	$C_{759,8}$	23	$[759,23,264]_2$
$C_{759,4}$	12	$[759,12,352]_2$	$C_{759,9}$	23	$[759,23,264]_2$
$C_{759,5}$	13	$[759,13,253]_2$	$C_{759,10}$	24	$[759,24,253]_2$

We make some observations about the codes. These properties are examined with certain detail in Proposition 4.3.1.

Proposition 4.3.1. *Let G be the mathieu group M_{24} and $C_{759,1}$, $C_{759,2}$, $C_{759,3}$ be non-trivial binary codes of dimension 11, 12, 22 respectively from a module of length 759.*

i Then $C_{759,1}$ is projective, doubly even, self orthogonal two weight $[759, 11,352]_2$ code. The dual code of $C_{759,1}$ is a $[759, 748, 3]_2$ is uniformly packed with weight 3.

ii Then $C_{759,2}$ is self orthogonal,projective and doubly even $[759, 12,352]_2$ code with weight 352. The dual code of $C_{759,2}$ is a $[759, 747, 3]_2$ code with weight 3.

iii Then $C_{759,6}$ is self orthogonal,projective and doubly even $[759, 22, 264]_2$ code *of weight 264. The dual code of $C_{759,6}$ is a [759, 737, 3]$_2$ with weight 3. Furthermore $Aut(C_{759,6}) \cong M_{24}$.*

Proof

i The polynomial of $C_{759,1}$ code is $W_x = 1 + 276x^{352} + 1771x^{384}$.From weight distribution we see that there are two weights of non-zero codewords of $C_{759,1}$. Since the weights are divisible by 4, $C_{759,1}$ is doubly even. Hence $C_{759,1}$ is self orthogonal. The minimum weight of $C^1_{759,1}$ code is 3. Hence $C^1_{759,1}$ is projective. It follows that $C^1_{759,1}$ is a 1-error-correcting code. A two-weight code is uniformly packed since .

ii The polynomial of this code $\mathrm{C}_{759,2}$ is $W_{C_{759,2}} = 1 + 276x^{352} + 2024x^{378} + 1771x^{384} + 24x^{506}$. The weights of codewords of $\mathrm{C}_{759,2}$ are divisible by 4. Since the weights of this codewords are divisible by 4, $\mathrm{C}_{759,2}$ is doubly even. Hence $\mathrm{C}_{759,2}$ is self orthogonal. The minimum weight of $\mathrm{C}^1_{759,2}$ code is 3. Hence $\mathrm{C}_{759,2}$ is projective.

iii The polynomial of this code $\mathrm{C}_{759,6}$ is $W(x) = 1 + 1288x^{264} + 26565x^{320} + 276828x^{352} + 510048x^{360} + 680064x^{376} + 1772771x^{384} + 807576x^{392} + 97152x^{408} + 21252x^{416} + 759x^{448}$.The weight distribution of $\mathrm{C}_{759,6}$ is given above. Since the weights all codewords of $\mathrm{C}_{759,6}$ are divisible by 4, $\mathrm{C}_{759,6}$ is doubly even. Hence $\mathrm{C}_{759,6}$ is self orthogonal. The minimum weight of $\mathrm{C}^{\perp}_{759,6}$ code is 3. Hence C_{22} is projective.

□

The binary code $C_{759,1}$ is connected to a strongly regular graph whose properties are given in lemma 4.3.2.

Lemma 4.3.2. *$T(C_{759,1})$ is a strongly regular [2048, 759, 310,264] graph with spectrum [759]^1,[207]276,[-2783] 1771.*

Remark 4.3.3. *From the weight distributions we can further make the following deductions;*

i. The codewords of minimum weight 352 in $C_{759,1}$ are isomorphic to $|M_{22} : 2.|$.

ii. The codewords of weight 384 in $C_{759,1}$ are isomorphic to $|2^6 : 3 : S_6|$

Designs of Minimum Weight in $C_{759,i}$

We determine t-designs of minimum weight in $C_{759,i}$. Table 4.11 shows Deigns of codewords of minimum weight in $C_{276,i}$. Column one gives the code C_i of weight m and column two represents the parameters of the 1-designs D_{w_m} . In column three we give the number of blocks of D_{w_m}, column four shows the automorphism group of the design D_{w_m}.

From table 4.11 we observe that $\mathrm{Aut}(D_{w_m}) \cong M_{24}$.

Table 4.11: Deigns of codewords of minimum weight in $C_{276,i}$

Code	D_{w_m}	No of Blocks	Aut(D_{w_m})
[759, 11, 352]	1-(759,352, 128)	276	M_{24}
[759, 12, 253]	1-(759,352, 128)	276	M_{24}
[759, 12, 352]	1-(759, 352, 128)	276	M_{24}
[759, 13, 253]	1-(759, 253, 8)	276	M_{24}
[759, 22, 264]	1-(759, 264, 448)	1288	M_{24}
[759, 23, 253]	1-(759, 253, 8)	24	M_{24}
[759, 23, 264]	1-(759, 264, 448)	1288	M_{24}
[759, 24, 253]	1-(759, 253, 8)	24	M_{24}

Symmetric 1-design

We use orbits of the point stabilizer to construct symmetric 1 - designs invariant under G constructed from orbits of the rank - 4 permutation representation of degree 759. Let Ω be the primitive G - set of degree 759 and $\Omega_1, \Omega_2, \Omega_3, \Omega_4$ with subdegrees 1, 30, 280 and 448 respectively denote the sub orbits of G on Ω with respect to the point stabilizer $2^8 : A_8$ group.

We consider the p - element subsets $\{i_1, i_2, i_3\}$ of the set$\{1, 2, 3\}$ to form $\begin{pmatrix} 3 \\ p \end{pmatrix}$ distinct unions of suborbits Ω_i. Table 4.12 shows Designs from primitive group of degree 759. Column one represents the 1-design D_k of orbit length k, the column TWO gives the orbit length, column three shows the parameters of the 1-designs D_k and column four gives the automorphism group of the design.

Table 4.12: Designs from primitive group of degree 759

Design	orbit length	parameters	Automorphism Group
D_{30}	30	1-(759,30,30)	M_{24}
D_{280}	280	1-(759,280,280)	M_{24}
D_{448}	448	1-(759,448,448)	A_{24}
D_{31}	31	1-(759,31,31)	M_{24}
D_{281}	281	1-(759,281,281)	M_{24}
D_{449}	449	1-(759,449,449)	M_{24}
D_{310}	310	1-(759,310,310)	M_{24}
D_{478}	478	1-(759,478,478)	M_{24}
D_{728}	728	1-(759,728,728)	M_{24}
D_{311}	311	1-(759,311,311)	M_{24}
D_{479}	479	1-(759,479,479)	M_{24}
D_{729}	729	1-(759,729,729)	M_{24}
D_{758}	758	1-(759,758,758)	M_{24}

Proposition 4.3.4. *Let G be the primitive group of degree 759 of mathieu simple group M_{24}. Define the set M such that $M = \{30, 280, 448, 31, 281, 449, 310, 478, 728, 311, 479, 729$ If $k \in M$ then Aut(D) $\cong M_{24}$.*

Proof

We consider the case when k $\in$ M. The only composition factor of Aut(D_k) is M_{24}. This implies that Aut $(D_k) \cong M_{24}$

Theorem 4.3.5. *Let G be the primitive group of degree 759 of M_{24} and C a linear code admitting G as an automorphism group. Then the following holds:*

(a) There exist a graph that is strongly regular associated with two weight codes.

(b) There exist a set of self orthogonal doubly even projective codes.

(c) There exist a set of Primitive Designs related to M_{24}.

(d) Aut(D_K)$\cong M_{24}$.

Proof

(a) See proposition lemma 4.3.2

(b) See proposition 4.3.1

(c) See table 4.11

(d) See table 4.12

4.4 The Representation of Degree 1288

From the action of the permutation group G on a finite set Ω, of degree 1288, we construct a 1288-dimensional permutation module invariant under G. We take the permutation module to be our working module and recursively find all submodules . The permutation module splits into 252 submodules. These submodules represent the dimensions of the codes associated with a module of length 1288 . The module breaks into nine completely irreducible parts of size 1, 11,11, 44, 44, 120, 220, 220 and 252 of multiplicities 4, 4, 4, 3, 3, 2, 1, 1 and 1 respectively. Table 4.13 shows the 1^{st} 140 submodules with the dimension k from this permutation module.

Table 4.13: The 1^{st} 140 Submodules with the Dimension k from 1288 Permutation Module.

k	#	k	#	k	#	k	#	k	#	k	#
0	1	112	1	276	2	407	1	474	1	539	3
1	1	186	1	277	1	417	1	483	3	540	3
11	1	187	1	286	2	418	1	484	4	551	1
12	1	230	1	287	3	428	1	485	1	561	1
22	1	231	4	288	1	429	1	494	1	562	1
23	1	232	2	297	2	450	1	495	2	572	1
45	1	241	1	298	3	451	3	496	1	573	2
56	1	242	2	299	1	452	1	506	3	574	1
57	1	243	1	331	1	461	3	507	3	583	1
66	1	252	1	332	1	462	5	517	5	584	2
67	2	253	2	342	1	463	1	518	4	585	1
68	1	254	1	343	1	472	4	528	5	595	1
111	1	275	1	406	1	473	6	529	5	596	1

The remaining submodules are of dimension $n - k$

Partial submodule lattice is as shown in Figure 4.4

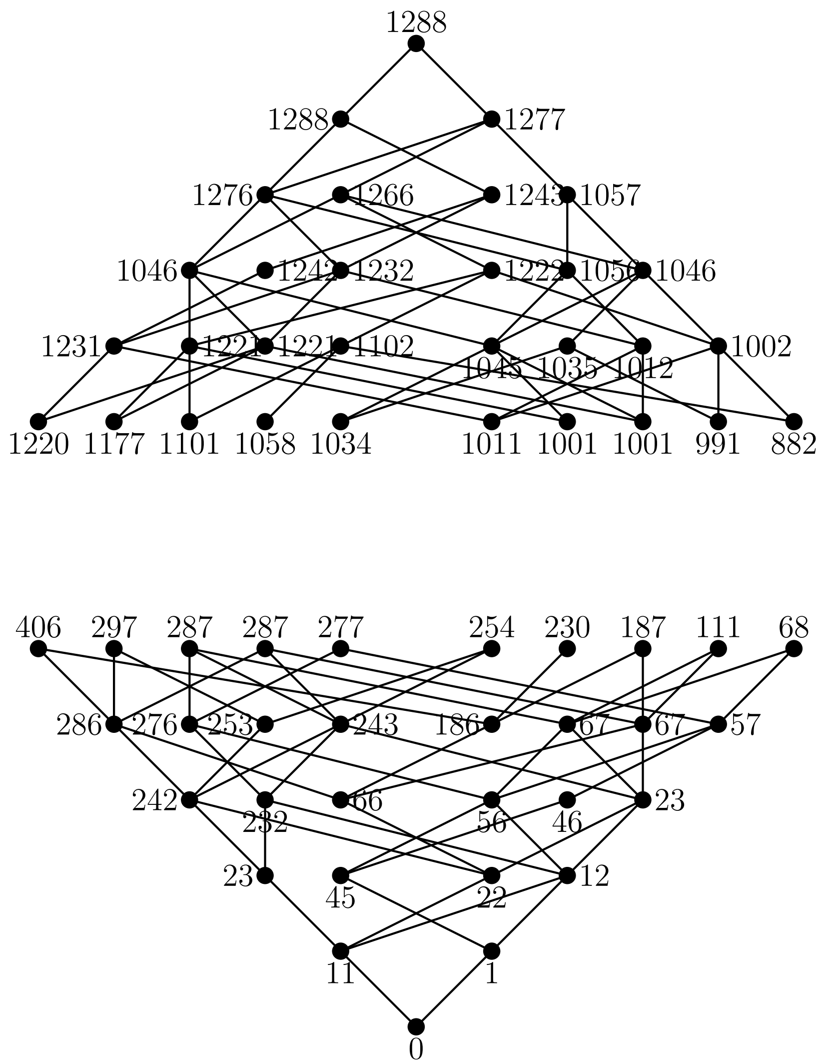


Figure 4.4: Submodule Lattice of degree 1288

From the lattice structure, submodules of dimension 1 and dimension 11 are irreducible.

We discuss four non trivial submodules of small dimensions 11, 12, 22, and 23 . The binary linear codes of these submodules are represented in table 4.14.

Table 4.14: Codes of small dimensions

Name	Dimension	Parameters
$C_{1288,1}$	11	$[1288,11,640]_2$
$C_{1288,2}$	12	$[1288,12,616]_2$
$C_{1288,3}$	22	$[1288,22,448]_2$
$C_{1288,4}$	23	$[1288,23,448]_2$

We make some observations about the codes. These properties are examined with certain detail in Proposition 4.4.1.

Proposition 4.4.1. *Let G be the mathieu group M_{24} and $C_{1288,1}$, $C_{1288,2}$, $C_{1288,3}$ be non-trivial binary codes of dimension 11, 12, 22 respectively derived from a module of length 1288. Then the following holds;*

i) $C_{1288,1}$ is a doubly even, self orthogonal and projective [1288, 11,640] binary code . The dual code of $C_{1288,1}$ is [1288, 1277, 3] binary code .

ii) $C_{1288,2}$ is a doubly even, self orthogonal and projective [1288, 12,616] binary code . The dual code of $C_{1288,2}$ is [1288, 1276, 4] binary code .

iii) $C_{1288,3}$ is a doubly even, self orthogonal and projective [1288, 23, 448] binary code . The dual code of $C_{1288,3}$ is [1288, 1265, 4] binary .

iv) $C_{1288,4}$ is doubly even, self orthogonal projective [1288, 23, 448] binary code . The dual code of $C_{1288,4}$ is a [1288, 1265, 4] .

proof

i The polynomial of this code $C_{1288,1}$ is $W_{C1_{288,1}} = 1 + 1771x^{640} + 276x^{672}$. We observe that both codewords have weights divisible by 4. Hence $C_{1288,1}$ is self orthogonal. The minimum weight of $C^{\perp}_{1288,1}$ code is 3. Hence $C_{1288,1}$ is projective.

ii The weight distribution of this code $C_{1288,2}$ is $W_{C_{1288,2}} = 1+276x^{616}+1771x^{648}+276x^{672}+x^{1288}$. We observe that both codewords have weights divisible by 4. Hence $C_{1288,2}$ is self orthogonal. The minimum weight of $C^{\perp}_{1288,2}$ code is 4. Hence $C_{1288,2}$ is projective.

iii The polynomial of this code $C_{1288,3}$ is $W_{C_{1288,3}} = 1 + 759x^{448} + 26565x^{576} + 170016x^{600} + 97152x^{616} + 510048x^{632} + 1772771x^{640} + 680064x^{648} + 637560x^{664} + 276828x^{672} + 21252x^{736} + 1288x^{792}$. Since the weight of all codewords of $C_{1288,3}$ are divisible by 4, $C_{1288,3}$ is doubly even. Hence $C_{1288,3}$ is self orthogonal. The minimum weight of $C^{\perp}_{1288,3}$ code is 4. Hence $C_{1288,3}$ is projective.

iv The polynomial of this code $C_{1288,4}$ is $W_{C_{1288,3}} = 1 + 759x^{448} + 1288x^{496} + 21252x^{552} + 26565x^{576} + 170016x^{600} + 373980x^{616}+637560x^{624}+510048x^{632}+2452835x^{640}+2452835x^{648}+510048x^{656}+637560x^{664} + 373980x^{672} + 170016x^{688} + 26565x^{712} + 21252x^{736} + 1288x^{792} + 759x^{840} + x^{1288}$. Since weights of all codewords of $C_{1288,4}$ are divisible by 4, $C_{1288,4}$ is doubly even. Hence $C_{1288,4}$ is self orthogonal. The minimum weight of $C^{\perp}_{1288,4}$ code is 4. Hence $C_{1288,4}$ is projective. $\square$

Since $C^{\perp}_{1288,1}$ is a two weight code, a strongly regular graph $\Gamma(C^{\perp}_{1288,1})$ is obtained.

Lemma 4.4.2. *$T(C^{\perp}_{1288,1})$ is a strongly regular [2048, 1288, 792,840] graph with spectrum* $[1288]^1, [8]^{1771}, [-56]^{276}$.

Remark 4.4.3. *This graph has not been mentioned by Calderbank.*

Remark 4.4.4. *Codewords of $C_{1288,1}$ and codewords of $C^{\perp}_{1288,1}$ are discussed geometrically;*

i. The words of $C_{1288,1}$ are the the blocks of the design D_{640}.

ii. The words of weight 640 in $C_{1288,1}$ are isomorphic to $2^6 : 3.S_6$.

iii. The codewords of weight 672 in $C_{1288,1}$ are isomorphic to $M_{12} : 2$.

Designs of Minimum Weight in $C_{1288,i}$

We determine designs of minimum weight in $C_{1288,i}$. Table 4.15 shows Deigns of minimum weight in $C_{1288,i}$. Column one indicates the code of weight m and column two shows the parameters of the 1-designs. In column three we give the number of blocks and column four we list the automorphism group of the design.

Table 4.15: Deigns of minimum weight in $C_{1288,i}$

Code	D_{w_m}	No of Blocks	Aut(D_{w_m})
[1288, 11, 640]	1-(1288, 640, 880)	1771	M_{24}
[1288, 12, 616]	1-(1288, 616, 138)	276	M_{24}
[1288, 22, 448]	1-(1288, 448, 264)	759	M_{24}
[1288, 23, 448]	1-(1288, 448, 264)	759	M_{24}

Table 4.15 shows that t-designs of minimum weights are isomorphic to M_{24}

Symmetric 1-design

In this section we examine all symmetric 1-designs invariant under Mathieu group M_{24} and constructed from orbits of the stabilizer. Let Ω be the primitive G - set of degree 1288 and $\Omega_1, \Omega_2, \Omega_3$ with subdegrees 1, 495 and 792 respectively denote the sub orbits of G on Ω with respect to the point stabilizer $M_{12}:2$ group.

We consider the subset $\{i_1, i_2, i_3\}$ of the set$\{1, 2, 3\}$ to form $\begin{pmatrix} 3 \\ p \end{pmatrix}$ distinct unions of suborbits Ω_i. Table 4.16 shows Designs from primitive group of degree 1288. Column one shows the 1-design D_k of orbit length k, column two represents the orbit length, the third column gives the parameters of the 1-designs D_k and column four gives the automorphism group of the design.

Table 4.16: Designs from primitive group of degree 1288

Design	orbit length	parameters	Automorphism Group
D_{495}	495	1-(1288,495,495)	M_{24}
D_{792}	792	1-(1288,792,792)	M_{24}
D_{496}	496	1-(1288,496,496)	M_{24}
D_{793}	793	1-(1288,793,793)	M_{24}
D_{1287}	1287	1-(1288,1287,1287)	

Proposition 4.4.5. *Let G be the mathieu simple group M_{24}, and Ω the primitive G-set of size 1288 defined by the action on the cosets of M_{12}:2. Let $\beta = \{\triangle^g \colon g \in G\}$ and $D_k = (\Omega, \beta)$. Define the sets M and N such that $M = \{495, 792, 496, 793\}$ and $N = \{1287\}$. If $k \in M$ then Aut(D_k) $\cong M_{24}$*

Proof First, we consider the case when k $\in$ M. The only composition factor of

Aut(D_k) is M_{24}. This implies that Aut(D_k) $\cong M_{24}$ $\square$

Theorem 4.4.6. *Let G be the primitive group of degree 1288 of M_{24} and C a linear code . Then there exist:*

(a) a strongly regular graphs related to two weight codes

(b) a set of self orthogonal doubly even projective codes. .

(c) a set of Primitive Designs related to M_{24}.

(d) a set of primitive symmetric 1-designs

Proof

(a) See lemma 4.4.2

(b) See proposition 4.4.2

(c) See table 4.15

(d) See table 4.16

4.5 Representation of Degree 1771

Suppose G is the Mathieu group M_{24}. The action of G on the sextet to generates the point stabilizer $2^6 : 3.S_6$. The group G acts on this point stabilizer to form orbits . The orbits of this point stabilizers are 1, 30, 280 and 448. For a primitive group G acting on a Ω, it follows from theorem 3.4.1 and 3.4.2 that if we form orbits of the point stabilizer and take their images under the action of the full group,represents the blocks of of a symmetric 1 - design.

Symmetric 1- Design

In this section we examine all designs invariant under G. Let Ω be the primitive G - set of degree 1771 and $\Omega_1, \Omega_2, \Omega_3, \Omega_4$, with subdegrees 1, 90, 240, 1440 respectively denote the sub orbits of G on Ω with respect to the point stabilizer $2^6 : 3.S_6$. We consider the subsets $\{i_1, i_2, i_3, i_4\}$ of the set$\{1, 2, 3, 4\}$ to form $\begin{pmatrix} 4 \\ \\ p \end{pmatrix}$ distinct unions of suborbits Ω_i. Observe that $k = \left| \bigcup_{i=1}^{p} \Omega_{i_j} \right|$ where $1 \leqslant p \leqslant 4$ and $1 < k < 1770$.

Table 4.17 shows Designs from primitive groups of degree 1771 .t Column one represents the 1-design D_k of orbit lengh k, column two gives the orbit length, column three shows the parameters of the 1-designs D_k and column four gives the automorphism group of the design.

Table 4.17: Designs from Primitive Group of Degree 1771

Design	orbit length	parameters	Automorphism Group
D_{90}	30	1-(1771,90,90)	M_{24}
D_{240}	280	1-(1771,240,240)	M_{24}
D_{1440}	1440	1-(1771,1440,1440)	A_{24}
D_{91}	31	1-(1771,91,91)	M_{24}
D_{241}	241	1-(1771,241,241)	M_{24}
D_{1441}	1441	1-(1771,1441,1441)	M_{24}
D_{330}	330	1-(1771,330,330)	M_{24}
D_{1530}	1530	1-(1771,1530,1530)	M_{24}
D_{1680}	1680	1-(1771,1680,1680)	M_{24}
D_{331}	331	1-(1771,331,331)	M_{24}
D_{1531}	1531	1-(1771,1531,1531)	M_{24}
D_{1681}	1681	1-(1771,1681,1681)	M_{24}
D_{1770}	1770	1-(1771,1770,1770)	M_{24}

Proposition 4.5.1. *Let G be the Mathieu simple group M_{24}, and Ω the primitive G-set of size 1771 defined by the action on the cosets of $M_{22}{:}2$. Let $\beta = \{\triangle^g \colon g \in G\}$ and $D_k = (\Omega, \beta)$. Then the $Aut(D_k) \cong M_{24}$*

Proof

The only composition factor of $\mathrm{Aut}(\mathrm{D}_k)$ is M_{24}. This implies that $\mathrm{Aut}(\mathrm{D}_k) \cong M_{24}$ □

Binary Codes

We note that the binary row span of the incidence matrices of each design D_k yield the code denoted C_k. We examine the properties of some of the codes C_k where computations are possible.

Proposition 4.5.2. *Let G be the primitive group of degree 1771 of M_{24} and C a linear code admitting G as an automorphism group. Then the following holds:*

i *C_{448} is a, self orthogonal and doubly even projective [1771, 22,264] binary code. The dual code $C_{448}^{\perp}$ is a [1771, 737, 3] binary code of weight 3.*

ii *C_{311} is a projective [1771, 23,264] binary code with 1288 words of weight 264. $C_{311}^{\perp}$ of C_{311} is a [1771, 736, 4] binary code.*

Proof

i The weight distribution of this code is $C_{448} = 1 + 1288x^{264} + 26565x^{320} + 276828x^{352} + 510048x^{360} + 680064x^{376} + 1772771x^{384} + 807576x^{392} + 97152x^{408} + 21252x^{416} + 759x^{448}$.From the weight distribution of C_{448} , we observe that codewords have weights divisible by 4. C_{448} is doubly even. Hence C_{448} is self orthogonal. The minimum weight of $C_{448}^{\perp}$ code is 3. Hence C_{448} is projective.

ii The weight distribution of this code is $C_{311} = 1 + 1288x^{264} + 759x^{311} + 26565x^{350} + ...$ The minimum weight of $C_{311}^{\perp}$ code is 4. Hence C_{311} is projective. □

Theorem 4.5.3. *Let G be the primitive group of degree 1771 of M_{24} and C a linear code and D a primitive design admitting G as an automorphism group. Then the following holds:*

(a) *There exist a self orthogonal doubly even projective code.*

(b) There exist a set of Primitive Symmetric 1-Designs related to M_{24}.

(c) Aut((D_k) $\cong M_{24}$

Proof

(a) See proposition 4.5.2

(b) See table 4.17

(c) See table 4.17

4.6 The Representation of Degree 2024

Let G be the Mathieu group M_{24}. Group G acts on the triad to generate the point stabilizer $L_3(4) : S_3$ .The point stabilizer is a maximal subgroup of degree 2024 in G. The group G acts on this point stabilizer to form orbits . The orbits of this point stabilizers are 1, 63, 210, 630 and 1120. Given a primitive permutation group G acting on a set Ω, it follows from theorem 3.4.1 and 3.4.2 that if we form orbits of the point stabilizer and take their images under the action of the full group, we obtain the blocks of of a symmetric 1 - design with the group G acting as an automorphism group.

Symmetric 1- Designs

In this section we examine all designs invariant under G. Let Ω be the primitive G - set of degree 2024 and $\Omega_1, \Omega_2, \Omega_3, \Omega_4, \Omega_5$, with subdegrees 1, 63, 210,630 and 1120 respectively denote the sub orbits of G on Ω with respect to the point stabilizer $L_3(4) : S_3$. We consider the p - element subsets $\{i_1, i_2, i_3, i_4, i_5\}$ of the set$\{1, 2, 3, 4, 5\}$ to form $\begin{pmatrix} 5 \\ p \end{pmatrix}$ distinct unions of suborbits Ω_i. Observe that $k = \left| \bigcup_{i=1}^{p} \Omega_{i_j} \right|$ where $1 \leqslant p \leqslant 5$ and $1 < k < 2024$.

In Table 4.18 the first column represents the 1-design D_k of orbit length k, the second column gives the orbit length, the third column shows the parameters of the 1-designs D_k and the fourth column gives the automorphism group of the design.

Table 4.18: Designs from primitive group of degree 2024

Design	orbit length	parameters	Automorphism Group
D_{63}	63	1-(2024, 63, 63)	S_{24}
D_{64}	64	1-(2024,64,64)	S_{24}
D_{210}	210	1-(2024,210,210)	M_{24}
D_{211}	211	1-(2024,211,211)	M_{24}
D_{630}	630	1-(2024,630,630)	S_{24}
D_{1120}	1120	1-(2024,1120,1120)	M_{24}
D_{631}	631	1-(2024,631,631)	S_{24}
D_{1121}	1121	1-(2024,1121,1121)	M_{24}
D_{273}	273	1-(2024,273,273)	M_{24}
D_{693}	693	1-(2024,693,693)	S_{24}
D_{1183}	1183	1-(2024,1183,1183)	M_{24}
D_{840}	840	1-(2024,840,840)	M_{24}
D_{1330}	1330	1-(2024,1330,1330)	S_{24}
D_{1750}	1750	1-(2024,1750,1750)	S_{24}
D_{274}	274	1-(2024,274,274)	M_{24}
D_{694}	694	1-(2024,694,694)	S_{24}
D_{1184}	1184	1-(2024,1184,1184)	M_{24}
D_{841}	841	1-(2024,841,841)	M_{24}
D_{1331}	1331	1-(2024,1331,1331)	S_{24}
D_{1751}	1751	1-(2024,1751,1751)	S_{24}
D_{903}	903	1-(2024,903,903)	M_{24}
D_{1393}	1393	1-(2024,1393,1393)	S_{24}
D_{1960}	1960	1-(2024,1960,1960)	S_{24}
D_{1813}	1813	1-(2024,1813,1813)	M_{24}
D_{904}	904	1-(2024,904,904)	M_{24}
D_{1394}	1394	1-(2024,1394,1394)	S_{24}
D_{2023}	2023	1-(2024,2023,2023)	S_{24}
D_{1961}	1961	1-(2024,1961,1961)	S_{24}
D_{1814}	1814	1-(2024,1814,1814)	M_{24}

Proposition 4.6.1. *Let G be the Mathieu simple group M_{24}, and Ω the primitive G-set of size 2024 defined by the action on the cosets of $L_3(4) : S_3$. Let M and N be the sets M =[210,211,1120,1121,273,1183, 840,274,1184,841,903,1813,904,1814] and N = [63, 64,630, 631,693,1330,1730,694, 1331,1751, 1393, 1960, 1394, 2023, 1961]. Let $\beta = \{\triangle^g \colon g \in G\}$ and $D_k = (\Omega, \beta)$. Then the following hold:*

i D_k is a primitive symmetric $1-(2024, \mid \triangle \mid, \mid \triangle \mid)$ design.

ii If $k \in M$*, then* $|Aut(D_k)| \cong M_{24}$

iii If $k \in N$*, then* $|Aut(D_k)| \cong S_{24}$

Proof

i From theorem 3.4.1, it is clear that G acts as an automorphism group, primitive on points and on blocks of the design and so $G \subseteq \mathrm{Aut}(D_k)$.

ii First, we consider the case when $k \in M$. The only composition factor of $\mathrm{Aut}(D_k)$ is M_{24}. This implies that $\mathrm{Aut}(D_k) \cong M_{24}$

iii We consider the case when $k \in N$. The composition factors of $\mathrm{Aut}(D_k)$ are $\mathbb{Z}_2$ and A_{24}. This implies that $\mathrm{Aut}(D_k) \cong S_{24}$. □

Binary Codes

We note that the binary row span of the incidence matrices of each design D_k yield the code denoted C_k. In the following subsections, we examine the properties of some of the codes C_k where computations are possible.

Proposition 4.6.2. *C_{631} is a projective [2024, 24,253] binary code . The dual code $C_{631}^{\perp}$ of C_{631} is a [2024, 2000 , 4] .*

Proof

The minimum weight of $C_{631}^{\perp}$ code is 4. Hence C_{631} is projective.

Theorem 4.6.3. *Let G be the primitive group of degree 1771 of M_{24} and C a linear code and D a primitive design admitting G as an automorphism group. Then the following holds:*

(a) There exist a self orthogonal doubly even projective code.

(b) There exist a set of Primitive Symmetric 1-Designs related to M_{24}.

Proof

(a) See proposition 4.6.2

(b) See table 4.18

4.7 The Representation of Degree 3795

Let G be the Mathieu group M_{24}. Group G acts on the trio to generate the point stabilizer $2^6 : L_3(2) : S_6$ .The point stabilizer is a maximal subgroup of degree 3795 in G. The group G acts on this point stabilizer to form orbits . The orbits of this point stabilizers are 1, 42, 56, 1008 and 2688. It follows from theorem 3.4.1 and 3.4.2 that if we form orbits of the point stabilizer and take their images under the action of the full group, we obtain the blocks of of a symmetric 1 - design with the group G acting as an automorphism group.

Symmetric 1-Designs

In this section we examine all designs invariant under G. Let Ω be the primitive G - set of degree 3795 and $\Omega_1, \Omega_2, \Omega_3, \Omega_4, \Omega_5$, with subdegrees 1, 42, 56, 1008 and 2688 respectively denote the sub orbits of G on Ω with respect to the point stabilizer $L_3(4) : S_3$. We consider the subsets $\{i_1, i_2, i_3, i_4, i_5\}$ of the set$\{1, 2, 3, 4, 5\}$ to form $\begin{pmatrix} 5 \\ \\ p \end{pmatrix}$ distinct unions of suborbits Ω_i. Observe that $k = \left| \bigcup_{i=1}^{p} \Omega_{i_j} \right|$ where $1 \leqslant p \leqslant 5$ and $1 < k < 3795$.

Table 4.19 shows Designs from Primitive Group of Degree 3795. Column one represents the 1-design D_k of orbit length k, column two gives the orbit length, column three shows the parameters of the 1-designs D_k and column four gives the automorphism group of the design.

Table 4.19: Designs from Primitive Group of Degree 3795

Design	orbit length	parameters	Automorphism Group
D_{42}	42	1-(3795, 42, 42)	M_{24}
D_{43}	43	1-(3795,43,43)	M_{24}
D_{56}	56	1-(3795,56,56)	M_{24}
D_{57}	57	1-(3795,57,57)	M_{24}
D_{1008}	1008	1-(2024,1008,1008)	M_{24}
D_{2688}	2688	1-(3795,2688,2688)	M_{24}
D_{1009}	1009	1-(3795,1009,1009)	M_{24}
D_{2689}	2689	1-(3795,2689,2689)	M_{24}
D_{98}	98	1-(3795,98,98)	M_{24}
D_{1050}	1050	1-(3795,1050,1050)	M_{24}
D_{2730}	2730	1-(3795,2730,2730)	M_{24}
D_{1064}	1064	1-(3795,1064,1064)	M_{24}
D_{2744}	2744	1-(3795,2744,2744)	M_{24}
D_{3696}	3696	1-(3795,3696,3696)	M_{24}
D_{99}	99	1-(3795,99,99)	M_{24}
D_{1051}	1051	1-(3795,1051,1051)	M_{24}
D_{2731}	2731	1-(3795,2731,2731)	M_{24}
D_{1065}	1065	1-(3795,1065,1065)	M_{24}
D_{2745}	2745	1-(3795,2745,2745)	M_{24}
D_{3697}	3697	1-(3795,3697,3697)	M_{24}
D_{1106}	1106	1-(3795,1106,1106)	M_{24}
D_{2786}	2786	1-(3795,2786,2786)	M_{24}
D_{3752}	3752	1-(3795,3752,3752)	M_{24}
D_{3738}	3738	1-(3795,3738,3738)	M_{24}
D_{1107}	1107	1-(3795,1107,1107)	M_{24}
D_{2787}	2787	1-(3795,2787,2787)	M_{24}
D_{3794}	3794	1-(3795,3794,3794)	M_{24}
D_{3753}	3753	1-(3795,3753,3753)	M_{24}
D_{3739}	3739	1-(3795,3739,3739)	M_{24}

Proposition 4.7.1. *Let G be the mathieu simple group M_{24}, and Ω the primitive G-set of size 3795 defined by the action on the cosets of $2^6 : L_3(2) : S_6$. Let $\beta = \{\triangle^g \colon g \in G\}$ and $D_k = (\Omega, \beta)$. Then the following hold:*

i D_k *is a primitive symmetric* $1-(3795, |\triangle|, |\triangle|)$ *design.*

ii $|Aut(D_k)| \cong M_{24}$

Proof

i From theorem 3.4.1, it is clear that G acts as an automorphism group, primitive on points and on blocks of the design and so G $\subseteq$ Aut(D_k).

ii The only composition factor of Aut(D_k) is M_{24}. This implies that Aut(D_k) $\cong M_{24}$ □

Theorem 4.7.2. *Let G be the primitive group of degree 3795 of M_{24} and D a primitive design admitting G as an automorphism group. Then the following holds:*

(a) There exist primitive symmetric 1-designs.

(b) $Aut|D| \cong M_{24}$.

Proof

(a) See table 4.19

(b) See table 4.19

4.8 Conclusion

We constructed and enumerated all G-invariant codes from primitive permutation representations of degree 24, 276, 759, and 1288 from the simple group M_{24}. The computations were carried recursively in Magma with a built-in component of Meat-Axe. We classified the G-invariant codes using the lattice diagram. From the lattice diagram we found one self dual [24, 12, 8] code, four irreducible codes and several decomposable codes. We also constructed codes of small dimensions due to computer limitations and found several self orthogonal and projective codes. We also found two strongly regular graphs from a representation of degree 276 and 759. These graphs are known. We determined designs from some binary codes using codewords of minimum weight. We found that all the designs were primitive. We constructed symmetric 1-designs from the primitive permutation representations of degree 24,276,759, 1771, 2024 and 3795. We found that in most cases the full automorphism group of the design was M_{24} .

Chapter 5

Mathieu Group M_{23}

M_{23} is the point stabilizer in M_{24}. It is a 3-transitive permutation group on 23 objects. . It is the automorphism group of the Steiner system S(4,7,23), whose 253 heptads arise from the octads of S(5,8,24) containing the fixed point. It is also described as the automorphism group of the binary Golay code of dimension 12, length 23, and minimal weight 7, or as a subcode of even weight words[35].

There are seven primitive permutation representations of degree 23, 253, 253,506,1288, 1771, and 40320 respectively [35]. The seven primitive permutation representations are as shown in the table 5.1 , where column one gives the structure of the maximal subgroups; two gives the degree (the number of cosets of the point stabilizer); three gives the order of the maximal subgroups; four gives the number of orbits of the point-stabilizer, and the rest give the length of the orbits.

The action of G on geometrical objects point, duad, heptad, octad, dodecad, and triad respectively describes the primitive representations . The elements of each degree generate a permutation module over $\mathbb{F}$. We determine orbits of the point stabilizer through cosset action of a group G on its maximal subgroups.

Table 5.1: Primitive permutation representations of M_{24} .

Max.sub	Degree	Order	#	Length	Length	Length	Length	Length
M_{22}	23	443520	2	22				
$L_3(4)$: 2_2	253	40320	3	42	210			
$2^4 : A_7$	253	40320	3	112	140			
A_8	506	20160	4	15	210	280		
M_{11}	1771	7920	8	20	60	90	160	480(3)
$2^4 : 3 \times A_5 : 2$	1288	7920	4	165	330	792		
23 : 11	40320	253	164	23(4)	253(159)			

In this chapter,we enumerate and classify all G-invariant codes of G preserved by primitive groups of degree 23, 253,253 and 506 using modular representation method. We study the properties of some binary codes where computations are possible. We determine symmetric 1-designs from the primitive group G.

5.1 The Representation of Degree 23

Given a permutation group G acting on a finite set Ω, we find all submodules of the permutation module. The submodules constitutes the building blocks for the construction of a lattice of submodules . Let G be the Mathieu group M_{23}. Group G acts on a point to generate the point stabilizer M_{22} . The point stabilizer is a maximal subgroup of degree 23 in G. The group G acts on this maximal subgroup over $\mathbb{F}_2$ to form a module of dimension 23 . We take the permutation module to be our working module and recursively find all maximal submodules . The recursion stops as soon as we obtain all maximal submodules. We find that permutation module splits into maximal submodules of dimension 1, 11, 12 and 22. The module breaks down into three completely irreducible parts of length 1, 11, and 11 with multiplicities 1, 1, and 1 respectively. The submodule lattice is as shown in Figure 4.1

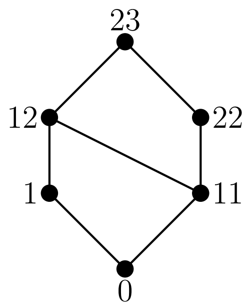


Figure 5.1: Submodule Lattice of the 23 Dimensional Permutation Module

The submodules of dimensions 1 and 11 are irreducible .

We obtain two non trivial submodules of dimensions 11 and 12. The binary linear code from this representations is [23,11,8] and its dual [23, 12, 7]. We shall denote the code $C_{23,1}$ and its dual $C_{23,1}^{\perp}$. The weight distribution of these codes is given in Table 5.2 below.

Table 5.2: The weight distribution of the codes from a 24-dimensional representation.

name	dim	0	7	8	11	12	15	16	23
$C_{23,1}$	11	1		506		1288		253	
$C_{23,1}^{\perp}$	12	1	253	506	1288	1288	506	253	1

We make some observations about the properties of these codes in Proposition 5.1.1.

Proposition 5.1.1. *Let G be the Mathieu group M_{23} and $C_{23,1}$ a binary code of dimension 11 from a module of degree 23. $C_{23,1}$ is self orthogonal doubly even projective [23, 11,8] binary code . The dual code $C_{23,1}^{\perp}$ of $C_{23,1}$ is a [23, 12, 7] . Furthermore $C_{23,1}$ is irreducible and Aut($C_{23,1}$) $\cong M_{23}$.*

proof

The submodule 12 represents the dimension of binary code $\mathrm{C}_{23,1}$. From this submodule we determine the binary linear code [23, 11,8]. The polynomial of this code is $W(x) = 1 + 506x^8 + 1288x^{12} + 253x^{16}$. From the polynomial we deduce that the weight of codewords are divisible by 4. Therefore $\mathrm{C}_{23,1}$ is doubly even. The minimum weight of $\mathrm{C}_{23,1}^{\perp}$ code is 7. Hence $\mathrm{C}_{23,1}$ is projective. From the lattice structure the submodule 12 is a direct sum of trivial submodules 11 and 1 respectively which implies that $\mathrm{C}_{23,1}$ is irreducible. For the structure of the automorphism group, let $\overline{G} \cong Aut(C_{24,1})$. Composition factors of $\overline{G}$ are $\mathbb{Z}_1$ and M_{23} and the order of $\overline{G}$ is 10200960. This implies that $\overline{G} = M_{23}$. Since $M_{23} \subseteq \overline{G}$, we conclude that $\overline{G} \cong M_{23}$ $\square$

Designs of Codewords of minimum weight in [23,11,8] Code

We determine designs of codewords of minimum weight in $C_{23,1}$. Table 5.3 shows deigns of codewords of minimum weight in $C_{23,1}$ where column one represents the code $C_{23,1}$ of weight m and column two gives the parameters of the 3-designs D_{w_m} . In column three we list the number of blocks of D_{w_m}, four tests whether or not a design D_{w_m} is primitive under the action of Aut(C).

Table 5.3: Deigns held by the support of codewords in $C_{23,1}$

m	D_{w_m}	No of Blocks	primitive
8	3-(23, 8, 16)	506	yes
12	3-(23, 12, 160)	1288	yes
16	3-(23, 16, 80)	253	yes
8	2-(23, 8, 56)	506	yes
12	2-(23, 12, 336)	1288	yes
16	2-(23, 16, 120)	253	yes
8	1-(23, 8, 176)	506	yes
12	1-(23, 12, 672)	1288	yes
16	1-(23, 16, 176)	253	yes

Remark 5.1.2. *From the results in table 5.3 we observe that Aut(C) is primitive on* D_{w_m}

Maximal subgroups of degree 506, 1288, and 253 in table 5.1 are stabilizers in M_{23} and the blocks 506, 1288,and 253 in table 5.3 represents codewords of weight 8, 12 and 16 respectively.

Symmetric 1- Designs

From theorem 3.4.1 , if we form orbits of the point stabilizer and take their images under the action of the full group, we obtain the blocks of of a symmetric 1 - design .

In this section we consider G to be the simple Mathieu group M_{23} and examine symmetric 1-design invariant under G constructed from orbits of the rank - 2 permutation representation of degree 23.

Table 5.4 shows Symmetric 1-Design where column one represents the 1-design D_k of orbit length k, column two gives the orbit length, column three shows the parameters of the symmetric 1-design D_k and column four gives the automorphism group of the design.

Table 5.4: Symmetric 1-Design

Design	orbit length	parameters	Automorphism Group
D_{22}	22	1-(23,22,22)	$A_{23}:2$

Proposition 5.1.3. *Let G be the mathieu simple group M_{23}, and Ω the primitive G-set of size 23 defined by the action on the cosets of M_{23}. Let $\beta = \{\triangle^g \colon g \in G\}$ and $D_k = (\Omega, \beta)$. Then the following hold:*

i *D_k is a primitive symmetric $1-(23, \mid \triangle \mid, \mid \triangle \mid)$ design.*

ii $Aut(D_k) \cong A_{23} : 2$

Proof

i From theorem 3.4.1, it is clear that G acts as an automorphism group, primitive on points and on blocks of the design and so G $\subseteq$ Aut(D_k).

ii The order of Aut(D_k) is 25852016738884976640000. The factors of 258520167388849766400 are 2 and 12926008369442488320000 which corresponds to the composition factors Z_2 and A_{23} and so Aut(D_k)= $A_{23} : 2$. This implies that $Aut(D_k) \approxeq A_{23} : 2$ □

Theorem 5.1.4. *Let G be the primitive group of degree 23 of M_{23} and C a linear code admitting G as an automorphism group. Then the following holds:*

(a) There exist a self orthogonal irreducible doubly even projective code.

(b) There exist a set of Primitive Designs related to M_{23}.

5.2 The 1^{st} Representation of Degree 253

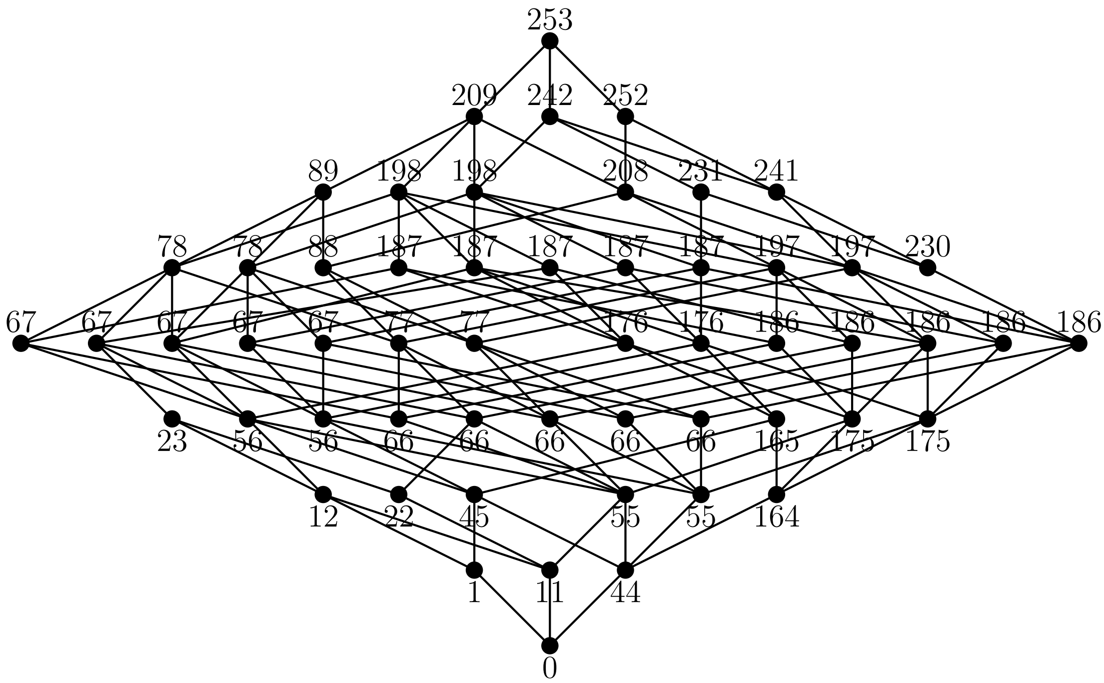
Let G be the Mathieu group M_{23}. Group G acts on a duad to generate the stabilizer $L_4(4):2$. The stabilizer is a maximal subgroup of degree 253 in G. The group G acts on this maximal subgroup over $\mathbb{F}_2$ to form a module of dimension 253 invariant under G. The module breaks down into three completely irreducible parts of length 1, 11, 44, 44 and 120 with multiplicities 1, 2, 2, 1, 1 and 1 respectively. The submodules of dimension 1, 11 and 44 are irreducible . The module splits into 54 maximal submodules. These submodules are the dimensions of the codes related with the module of dimension 253 invariant under G. Table 5.5 shows the Submodules from a Module of dimension 253 . Column k represents the dimension of the submodule and # the number of the submodules of each dimension.

Table 5.5: Submodules from a Module of dimension 253

k	#	k	#	k	#	k	#
0	1	55	2	164	1	208	1
1	1	56	2	165	1	209	1
11	1	66	5	175	2	230	1
12	1	67	5	176	2	231	1
22	1	77	2	186	5	241	1
23	1	78	2	187	5	242	1
44	1	88	1	197	2	252	1
45	1	89	1	198	2	253	1

The submodule lattice is as shown in Figure 5.2

Figure 5.2: Submodule Lattice of Permutation Module of dimension 253



We discuss three non trivial submodules of small dimensions 11, 12 and 22. The binary linear codes from this representations are [253,11,112], [253, 12,112] and [253, 22, 22]. We make some observations about the properties of these codes. These properties are examined with certain detail in Proposition 5.2.1.

Proposition 5.2.1. *Let G be the Mathieu group M_{23} and $C_{253,1}$, $C_{253,2}$, $C_{253,3}$, $C_{253,4}$ be non-trivial binary code of dimension 11, 12, 22, 23 respectively obtained from the permutation module of degree 23. Then the following holds;*

- i *$C_{253,1}$ is self orthogonal doubly even projective [253, 11,112] binary code . [253, 242, 3] is the dual code of $C_{253,1}$. Furthermore $C_{253,1}$ is irreducible and Aut($C_{253,1}$) $\cong M_{23}$.*
- ii *$C_{253,2}$ is projective [253, 12,112] binary code . [253, 241, 4] is the dual code of $C_{253,2}$. Furthermore $C_{253,2}$ is decomposable and Aut($C_{253,2}$) $\cong M_{23}$.*
- iii *$C_{253,3}$ is self orthogonal singly even projective [253, 22,22] binary code.* $[253, 231, 3]_2$ *is the dual code of $C_{253,3}$. Furthermore Aut($C_{253,1}$) $\cong S_{253}$.*

proof

- i The submodule 11 represents the dimension of binary code $\mathrm{C}_{253,1}$. From this submodule we determine the binary linear code $[253, 11,112]_2$. The polynomial of this code is $W(x) = 1 + 253x^{112} + 506x^{120} + 1288x^{132}$. From the polynomial we deduce that the weight of this codewords are divisible by 4. Hence $\mathrm{C}_{253,1}$ is doubly even. The minimum weight of $\mathrm{C}^{\perp}_{253,1}$ code is 3. Hence $\mathrm{C}_{253,1}$ is projective. From the lattice structure the submodule 11 can not be broken down which implies that $\mathrm{C}_{23,1}$ is irreducible. For the structure of the automorphism group, let $\overline{G} \cong Aut(C_{253,1})$. $\overline{G}$ has only one Composition factor M_{253} and the order of $\overline{G}$ is 10200960. This implies that $\overline{G} = M_{23}$. Since $M_{23} \subseteq \overline{G}$, we conclude that $\overline{G} \cong M_{23}$

ii The submodule 12 represents the dimension of binary code $\mathrm{C}_{253,2}$. From this submodule we determine the binary linear code $[253,\ 12{,}112]_2$. The partial weight enumerator of this code is $W(x) = 1 + 253x^{112} + 506x^{120} + 1288x^{121} + ...$ The minimum weight of $\mathrm{C}_{253,2}^{\perp}$ code is 4. Hence $\mathrm{C}_{253,2}$ is projective. From the lattice structure the submodule 12 is a direct sum of 11 and 1 which implies that $\mathrm{C}_{23,2}$ is irreducible. For the structure of the automorphism group, let $\overline{G} \cong Aut(C_{253,2})$. $\overline{G}$ has only one Composition factor M_{253} and the order of $\overline{G}$ is 10200960. This implies that $\overline{G} = M_{23}$. Since $M_{23} \subseteq \overline{G}$, we conclude that $\overline{G} \cong M_{23}$

iii The submodule 22 represents the dimension of binary code $\mathrm{C}_{253,3}$. From this submodule we determine the binary linear code $[253,\ 22{,}22]_2$. The polynomial of this code is $W(x) = 1 + 23x^{22} + 253x^{42} + 1771x^{60} + 8855x^{76} + 33649x^{90} + 100947x^{102} + 245157x^{112} + 490314x^{120} + 817190x^{126} + 1144066x^{130} + 1352078x^{132}$. We deduce that the weights of this codewords are divisible by 2. $\mathrm{C}_{253,2}$ is singly even. The weight of $\mathrm{C}_{253,3}^{\perp}$ code is 3. Hence $\mathrm{C}_{253,3}$ is projective. For the structure of the automorphism group, let $\overline{G} \cong Aut(C_{253,1})$. $\overline{G}$ has two Composition factors M_{253} and $\mathbb{Z}_2$. This implies that $\overline{G} = S_{253}$. We conclude that $\overline{G} \cong M_{23}$ $\square$

Designs of Codewords of Minimum Weight in $C_{253,i}$ Code

We determine designs of codewords of minimum weight in $C_{23,i}$. Table 5.6 shows Deigns of codewords in $C_{253,i}$ where column one represents the code $C_{23,i}$ of minimum weight m and column two gives the parameters of the t-designs D_{w_m} . In column three we list the number of blocks of D_{w_m}, four tests whether or not a design D_{w_m} is primitive .

Table 5.6: Deigns of codewords in $C_{253,i}$

m	D_{w_m}	No of Blocks	primitive
112	1-(253, 112, 112)	253	yes
22	1-(253, 22, 2)	23	yes
3	1-(253, 3, 21)	1771	yes
4	1-(253, 4, 1260)	79695	yes

Remark 5.2.2. *From the results in table 5.6 we observe that Aut(C) is primitive on* D_{w_m}

Symmetric 1- Designs

In this section we consider G to be the simple Mathieu group M_{253} and examine symmetric 1-design invariant under G constructed from orbits of the rank - 3 permutation representation of degree 253. Table 5.7 shows Symmetric 1-Design where column one represents the 1-design D_k of orbit length k, column two gives the orbit length, t column three shows the parameters of the symmetric 1-design D_k and column four gives the automorphism group of the design.

Table 5.7: Symmetric 1-Design

Design	orbit length	parameters	Automorphism Group
D_{42}	42	1-(253,42,42)	$A_{23}:2$
D_{210}	210	1-(253,210,210)	$A_{23}:2$
D_{43}	43	1-(253,43,43)	$A_{23}:2$
D_{211}	211	1-(253,211,211)	$A_{23}:2$
D_{252}	252	1-(253,252,252)	$A_{253}:2$

Proposition 5.2.3. *Let G be the mathieu simple group M_{23}, and Ω the primitive G-set of size 253 defined by the action on the cosets of M_{23}. Let $\beta = \{\triangle^g \colon g \in G\}$ and $D_k = (\Omega, \beta)$. Then the following hold:*

i D_k is a primitive symmetric $1-(23, \mid \triangle \mid, \mid \triangle \mid)$ design.

ii $Aut(D_k) \cong A_{23}:2$ for some k= 42, 210, 43, 211

Proof

i From theorem 3.4.1, it is clear that G acts as an automorphism group, primitive on points and on blocks of the design and so G $\subseteq$ Aut(D_k).

ii The composition factors of Aut(D_k) are Z_2 and A_{23} and so Aut(D_k)= $A_{23}:2$. This implies that $Aut(D_k) \approxeq A_{23}:2$

□

Theorem 5.2.4. *Let G be the primitive group of degree 23 of M_{23} and C a linear code admitting G as an automorphism group. Then the following holds:*

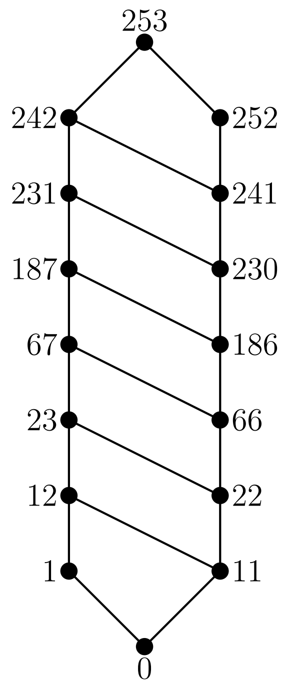
(a) There exist a self orthogonal irreducible doubly even projective code.

(b) There exist a set of Primitive Designs related to M_{23}.

5.3 The 2nd Representation of Degree 253

Let G be the Mathieu group M_{23}. Group G acts on heptad to generate a maximal subgroup of degree 253 in G. The group G acts on the maximal subgroup over $\mathbb{F}_2$ to form a module of dimension 253 invariant under G. The module breaks down into three completely irreducible parts of dimensions 1, 11, 44, 44 and 120 with multiplicities 1, 2, 2, 1 and 1 respectively. The two irreducible submodules are of dimension 1 and 11 . The module splits into 14 submodules of dimension 1, 11, 12, 22, 23, 66, 67, 186, 187, 230, 231, 241, 242 and 252. These submodules are the dimensions of the codes related with the module of dimension 253 . The submodule lattice is as shown in Figure 5.3

Figure 5.3: Submodule lattice of permutation module of dimension 253



We discuss four non trivial submodules of small dimensions 11, 12, 22 and 23. The binary linear codes from this representations are [253,11,112], [253, 12,77] , [253, 22, 88] and [253, 23, 77]. We make some observations about the properties of these codes. These properties are examined with certain detail in Proposition 5.3.1.

Proposition 5.3.1. *Let G be the Mathieu group M_{23} and $C_{253,1}$, $C_{253,2}$, $C_{253,3}$, $C_{253,4}$ be non-trivial binary code of dimension 11, 12, 22, 23 respectively obtained from the permutation module of degree 253. Then the following holds;*

i $C_{253,1}$ *is self orthogonal, doubly even and projective [253, 11,112] binary code . [253, 242, 4] is the dual code of* $C_{253,1}$ *. Furthermore* $C_{253,1}$ *is irreducible and* $Aut(\ C_{253,1}) \cong M_{23}$.

ii $C_{253,2}$ *is [253, 12,77] binary code . [253, 241, 4] is the dual code of* $C_{253,2}$ *. Furthermore* $C_{253,2}$ *is decomposable and* $Aut(\ C_{253,2}) \cong M_{23}$.

iii $C_{253,3}$ *is self orthogonal, doubly even and projective [253, 22,88] binary code . [253, 231, 5] is the dual code of* $C_{253,3}$ *. Furthermore* $C\ \perp_{253,3}$ *is 3-error correcting code and* $Aut(\ C_{253,3}) \cong M_{23}$.

iv $C_{253,4}$ *is projective [253, 23,77] binary code . [253, 230, 6] is the dual code of* $C_{253,4}$ *. Furthermore* $C_{253,4}$ *is decomposable and* $Aut(\ C_{253,4}) \cong M_{23}$.

proof

i The submodule 11 represents the dimension of binary code $\mathrm{C}_{253,1}$. From this submodule we determine the binary linear code $[253, 11,112]_2$. The polynomial of this code is $W(x) = 1 + 253x^{112} + 1771x^{128} + 23x^{176}$. We deduce that the weight of codewords are divisible by 4. $C_{253,1}$ is doubly even. The weight of $C^{\perp}_{253,1}$ code is 4. Hence $C_{253,1}$ is projective. From the lattice structure the submodule 11 is trivial which implies that $C_{23,1}$ is irreducible. For the structure of the automorphism group, let $\overline{G} \cong Aut(C_{253,1})$. $\overline{G}$ has only one composition factor M_{23} and the order of $\overline{G}$ is 10200960. This implies that $\overline{G} = M_{23}$. Since $M_{23} \subseteq \overline{G}$, we conclude that $\overline{G} \cong M_{23}$

ii The submodule 12 represents the dimension of binary code $C_{253,2}$. From this submodule we determine the binary linear code $[253, 12{,}112]_2$. The weight of $C^{\perp}_{253,2}$ code is 4. Hence $C_{253,2}$ is projective. From the lattice structure the submodule 12 is a direct sum of 11 and 1 which implies that $C_{23,2}$ is decomposable. For the structure of the automorphism group, let $\overline{G} \cong Aut(C_{253,2})$. $\overline{G}$ has only one composition factor M_{23} and the order of $\overline{G}$ is 10200960. This implies that $\overline{G} = M_{23}$. Since $M_{23} \subseteq \overline{G}$, we conclude that $\overline{G} \cong M_{23}$

iii The submodule 22 represents the dimension of binary code $C_{253,3}$. From this submodule we determine the binary linear code $[253, 22{,}88]_2$. From weight distribution , $C_{253,3}$ is doubly even. The weight of $C^{\perp}_{253,3}$ code is 5. For the structure of the automorphism group, let $\overline{G} \cong Aut(C_{253,3})$. $\overline{G}$ has only one composition factor M_{23} and the order of $\overline{G}$ is 10200960. This implies that $\overline{G}$ $= M_{23}$. Since $M_{23} \subseteq \overline{G}$, we conclude that $\overline{G} \cong M_{23}$

iv The submodule 23 represents the dimension of binary code $C_{253,4}$. From this submodule we determine the binary linear code $[253, 23,77]_2$. The weight of $C^{\perp}_{253,4}$ code is 6. From the lattice structure the submodule 23 is a direct product of 22 and 1 which implies that $C_{23,4}$ is decomposable. For the structure of the automorphism group, let $\overline{G} \cong Aut(C_{253,4})$. $\overline{G}$ has only one composition factor M_{23} and the order of $\overline{G}$ is 10200960. This implies that $\overline{G} = M_{23}$. Since $M_{23} \subseteq \overline{G}$, we conclude that $\overline{G} \cong M_{23}$ $\square$

Designs of codewords of minimum weight in $C_{253,i}$

We determine designs of codewords of of minimum weight in $C_{253,i}$. Table 5.8 shows Deigns of codewords of minimum weight in $C_{253,i}$ where column one represents the code $C_{23,i}$ of weight m and column two gives the parameters of the 1-designs D_{w_m} . In column three we list the number of blocks of D_{w_m}, four tests whether or not a design D_{w_m} is primitive .

Table 5.8: Deigns of codewords of minimum weight in $C_{253,i}$

Code	m	Designs	No of Blocks	Automorphism group	Primitive
$C_{253,1}$	112	1-(253, 112, 112)	253	M_{23}	Yes
$C_{253,2}$	77	1-(253, 77, 7)	23	M_{23}	yes
$C_{253,3}$	88	1-(253, 88, 448)	1288	M_{23}	yes
$C_{253,4}$	77	1-(253, 77, 7)	23	M_{23}	yes

Remark 5.3.2. *From the results in table 5.8 we observe that Aut(C) is primitive on all designs of minimum weight.*

Maximal subgroups of degree 23, 253, and 1288 in table 5.1 are stabilizers in M_{23}

and the blocks 23, 253,and 1288 in table 5.8 represents codewords of weight 77, 88 and 112 respectively.

Symmetric 1- Designs

It follows from theorem 3.4.1 that if we form orbits of the point stabilizer and take their images under the action of the full group, we get blocks of a symmetric 1 - design with the group G acting as an automorphism group. In this section we take G to be the Mathieu group M_{23} and examine symmetric 1-design invariant under G constructed from orbits of the rank - 3 permutation representation of degree 253. Table 5.9 shows Symmetric 1-Design where column one represents the 1-design D_k of orbit length k, the column two gives the orbit length, column three shows the parameters of the symmetric 1-design D_k and column four gives the automorphism group of the design.

Table 5.9: Symmetric 1-Design

Design	orbit length	parameters	Automorphism Group
D_{112}	112	1-(253,112,112)	M_{23}
D_{140}	140	1-(253,140,140)	M_{23}
D_{113}	113	1-(253,113,113)	M_{23}
D_{141}	141	1-(253,141,141)	M_{23}
D_{252}	252	1-(253,252,252)	$A_{253}:2$

Proposition 5.3.3. *Let G be the mathieu simple group M_{23}, and Ω the primitive G-set of size 253 defined by the action on the cosets of M_{23} . Let $\beta = \{\triangle^g \colon g \in G\}$ and $D_k = (\Omega, \beta)$.Let M=[112,140,113,141] and N=[252]. Then the following hold:*

i D_k *is a primitive symmetric* $1-(23, \mid \triangle \mid, \mid \triangle \mid)$ *design.*

ii For $k \in M$, $Aut(D_k) \cong M_{23}$

iii For $k \in M$, $Aut(D_k) \cong A_{253} : 2$

Proof

i From theorem 3.4.1 it is clear that G acts as an automorphism group, primitive on points and on blocks of the design and so G $\subseteq$ Aut(D_k).

ii Aut(D_k) has only one composition factor M_{23} . This implies that $Aut(D_k) \approxeq M_{23}$

iii The composition factors ofAut(D_k) are Z_2 and A_{253} This implies that $Aut(D_k) \approxeq A_{253} : 2$ □

Theorem 5.3.4. *Let* G *be the primitive group of degree 23 of* M_{23} *and* C *a linear code admitting* G *as an automorphism group. Then the following holds:*

(a) There exist a set of self orthogonal doubly even projective codes.

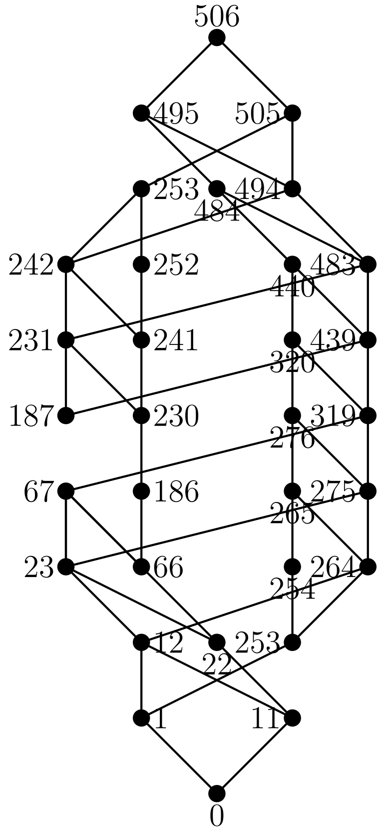
(b) Aut(C) $\cong M_{23}$

(c) Aut(C) is primitive on all t-designs held by the support of codewords of minimum weight related to M_{24}.

5.4 The Representation of degree 506

Given a permutation group G acting on a finite set Ω, we decompose the permutation module into submodules. These constitutes the building blocks for the construction of a lattice of submodules where possible . Let G be the Mathieu group M_{23}. Group G acts on octad to generate the maximal subgroup of degree 503 in G. The group G acts on a maximal subgroup over $\mathbb{F}_2$ to form a module of dimension 506 invariant under G. The module breaks down into three completely irreducible components of dimensions 1,11, 11, 44, 44, 120 and 252 with multiplicities 2, 2, 2, 1, 1, 1 and 1 respectively. There two irreducible submodules of dimension 1 and 11 in this representation . The permutation module splits into 30 maximal submodules. The 1st five submodules are 1, 11, 12, 22 and 23. The submodule lattice is as shown in Figure 5.4

Figure 5.4: Submodule lattice of the 506 dimensional permutation module



We discuss four non trivial submodules of small dimensions 11, 12, 22 and 23. The binary linear codes from this representations are [506,11,176], [506, 12,176] , [506, 22, 176] and [506, 23, 170]. We make some observations about the properties of these codes. These properties are examined with certain detail in Proposition 5.4.1.

Proposition 5.4.1. *Let G be the Mathieu group M_{23} and $C_{506,1}$, $C_{506,2}$, $C_{506,3}$, $C_{506,4}$ be non-trivial binary codes of dimension 11, 12, 22, 23 obtained from the permutation module of degree 506. Then*

i . $C_{506,1}$ is self orthogonal, doubly even and projective [506, 11,176] binary code

. [506, 495, 3] is the dual code of $C_{506,1}$ *. Furthermore* $C_{506,1}$ *is irreducible and Aut(* $C_{506,1}$*)* $\cong M_{23}$*.*

ii . $C_{506,2}$ is self orthogonal singly even and projective [506, 12,176] code . [506, 494, 4] is the dual code of $C_{506,2}$. Furthermore $C_{506,2}$ is decomposable and Aut($C_{506,2}$) $\cong M_{23}$.

iii . $C_{506,3}$ is self orthogonal doubly even projective [506, 22,176] code . [506, 484, 4] is the dual code of $C_{506,3}$. Furthermore Aut($C_{506,3}$) $\cong M_{23}$.

iv . $C_{506,4}$ is self orthogonal, doubly even and projective [506, 23,170] code. [506, 483, 4] is the dual codeof $C_{506,4}$. Furthermore Aut($C_{506,4}$) $\cong M_{23}$.

proof

i .The submodule 11 represents the dimension of binary code $C_{506,1}$. From this submodule we determine the binary linear code $[503, 11{,}176]_2$. The weight polynomial of this code is $W(x) = 1 + 23x^{176} + 253x^{240} + 1771x^{256}$. We deduce that weight of all codewords is divisible by 4. $C_{506,1}$ is doubly even. The weight of $C^{\perp}_{506,1}$ code is 3. Hence $C_{506,1}$ is projective. From the lattice structure the submodule 11 is a direct sum of trivial submodules 10 and 1 respectively which implies that $C_{506,1}$ is irreducible. For the structure of the automorphism group, let $\overline{G} \cong Aut(C_{506,1})$. $\overline{G}$ has only one Composition factor M_{23} and the order of $\overline{G}$ is 10200960. This implies that $\overline{G} = M_{23}$. Since $M_{23} \subseteq \overline{G}$, we conclude that $\overline{G} \cong M_{23}$

ii .The submodule 12 represents the dimension of binary code $C_{506,2}$. From this submodule we determine the binary linear code $[503,\ 12{,}176]_2$. The weight polynomial of this code is $W(x) = 1 + 23x^{176} + 253x^{240} + 1771x^{250} + 1771x^{256} + 253x^{266} + 23x^{330} + x^{506}$. We deduce that weight of all codewords is divisible by 2. $C_{506,2}$ is singly even. The weight of $C^{\perp}_{506,2}$ code is 4. Hence $C_{506,2}$ is projective. From the lattice structure the submodule 12 is a direct sum of 11 and 1 respectively which implies that $C_{506,2}$ is decomposable. For the structure of the automorphism group, let $\overline{G} \cong Aut(C_{506,2})$. $\overline{G}$ has only one Composition factor M_{23} and the order of $\overline{G}$ is 10200960. This implies that $\overline{G} = M_{23}$. Since $M_{23} \subseteq \overline{G}$, we conclude that $\overline{G} \cong M_{23}$

iii .The submodule 22 represents the dimension of binary code $C_{506,3}$. From this submodule we determine the binary linear code $[503,\ 22{,}176]_2$. The weight polynomial of this code is $W(x) = 1 + 1311x^{176} + 8855x^{208} + 17710x^{216} + 15456x^{220} + 60720x^{232} + 198352x^{236} + 554829x^{240} + 141680x^{244} + 212520x^{248} + 1275120x^{252} + 729652x^{256} + 89056x^{260} + 212520x^{264} + 344080x^{268} + 283360x^{272} + 28336x^{276} + 14674x^{280} + 4048x^{316} + 1771x^{320} + 253x^{336}$. We deduce that weights of all codewords are divisible by 2. $C_{506,3}$ is doubly even. The minimum of $C^{\perp}_{506,3}$ code is 4. Hence $C_{506,3}$ is projective. For the structure of the automorphism group, let $\overline{G} \cong Aut(C_{506,2})$. $\overline{G}$ has only one Composition factor M_{23} and the order of $\overline{G}$ is 10200960. This implies that $\overline{G} = M_{23}$. Since $M_{23} \subseteq \overline{G}$, we conclude that $\overline{G} \cong M_{23}$

iv .The submodule 23 represents the dimension of binary code $C_{506,4}$. From this submodule we determine the binary linear code $[503, 23,170]_2$. The weight enumerator of this code is $W(x) = 1+253x^{170}+1311x^{176}+1771x^{186}+4048x^{190}+ 8855x^{208}+17710x^{216}+15456x^{220}+14674x^{226}+28386x^{230}+60720x^{232}+283360x^{234}+ 198352x^{236}+344080x^{238}+554829x^{240}+212520x^{242}+141680x^{244}+89056x^{246}+ 212520x^{248}+729652x^{250}+1275120x^{252}+1275120x^{254}+729652x^{256}+212520x^{258}+ 89056x^{260}+141680x^{262}+212520x^{264}+554829x^{266}+344080x^{268}+198352x^{270}+ 283360x^{272}+60720x^{274}+28336x^{276}+14674x^{280}+15456x^{286}+17710x^{290}+ 8855x^{298}+4048x^{316}+1771x^{320}+1311x^{330}+253x^{336}+x^{506}$. From weight polynomial we deduce that all weights of codewords are divisible by 2. $C_{506,4}$ is singly even. The minimum weight of $C^{\perp}_{506,4}$ code is 4. Hence $C_{506,4}$ is projective. For the structure of the automorphism group, let $\overline{G} \cong Aut(C_{506,4})$. $\overline{G}$ has only one Composition factor M_{23} and the order of $\overline{G}$ is 10200960. This implies that $\overline{G} = M_{23}$. Since $M_{23} \subseteq \overline{G}$, we conclude that $\overline{G} \cong M_{23}$ □

Designs of Codewords of Minimum Weight in $C_{506,i}$ Code

Suppose that D_m is a design of codewords of minimum weight m in $C_{506,i}$, we determine the primitivity of Aut(C) . Table 5.10 shows Deigns of codewords of minimum weight in $C_{506,i}$ where t column one represents the minimum weight of a codeword in $C_{506,i}$ and column two gives the parameters of the t-designs D_m . Column three represents the Aut (D_m), four tests whether or not a design D_m is primitive under the action of Aut(D_m).

Table 5.10: Deigns of codewords of minimum weight in $C_{506,i}$

m	D_m	Aut(D_m)	primitive
176	1-(506, 176, 8)	M_{23}	yes
3	1-(506, 3, 105)	M_{23}	yes
70	1-(506, 170, 85)	M_{23}	yes
4	1-(506, 4, 210)	M_{23}	yes

Remark 5.4.2. *From the results in table 5.10 we observe that Aut(D_m) is primitive on D_m*

Symmetric 1- designs

It follows from theorem 3.4.1 that if we form orbits of the point stabilizer from a primitive permutation group G acting on a set Ω, and take their images under the action of the full group, we obtain the blocks of of a symmetric 1 - design with the group G acting as an automorphism group. In this section we consider G to be the simple Mathieu group M_{23} and examine symmetric 1-design invariant under G constructed from orbits of the rank - 2 permutation representation of degree 506. Table 5.11 shows Symmetric 1-Design where column onne represents the 1-design D_k of orbit length k, column two gives the orbit length, column three shows the parameters of the symmetric 1-design D_k and column four gives the automorphism group of the design.

Table 5.11: Symmetric 1-Design

Design	orbit length	parameters	Automorphism Group
D_{15}	15	1-(506,15,15)	M_{23}
D_{210}	210	1-(506,210,210)	M_{23}
D_{280}	280	1-(506,280,280)	M_{23}
D_{16}	16	1-(506,16,16)	M_{23}
D_{211}	211	1-(506,211,211)	M_{23}
D_{281}	281	1-(506,281,281)	M_{23}
D_{225}	225	1-(506,225,225)	M_{23}
D_{295}	295	1-(506,295,295)	M_{23}
D_{490}	490	1-(506,490,490)	M_{23}
D_{226}	226	1-(506,226,226)	M_{23}
D_{296}	296	1-(506,296,296)	M_{23}
D_{491}	491	1-(506,491,491)	M_{23}
D_{505}	505	1-(506,505,505)	$A_{506}:2$

Proposition 5.4.3. *Let G be the mathieu simple group M_{23}, and Ω the primitive G-set of size 506 defined by the action on the cosets of M_{23}. Let $\beta = \{\triangle^g : g \in G\}$ and $D_k = (\Omega, \beta)$. Then the following hold:*

i *D_k is a primitive symmetric $1-(506, \mid \triangle \mid, \mid \triangle \mid)$ design.*

ii *$Aut(D_k) \cong M_{23}$*

iii *$Aut(D_k) \cong A_{506} : 2$*

Proof

i From theorem 3.4.1, and from this it is clear that G acts as an automorphism group, primitive on points and on blocks of the design and so G $\subseteq$ Aut(D_k).

ii The only composition factor of Aut(D_k) is M_{23}. This implies that $Aut(D_k) \approxeq$

M_{23}

iii The composition factors of $\mathrm{Aut}(D_k)$ are $\mathbb{Z}_2$ and $\mathbb{A}_{506}$. This implies that $Aut(D_k) \approxeq A_{506} : 2$ $\square$

Theorem 5.4.4. *Let G be a simple group M_{23} , C the 1st non trivial binary code from a representation of degree 506 and D_m a t-design held by the support of codeword of minimum weight. Then the following hold:*

(a) C is projective, self orthogonal doubly even code .

(b) Aut(C) $\cong M_{24}$

(c) Aut(D_m) is primitive on all designs of codewords of minimum weight related to M_{23}.

5.5 Conclusion

We constructed and enumerated all G-invariant codes from primitive permutation representations of degree 23, 253, and 253 from the simple group M_{23}. We classified the G-invariant codes using the lattice diagram. From the lattice diagram we did not find any self dual code. There were five irreducible codes and several decomposable codes. We also constructed codes of small dimensions due to computer limitations and found several self orthogonal and projective codes. There was no strongly regular graph from the three representations. We determined designs from some binary codes using codewords of minimum weight. We found that all the designs were primitive. We constructed symmetric 1-designs from the primitive permutation representations of degree 23, 253 and 253. We found that in most cases the full automorphism group of the design was M_{23}

References

[1]. E. F. Assmus, Jr. and J. D. Key, (1996). Designs and their codes: an update, *Designs, Codes and Cryptography.* Vol 9, Issue 1, 7 - 27.

[2]. T. Beth, D. Jungnickel, and H. Lenz, (1999). *Design Theory*, Cambridge University Press, Cambridge, ISBN 9780521772310.

[3]. N. L. Biggs and A. T. White(1979). *Permutation Groups and Combinatorial Structures*, Cambridge University Press, London Mathematical Society Lecture Note Series 33, ISBN 9780511600739.

[4]. E. Byrn, M. Greerath, and Honold T (2008). Ring geometries, two weight codes and strongly regular graphs, *Designs Codes and Cryptology*, 1 - 16.

[5]. R. Calderbank and W. M. Kantor (1986). The geometry of two-weight codes, *The London Mathematical Society*, Vol 18, 97 - 122.

[6]. P. J. Cameron and J. H. van Lint (1991), *Designs, Graphs, Codes and their Links*, Cambridge University Press, Cambridge, London Mathematical Society, Student Texts 22, ISBN 9780511623714.

[7]. P. J. Cameron(1999), *Permutation Groups*, London Math. Soc. Student Texts 45, Cambridge Univer-sity Press, Cambridge, 232pp. ISBN: 0 521 65302 9

(Hardback), 0 52165378 9 (Paperback)

[8]. Y. Cheng and N. J. Sloane(1989),Codes from symmetry groups and [32, 17, 8] code, *SIAM Journal on Discrete Mathematics*, Vol. 2, No. 1 : pp. 28-37

[9]. L. Chikamai, J. Moori, and B. G. Rodrigues(2012), *Linear codes obtained from 2-modular representations of some finite simple groups*.Ph.D. thesis DSpace software copyright 2002-2013 Duraspace

[10]. P. Delsarte (1972),Weight of linear codes and strongly regular normed spaces, *Discrete Mathematics* Volume 3, Issues 13, Pages 47-64

[11]. U. Dempwolff(2001),Primitive rank-3 groups on symmetric designs.*Designs, Codes and Cryptography*, Volume 22, Issue 2, pp 191207

[12]. J. D. Dixon and B. Mortimer(1996),The Structure of the Symmetric Groups, *Permutation Groups*, Springer Verlag, New York.

[13]. M.J.E Golay(1949), *Notes on digital coding* Proc.IRE,687

[14]. M. Grassl(2006), *Searching for Linear Codes with Large Minimum Distance*,Discovering Mathematics with Magma (Wieb Bosma and John Cannon, eds.), Springer, New York.

[15]. W. H. Haemers (1979), *Eigenvalue Techniques in Design and Graph Theory*, Ph.D. thesis, Eindhoven University of Technology.

[16]. R.P.Hansen (2011), *Construction and Simplicity of the Large Mathieu Group*,,Masters Theses 4053.

[17]. D. G. Higman, *Finite permutation groups of rank 3*, Math. Z. 86 (1964), 145156.

[18]. W. M. Kantor and R. A. Liebler (1982), *The rank-3 permutation representations of the finite classical groups*, Trans. American Math. Soc. 271 , 171.

[19]. J. D. Key and J. Moori(2002), *Designs, codes and graphs from the Janko groups J_1 and J_2*, J. Combin. Math. and Combin. Comput. 40 , 143159.

[20]. M. W. Liebeck(1987), *The affine permutation groups of rank three*, Proc. London Math. Soc. 54 , no. 3, 477516.

[21]. M. W. Liebeck and J. Saxl(1986), *The finite permutation groups of rank three, Bull.*London Math. Soc. 18 , 165172.

[22]. J. Moori and G.F. Randriafanomezantsoa (2014), *Designs and codes from certain finite groups.*Transactions on CombinatoricsISSN (print): 2251-8657, ISSN (on-line): 2251-8665Vol. 3 No. 1 (2014), pp. 15-28. University of Isfahan

[23]. B. G. Rodrigues(2003), *Codes of Designs and Graphs from Finite Simple Groups*, Ph.D. thesis, University of Natal, Pietermaritzburg,

[24]. J. J. Rotman(1995), *An Introduction to the Theory of Groups*, Fourth ed., SpringerVerlag,New York, Inc.

[25]. S. A. Spence(2002), *Introduction to Algebraic Coding Theory*,Supplementary

material for Math 336 Cornell University.

[26]. R. A. Wilson, R. A. Parker, and J. N. Bray, *Atlas of Finite Group Representations*, `http://brauer.maths.qmul.ac.uk/Atlas/clas/S62/`.

[27]. S.M. Tendai(2014), *On the existence of self-dual codes invariant under permutation groups*, Msc. thesis, University of KwaZulu-Natal.

Appendices

A) A representation of degree 276

$G < x, y >$:= PermutationGroup¡24— $[4, 7, 17, 1, 13, 9, 2, 15, 6, 19, 18, 21, 5, 16, 8, 14, 3, 11, 10, 24, 12, 23, 22, 20]$,$[4, 21, 9, 6, 18, 1, 7, 8, 15, 5, 11, 12, 17, 2, 3, 13, 16, 10, 24, 20, 14, 22, 19, 23]$
print "Group G is M24 ¡ Sym(24)";

M:=MaximalSubgroups(G);
H:=M[6]'subgroup;
a1,a2,a3:=CosetAction(G,H);
g1:=PermutationModule(a2,GF(2)); g1;
GModule g1 of dimension 276 over GF(2)
m:= Submodules(g1);m;

GModule of dimension 0 over GF(2),
GModule of dimension 1 over GF(2),
GModule of dimension 11 over GF(2),
GModule of dimension 12 over GF(2),
GModule of dimension 22 over GF(2),
GModule of dimension 23 over GF(2),
GModule of dimension 23 over GF(2),
GModule of dimension 23 over GF(2),
GModule of dimension 24 over GF(2),
GModule of dimension 55 over GF(2),
GModule of dimension 56 over GF(2),
GModule of dimension 66 over GF(2),
GModule of dimension 66 over GF(2),
GModule of dimension 66 over GF(2),
GModule of dimension 67 over GF(2),
GModule of dimension 67 over GF(2),
GModule of dimension 67 over GF(2),
GModule of dimension 67 over GF(2),
GModule of dimension 67 over GF(2),
GModule of dimension 68 over GF(2),
GModule of dimension 77 over GF(2),
GModule of dimension 78 over GF(2),
GModule of dimension 78 over GF(2),

GModule of dimension 78 over GF(2),
GModule of dimension 78 over GF(2),
GModule of dimension 79 over GF(2),
GModule of dimension 89 over GF(2),
GModule of dimension 90 over GF(2),
GModule of dimension 186 over GF(2),
GModule of dimension 187 over GF(2),
GModule of dimension 197 over GF(2),
GModule of dimension 198 over GF(2),
GModule of dimension 198 over GF(2),
GModule of dimension 198 over GF(2),
GModule of dimension 198 over GF(2),
GModule of dimension 199 over GF(2),
GModule of dimension 208 over GF(2),
GModule of dimension 209 over GF(2),
GModule of dimension 209 over GF(2),
GModule of dimension 209 over GF(2),
GModule of dimension 209 over GF(2),
GModule of dimension 209 over GF(2),
GModule of dimension 210 over GF(2),
GModule of dimension 210 over GF(2),
GModule of dimension 210 over GF(2),
GModule of dimension 220 over GF(2),
GModule of dimension 221 over GF(2),
GModule of dimension 252 over GF(2),
GModule of dimension 253 over GF(2),
GModule of dimension 253 over GF(2),
GModule of dimension 253 over GF(2),
GModule of dimension 254 over GF(2),
GModule of dimension 264 over GF(2),
GModule of dimension 265 over GF(2),
GModule of dimension 275 over GF(2),
GModule g1 of dimension 276 over GF(2)

$\#m$;
56
$[\#m[i] : iin[1..\#m]]$;
1, 2, 2048, 4096, 4194304, 8388608, 8388608,
8388608, 16777216, 36028797018963968,
72057594037927936,
73786976294838206464, 73786976294838206464,
73786976294838206464, 147573952589676412928,

1475739525896764129 28,
1475739525896764129 28, 1475739525896764129 28,
1475739525896764129 28, 2951479051793528258 56,
151115727451828646838272,
302231454903657293676544,
302231454903657293676544,
302231454903657293676544,
302231454903657293676544, 604462909807314587353088, 618970019642690137449562112,
1237940039285380274899124224,
98079714615416886934934209737619787751599303819750539264,
196159429230833773869868419475239575503198607639501078528,
200867255532373784442745261542645325315275374222849104412672,
401734511064747568885490523085290650630550748445698208825344,
401734511064747568885490523085290650630550748445698208825344,
401734511064747568885490523085290650630550748445698208825344,
401734511064747568885490523085290650630550748445698208825344,
803469022129495137770981046170581301261101496891396417650688,
4113761393303015105387422956393376262456839664083949658371522 56,
8227522786606030210774845912786752524913679328167899316743045 12,
8227522786606030210774845912786752524913679328167899316743045 12,
8227522786606030210774845912786752524913679328167899316743045 12,
8227522786606030210774845912786752524913679328167899316743045 12,
8227522786606030210774845912786752524913679328167899316743045 12,
16455045573212060421549691825573505049827358656335798633486090 24,
16455045573212060421549691825573505049827358656335798633486090 24,
16455045573212060421549691825573505049827358656335798633486090 24,
168499666669691498716668844293872691710232152640878578006897564 0576,
33699933333938299743333768858774538342046430528175715601379512 81152,
723700557733226221397318656304299424082937404160253525246609900049457060 2496,
1447401115466452442794637312608598848165874808320507050493219800098914120 4992,
1447401115466452442794637312608598848165874808320507050493219800098914120 4992,
1447401115466452442794637312608598848165874808320507050493219800098914120 4992,
2894802230932904885589274625217197696331749616641014100986439600197828240 9984,
2964277484475294602843417216222410441043711607440398439410114150602576118 7823616,
5928554968950589205686834432444820882087423214880796878820228301205152237 5647232,
607084028820540334662331845882349658325752137203793600391191378043407589126627655 68
121416805764108066932466369176469931665150427440758720078238275608681517825325531 1
c1:=LinearCode(Morphism(m[3],g1));
c2:=LinearCode(Morphism(m[4],g1));
c3:=LinearCode(Morphism(m[5],g1));
c4:=LinearCode(Morphism(m[6],g1));

A:=c1;
$[Length(A), Dimension(A), MinimumDistance(A)]$;
$[276, 11, 128]$
WeightDistribution(A);
$[< 0, 1 >, < 128, 759 >, < 144, 1288 >]$
B:=AutomorphismGroup(A);
CompositionFactors(B);
G — M24
1 wt:=WeightDistribution(A);
wt:=128;
wt;
128
wds := Words(A, wt);
#wds;
759
D := Design¡ 1, Length(A) — wds ¿;
D;
1-(276, 128, 352) Design with 759 blocks
E:=AutomorphismGroup(D);
CompositionFactors(E);
G — M_{24}
1
st:=Stabilizer(a2,1);st;
Permutation group st acting on a set of cardinality 276
$Order = 887040 = 2^8 * 3^2 * 5 * 7 * 11$
orbs:=Orbits(st);#orbs;
3
$[\#orbs[i] : iin[1..\#orbs]]$; $[1, 44, 231]$ k:=[orbs[1],orbs[2], orbs[3],orbs[1] join orbs[2], orbs[1] join orbs[3], orbs[2] join orbs[3]];
$[\#k[i] : iin[1..\#k]]$;
$[1, 44, 231, 45, 232, 275]$
$blox := Setseq(k[5]^a 2)$;
D:=Design¡1,v—blox¿;

D:=Design¡1,v—blox¿ ;
^{D};
$1 - (276, 128, 352) Designwith 759 blocks$
$E := AutomorphismGroup(D)$;
$CompositionFactors(E)$;
$G|M24$
1

B) Publications

1).**Some Codes, Designs and Graphs of Degree 759 related to Mathieu Group** M_{24}

ISBN: 05B05, 20D45, 94B05

Abstract
Let G be a primitive group . We enumerate and classify all G-invariant codes preserved by primitive group of degree 276 related to M_{24} *using modular representation method. We determine binary codes of small dimensions and study their properties . We construct some t- designs using codewords of minimum weight and determine their primitivity . We establish the links between primitive groups, codes, designs and graphs. We construct self-dual symmetric 1-designs preserved by primitive groups of* M_{24} *. We study the properties of these designs.*

Key words: Binary codes, designs and Modules

2). **A Primitive Representation of Degree 276 Related to Mathieu Group**M_{24}

ISSN (Print) 2319 - 4537, (Online) 2319 - 4545.

Abstract
Let G be a primitive group M24. We construct and enumerate all binary linear codes preserved by primitive group of degree 276. We study the properties of these codes where computations are possible. We look for the existence of two weight codes and strongly regular graphs. We determine designs defined by the support of codewords of minimum weight and establish links with primitive groups, codes and graphs. We construct and enumerate all symmetric 1-designs preserved by this primitive group.

Keywords: Strongly Regular Graph, Two Weight Code, Symmetric 1-Design, Automorphism Group, Modular Representation.