CODES, DESIGNS AND GRAPHS OBTAINED FROM SOME PROJECTIVE SYMPLECTIC GROUP

Rukaria Lydiah Kananu

A Thesis submitted in fullfilment of the requirements for the degree of Doctor of Philosophy in Pure Mathematics in the Faculty of Science of Kibabii University

2019

Declaration

The research reported in this Thesis was carried out under the supervision of Dr. Lucy Walingo Chikamai, Mathematics Department, Kibabii University and Prof. Ireri kamuti, Mathematics Department, Kenyatta University. It is the authors original work except where otherwise due reference has been made. It has not been submitted before for any other degree to any other institution.

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

Rukaria Lydiah Kananu

PhD/MAT/01/14

Approval

We, the undersigned certify that we have read and hereby recommend for acceptance of Kibabii University a Thesis entitled,"Codes, Designs and Graphs obtained from some Projective Symplectic Groups ".

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

Dr. Lucy Chikamai

Department of Mathematics

Kibabii University.

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

Prof. Ireri Kamuti

Department of Mathematics

Kenyatta University.

Copyright

This thesis is a copyright material under the Berne convention, the copyright Act of 1999 and other international and national enactments in that behalf on intellectual property. It may not be reproduced by any means in full or in parts except for short extracts in fair dealings, for research or private study, critical scholarly review or disclosure with acknowledgement, with written permission of the Dean School of Graduate Studies on behalf of both the author and Kibabii University.

Abstract

After the classification of finite simple groups, there is still much work to be done to give a clear geometric identification of the finite simple groups. There are also many problems in enumerating and characterizing a structure which either has a particular group acting on it or which has some degree of symmetry from a group action. It has been shown that there exists interplay between finite simple groups and codes. In this thesis we construct and enumerate binary linear codes for the projective symplectic group $S_8(2)$ from the permutation representations of degree 120, 136, 255, 2295, 5355, 5440 and 11475. We find that the support of codewords of a given weight in a code hold a combinatorial design, or represent points of a projective space $PG(2m-1,q)$, or represent the rows of the adjacency matrix of a graph or equivalently are the incidence vectors of the blocks of a design. Through coding theory, the interplay between the combinatorial objects is enhanced and the internal structures of the group characterized.

Dedication

To my late mother Gladys Naitore Rukaria who was my first Mathematics teacher.

Acknowledgements

I offer my most sincere gratitude to my supervisors Dr Lucy Chikamai and Professor Ireri Kamuti for their selfless invaluable guidance without whom the present work would not have been possible.

With great humility, l appreciate Kibabii University for offering me a chance to pursue my dreams in the University and providing us with selfless lectures and excellent facilities. I acknowledge the entire members of staff at Kibabii University Department of Mathematics for your great welcome and hospitality any time l visited my Supervisor.

To my colleagues Vincent and Cedric, l salute you for your invaluable contributions during our discussion time.

I thank the Chairman of the Pure and Applied Mathematics Department: Esther Njue, the Director of the School of Mathematics: Professor Thomas Onyango and the Executive Dean of the Faculty of Science and Technology: Professor Francis Gatheri, all of the Technical University of Kenya, for reducing my workload by half within the 2017- 2018 academic year, to enable me compile my research findings.

To my daughters Lorraine and Lynnette, thank you for your invaluable support in attending to most of the house chores during the course of this research. To my apple in the eye, Baby Brielle for your lovely "distractions" at the most appropriate times.

Above all, I thank God for His favor upon me, for setting me apart to be able to start and complete this kind of assignment.

List of notations and terminologies

C	Linear code.
$\mathcal{D}$	An incidence structure
Γ	A graph
$\|\Omega\|$	Cardinality of a set
$\|\triangle\|$	Length of an orbit
$\mathbb{F}G$	Group algebra
$\mathbb{F}\Omega$	$\mathbb{F}$G - module
$1_G, e$	Identity of the element of group G.
I_n	Identity matrix of order n
$\emptyset$	Empty set
V	Vector space
$\mathbb{F}$	A Field
GF(q), $\mathbb{F}_q$	The Galois Field of q elements
G, H, K	Groups
S	Base Set
$\|G\|$	Order of a group G
$Aut(G)$	Automorphism group of G
$Aut(C)$	Automorphism group of a code C
$Aut(\mathcal{D})$	Automorphism group of a design $\mathcal{D}$
K< G	K is a proper subgroup of G
$K \leq G$	K is a subgroup of G
$K \trianglelefteq G$	K is normal subgroup of G
$H \cong G$	H is isomorphic to G
gkg^{-1}	Conjugation of k by g
$[n, k, d]_q - Code$	a q - ary code of length n, dimension k, minimum distance d
$C_P\mathcal{D}$	p-ary code of an incidence structure $\mathcal{D}$
$GL_n(q)$	General linear group of dimension n over $\mathbb{F}_q$

$GL(V)$	General linear group over V
$PGL(n,q)$	Projective general linear group
$PSL(n,q)$	Projective special linear group
$dim(V)$	The dimension of a vector space V
S_n	The symmetric group on n symbols
S_Ω	Symmetry group on Ω
G.H	A general extension of G by H
G:H	A split extension of G by H
$G^{\cdot}H$	A non split extension of G by H
G_α	Stabilizer of $\alpha \in \Omega$ when G acts on Ω
A_n	The alternating group on n symbols
H^n	Direct product of n groups which are isomorphic to H
p^{n+m}	An extension of p^n by p^m
PG(n,q)	Projective space of order n over $GF(q)$
[G : H]	Index of H in G
$S_n(q)$	Projective Symplectic group of degree n over GF(q)

Table of Contents

Chapter 1

Introduction

In 1948, Claude Shannon published the paper, " A Mathematical theory of Communication "that prompted the start of algebraic coding theory and information theory [1]. This was as a result of an effort to detect and control errors caused by distortion and interference during data transmission and data storage. In error correcting codes redundant information is added to a message in order to detect and correct errors once data is transmitted. For instance in radio communication between pilots and radar controls, alphabetical letters are spoken phonetically as "Alpha", "Bravo", "Charlie" etc however "Adams", "Boston", "Chicago" is more frequently used for spellings in telephone conversations. Adding a parity check symbol aids in detecting errors like in ISBN code for books, the European Article Numbering (EAN) and the Universal Product Cost (UPC) for articles. There exists immense application of error correcting codes in applications such as audio visual media, deep space communication and error tolerant computers. Considering the block diagram of a communication system, the encryption and decryption of codes utilizes mathematical tools in algebra and combinatorics. Shannon's paradigm gave rise to information theory and his findings support what is and what is not possible in a probabilistic sense. Though coding theory is rooted in communications, it is richly related to many other combinatorial objects such as groups, designs, graphs, and finite geometries to name just but a few. The properties of the codes and the other combinatorial objects derive from the underlying structure. The structure of a group is deeply embedded with the structure of the objects it preserves. To some extent we can say that these objects exist in the group itself. This not only aids in understanding the chosen group, it enhances the characterization of the combinatorial objects and also brings out the interplay between these combinatorial objects.

The Classification of Finite Simple Groups (CFSG) was a monumental achievement in February 1981. The CFSG theorem states that every finite simple group is isomorphic to

one of the following: - a Cyclic group C_p of prime order p, an Alternating group A_n for $n \geq 5$, a Classical group (Linear, Unitary, Symplectic, Orthogonal), an exceptional group of Lie type and one of the 26 Sporadic simple groups [8]. This theorem has been proved in approximately 15000 pages of journal papers by hundreds of authors. This impressive and monumental achievement in the history of Mathematics can only be appreciated if clearly understood though it is difficult considering the volume of work involved. To this day no one researcher clearly understands the entire proof. This has led to a team of researchers to embark on a study of how to simplify the proof. To help achieve this, an understanding of the internal structures of these groups is needed and various mathematical tools and methods must be utilized. This is mainly being done by using combinatorial objects like codes, designs, graphs and finite geometries.

This thesis is a study of binary linear codes obtained from the projective symplectic group of order 8 in $\mathbb{F}_2$. This group is denoted as $S_8(2)$ using the $\mathbb{ATLAS}$ [8] standard notation. This is an enumeration and classification problem which is not only important in itself but also shows how finite simple groups, codes, designs and finite geometries interact. We are of the view that since enumeration and classification problems are labor intensive, the enumeration and classification of linear codes invariant under the prescribed group is an intricate problem. The probability of finding all codes invariant under large groups diminishes due to the large degree of their representation and the large dimension of the submodules of a permutation module linked to a given permutation representation. Also a definite or complete answer may not easily be attainable due to the many perspectives and approaches available and also due to current computational limitations especially when the degree of the primitive representations is large.

In chapter 2 we present general results on group theory and combinatorial structures that will be required in the thesis. This chapter gives the background materials and results required from the theories of groups, codes, designs, representation theory, finite geometry and graphs for the development and application of the methodology.

In chapter 3 we discuss two methods of constructing codes from the simple finite groups. In the first method discussed, we use a series of maximal submodules of the corresponding

permutation module. The module is broken into irreducible non isomorphic submodules, which are actually the q - ary codes. This method is advantageous in that it provides an explicit basis of the code. However, the method pauses a lot of computational limitations when the primitive permutation representation has a large degree. In the second method the primitive permutation representations of simple groups are considered to construct the symmetric self dual 1 - designs. The row vectors of the incidence matrix of the block design are the codewords of a code C.

In chapter 4, we describe the general projective symplectic group $S_{2m}(q)$ and our chosen specific projective symplectic group $S_8(2)$. We chose this group because no study has been done to try and establish the interplay between the combinatorial objects it holds. Previous studies focusing on this subject area for symplectic groups have been carried out on $S_4(3)$ and $S_4(4)$ by Rodriguez in [23, 24] and on $S_6(2)$ by Chikamai in [7]. We explore the interplay between the combinatorial structures for the group $G = S_8(2)$ for the primitive permutation representation of degree 120 by first establishing the codes as $G-$*invariant* submodules. We find that the words of the codewords with minimum weight have a geometrical meaning and that the automorphism group of the code is the group $S_8(2)$ or $L_8(2)$.

In chapter 5, we establish the interplay between the combinatorial structures for the group G for the primitive permutation representation of degree 136 by first establishing the codes as $G-$ *invariant* submodules.

Chapter 6 gives key results on the interplay between the combinatorial structures for permutation representation of degree 255. The words of minimum weight of a code spans the incidence matrix of the geometric 1 - design generated from the code.

In chapter 7 a method described by Key and Moori in [18] has been applied to the permutation representations of degree 2295, 5355, 5440 and 11475 to constuct the symmetric 1 - designs and where possible, the codes of the design. Where computationally possible, we were able to establish the relationship between the 1 - symmetric designs, the code it holds, the associated graph and the properties of these structures.

We conclude with an insight of continuing with this study further, at that point in time when we are able to overcome all or most of the computational limitations.

In the appendix, we list some MAGMA implementations of the methods used and some weight distributions of some codes.

Chapter 2

Basic Concepts

In this chapter we present general results on group theory and combinatorial structures that will be required in the thesis. This chapter gives the background materials and results required from the theories of groups, codes, designs, representation theory, finite geometry and graphs for the development and application of the methodology.

2.1 Groups

Groups came in place as a tool for studying symmetrical objects. The symmetry of the object is defined as a transformation of the object that preserves its vital structure. It is always possible to regard any object as a set endowed with an added structure. Thus a symmetry is a structure preserving one by one and onto mapping form a set to itself.

Definition 2.1.1. *Given a non-empty set G equipped with a binary operation $* : G \times G \to G$. The pair $(G, *)$ is a called a* ***group*** *if :*

i) Closure property: For all $x, y \in G, x * y \in G$.

ii) $*$ is associative. That is for all $x, y, z \in G, (x * y) * z = x * (y * z)$.

iii) Some element e of G is an identity element for G. That is $e * x = x * e = x$ for all x in G

iv) For every element $x \in G$, there exists an inverse element $x^{-1} \in G : x^{-1} * x = x * x^{-1} = e$.

Definition 2.1.2. ***Group Action***
Given a group G and a non - empty set Ω, the left action of G on the set Ω is defined as follows: for every $\alpha \in \Omega$ and $g \in G$, there exists a unique element $g\alpha \in \Omega$ such that for all $\alpha \in \Omega$ and $g_1, g_2, \in G$;

i) $(g_1, g_2)\alpha = g_1(g_2\alpha)$

ii) $e\alpha = \alpha$ *where* e *is the identity in* G.

To an abstract group, group actions provide more concrete understanding of the set Ω on which the group is acting. That set can be the group itself or a set of subsets of that group. The main tools used in the construction methods used throughout this thesis are based on group actions.

Definition 2.1.3. ***Orbit***

Given the action of G *on the set* Ω *and* $\alpha \in \Omega$, *the orbit of* α *is the set* $Orb_G(\alpha) = \{g\alpha : g \in G\}$.

Definition 2.1.4. ***Stabilizer***

Let the group G *act on a set* Ω *and let* $\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_t \in \Omega$.

i) *The stabilizer of* α_0 *in* G *is* $Stab_G(\alpha_0) = \{g \in G : g\alpha_0 = \alpha_0\}$. *This set is also denoted by* G_{α_0} *and it is a subgroup of* G.

ii) *The stabilizer of the* t *points* $\alpha_1, \alpha_2, \cdots, \alpha_t$ *is the subgroup* $G_{\alpha_1,\alpha_2,\cdots,\alpha_t} = \{g \in G : g\alpha_i = \alpha_i, 1 \leq i \leq t\}$.

iii) *If* $Y \subseteq \Omega$, *the stabilizer of* Y *is the subgroup* $G_Y = \{g \in G : gY = Y\}$.

Remark 2.1.1. *If* $Y = \{\alpha_1, \alpha_2, \cdots, \alpha_t\}$,*then* $G_{\alpha_1,\alpha_2,\cdots,\alpha_t} < G_Y$.

Definition 2.1.5. ***Transitive Action***

Given a group G *acting on a non - empty set* Ω*:*

i) *The action is said to be transitive if for each pair of points* $\alpha_1, \alpha_2 \in \Omega$, *there exists a* $g \in G$ *such that* $g\alpha_1 = \alpha_2$. *That is, the action has a single orbit.*

ii) G *is* k *- transitive on the set* Ω *if for each pair of ordered* k *- tuples of different elements of* Ω, *there corresponds a single element of* G *which maps the first element to the second element. That is, for all* $(\alpha_1, \alpha_2, \cdots, \alpha_k), (\beta_1, \beta_2, \cdots, \beta_k) \in \Omega$, *with* $\alpha_i \neq \alpha_j$ *and* $\beta_i \neq \beta_j$, *we can find a* $g \in G$ *such that* $g\alpha_i = \beta_i$.

iii) *The action of* G *on the set* Ω *is said to be faithful if for all* $g \in G$ *and* $\alpha \in \Omega, g\alpha = \alpha$ *iff* $g = eG$ *where* e *is the identity in* G. *In this case* G *is said to be* ***faithful*** .

Definition 2.1.6. ***Group Extension***
Let S and T be groups. The extension of S by T is any group G with a normal subgroup $M \cong S$, for which $G/M \cong T$. In this case G is denoted by $S.T$.

Remark 2.1.2. *Given $S \trianglelefteq G$ and $T < G$ with $S \cap T = \{e\}$, the extension $G = S.T$ is called a* ***split extension*** *or* ***a semi direct product*** *and is denoted by $S : T$. A non split extension is any extension $S.T$ which is not a split extension and is denoted by $S.T$.*

If we consider the extension as a product between two groups and the quotient as a division, then a simple group is an irreducible finite group. Irreducible in the sense that it is not a product (extension) of any other finite groups.

Definition 2.1.7. ***Simple Group*** *A group G having no non trivial normal subgroups is said to be simple.*

By Jordan Holder's theorem, any group G with known cardinality can be broken down into a unique set of simple groups and can also be reconstructed as particular successive extensions by these simple groups [3]. Hence the finite simple groups are the building blocks of finite groups. The classification of all finite simple groups theoretically implies a classification of all finite groups.

Theorem 2.1.1. [8] *CFSG theorem:*
Every finite simple group is isomorphic to one of the following groups:

i) A cyclic group C_p of prime order p.

ii) An alternating group A_n of degree n, for $n \geq 5$.

iii) A simple group of Lie type:
- *The classical Lie groups, namely:*

- Linear: $L_n(q), n \geq 2$

- Unitary: $U_n(q), n \geq 3, q \geq 3$

- Symplectic: $S_{2n}(q), n \geq 2, q \geq 2$

-Orthogonal: $O^{\varepsilon}_{2n}(q), n \geq 4, \varepsilon = \pm O_{2n+1}(q), q odd$ Where q is a prime power of p.

- *The Exceptional groups of Lie type and the twisted groups of Lie type.*

iv) One of the Sporadic simple groups:

- *The Mathieu groups:* $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$.
- *The groups related to the Leech Lattice:*

-The Conway groups Co_1, Co_2, Co_3

-The MacLaughlin group MCL

-Suzuki group Suz

-Higman Sims group HS

v) The Fisher groups $Fi_{22}, Fi_{23}, Fi'_{24}$.

vi) The Monster M; baby monster B; Thompson group Th; Hold group Hc; Harada-Norton group HN.

vii) The Pariahs:

- *Janko groups* J_1, J_2, J_3
- *O Nan group ON*
- *Lyon group* L_y
- *Rudavalis group Ru*

Definition 2.1.8. ***Permutation Group***

Given a non- empty set Ω*, the symmetric group on the set* Ω *is the group* S_Ω *of all permutations of* Ω*. If* $|\Omega| = n, S_\Omega$ *is denoted by* S_n*. A permutation group* G *on a set* Ω *is a subgroup of* S_Ω*.*

We may regard the permutation group G on Ω as a permutation group on $\Omega \times \Omega$ defined by $g(\alpha, \beta) = (g\alpha, g\beta), \alpha, \beta \in \Omega, g \in G$. The orbit of G containing the point $\alpha \in \Omega$ is the set $\alpha^g = \{g\alpha : g \in G\}$. The number of orbits of G on $\Omega \times \Omega$ is called the **rank of** G **on** Ω and denoted by rank (G). The pairs (α, α) and (β, α) for distinct points $\alpha, \beta \in \Omega$ lie in different orbits of G on $\Omega \times \Omega$. For $|\Omega| > 1$, rank (G) is at least 2. A permutation group is said to be doubly transitive (or 2- transitive) on Ω if it is transitive on the ordered pairs of distinct points of Ω, which means that for $|\Omega| > 1$, the doubly transitive groups are the permutation groups of rank 2.

Definition 2.1.9. ***Representation***

Given a finite dimensional vector space V over a finite field $\mathbb{F}$, a representation ρ is a homomorphism from G to $GL(V)$ (the group of all linear transformations over V). The dimension of V is called the degree of the representation.

If $\dim(V) = n$ with a basis B, then we can obtain an isomorphism from $GL(V)$ *to* $GL(n, \mathbb{F})$.

In mathematics, the term representation, simply implies structure preserving function. Hence in theory of groups, a representation is a homomorphism. More importantly it is a homomorphism from a group one is trying to study to another that is more concrete and probably easier to understand. The simplest two types of groups are; the group of all permutations of an arbitrary set Ω, and the group of all invertible linear transformations on an arbitrary vector space. The linear transformations and the permutation representations are the most studied in finite groups.

Definition 2.1.10. ***Permutation Representation***

Given a group G and a non empty set Ω, the action of G on Ω gives a homomorphism from G to the group of permutations on Ω called the ***permutation representation*** *of G on Ω.*

Definition 2.1.11. ***Character of Permutation Representation***

Given a group G acting on a non empty set Ω, the character π of the permutation representation of G on Ω is defined by $\pi(g) = |Fix(g)|$, for all $g \in G$.

Definition 2.1.12. ***Block***

Given a transitive permutation group G on a finite set Ω, a block B is a non-empty subset of Ω such that for every $g \in G$, either $g(B) = B$ or $g(B) \cap B = \emptyset$ where $g(B) = \{g(b) : b \in B\}$.

In particular $\emptyset, \Omega$ and all single element subsets of Ω are called the **trivial blocks** .

Definition 2.1.13. ***Primitive Permutation Representation***

Given a group G acting transitively on a finite set Ω, if the only blocks are the trivial blocks, then action is said to be ***primitive*** *. Otherwise the action is* ***imprimitive*** *.*

Any 2 - transitive group is primitive [3]. If G is a transitive permutation group on Ω, then G is primitive if and only if G_α is a maximal subgroup of G for all $\alpha \in \Omega$.

Theorem 2.1.2. ***Cayley's theorem*** *Given a group G of order n, then G is isomorphic to some subgroup of the symmetric group S_n.*

2.2 Basics of Coding Theory

This section, provides the preliminaries of the theory of linear codes. Given $\mathbb{F}_q$ as a finite field of q elements with $q = p^r$ for a prime number p and a natural number r, our study is on binary codes; hence the finite field is $\mathbb{F}_2$. We denote the vector space of n tuples of elements of $\mathbb{F}_q$ by $V = \mathbb{F}_q^n$. Codes provide a structured way to send information, with extra bits such that should an error occur in the transmitted message, it may not only be detected by the receiver, but also corrected.

Definition 2.2.1. ***Linear code***
Let $\mathbb{F}$ be a finite field, then $\mathbb{F}^n$, which is the set of all n - tuples of $\mathbb{F}$ is a vector space over $\mathbb{F}$ for a natural number n. A linear code C of length n is a subspace of $\mathbb{F}^n$.

The elements of code C are called **codewords** and the field $\mathbb{F}$ is called the **alphabet** . C is said to be binary, ternary, quaternary, etc, if the alphabet is of size 2, 3, 4, etc.

Definition 2.2.2. ***Hamming distance***
For vectors $a = (a_1, a_2, \cdots, a_n)$ and $b = (b_1, b_2, \cdots, b_n) \in \mathbb{F}^n$, the Hamming distance is defined by $d(a, b) = |\{i|1 \leq i \leq n, a_i \neq b_i\}|$. That is, the Hamming distance $d(a, b)$ between the vectors a and b, is the number of coordinate places where they differ. The set $\{i|1 \leq i \leq n, a_i \neq 0\}$ is called the ***support of*** *a .*

Definition 2.2.3. ***Weight and Minimum Distance***
For $a \in \mathbb{F}^n$, the weight $w(a)$ of a is defined as $w(a) = d(a, 0)$. In other words the weight of a word is the number of non - zero coordinates that the word has. Clearly this shows that $d(a, b) = w(a - b)$. The minimum weight of a code C is a measure of its error correcting capabilities.The minimum distance d of a code C, is the minimum of all the distances between the codewords. That is, $d = min\{w(a - b)|a, b \in C, a \neq b\}$. For linear codes, the minimum weight is the minimum distance. Given a linear code $C = [n, k, d]_q$, the singleton bound is $d \leq n - k + 1$.

Our interest in this thesis is linear error correcting codes. In view of this, given the length of a linear code and its dimension, from MAGMA, we can find the best known

linear code upper bound (BKLCUpperBound) and best known linear code lower bound (BKLCLowerBound) minimum distance.

Definition 2.2.4. ***Parameters of a code***

A subspace C of $\mathbb{F}^n$ of dimension k is called an $[n,k]$ code over $\mathbb{F}$. Should the minimum distance d of C be known, then C is called an $[n,k,d]$ code and the variables n,k,d are called the ***parameters of the code*** *C .*

Given $G \leq S_n$ as a permutation group, the natural action of the group G on the set $\Omega = \{1, 2, \cdots, n\}$ induces an action on $\mathbb{F}^n$ (hence on any $[n,k]$ code) given by $\sigma(a) = a^\sigma = (a_{\sigma_{(1)}}, a_{\sigma_{(2)}}, \cdots, a_{\sigma_{(n)}})$ where $a = (a_1, a_2, \cdots, a_n)$ and $\sigma \in G$. If C is an $[n,k]$ code, then $\sigma(C) = C^\sigma = \{\sigma(a) | a \in C\}$.

Definition 2.2.5. ***Weight Distribution***

Let $A_i(a)$ denote the number of codewords at distance i from a codeword $a \in C$, an $[n,\ k,\ d]_q$ code. For numbers $0 \leq i \leq n$, the numbers $A_i(a)$ are called the weight distribution of C with respect to a. Clearly $A_0(a) = 1$, $A_i(a) \geq 0$ and $\sum_i A_i(a) = q^k$.

Definition 2.2.6. ***Weight Enumerator***

Let C be a linear $[n,\ k,\ d]_q$ code and let A_k denote the number of codewords of weight k. Let $k_1 < k_2 < \ldots < k_i$ be the hamming weights that occur in C. The weight enumerator of C is the polynomial $\sum_{k=0}^{n} A_k x^{n-k}$. The weight distribution of C is symmetric if $A_k = A_{n-k}, \quad 0 \leq k \leq n$.

Definition 2.2.7. ***Even, Doubly Even Code***

An ***even code*** *has codewords with weght divisible by two while a* ***doubly even code*** *has codewords whose weight is divisible by four.*

Definition 2.2.8. ***Equivalent Codes***

Two [n, k] codes C_1 and C_2 are equivalent if there exists a permutation $\delta \in S_n$ such that $C_1 = {C_2}^\delta$. Equivalent codes have the same parameters and properties, so the classification of codes is up to equivalence.

Definition 2.2.9. ***G - invariant code***

Let $G \leq S_n$ be a permutation group and C be an [n, k] code. Define $G(C) = C^G = \{ a^g | a \in C, \ g \in G\}$. The code C is said to be G – invariant if $C^G = C$.

Definition 2.2.10. ***Automorphism of a code***

Given an $[n, k, d]$ *linear code* C *over* $\mathbb{F}_q$*, any isomorphism of* C *onto itself is called an automorphism of* C *and the set of all automorphisms of* C *denoted by* $Aut(C)$ *is called the automorphism group of* C*.*

$Aut\,(C)$ is a subgroup of S_n if $C \subseteq \mathbb{F}_q^n$ or S_Ω if $C \subseteq \mathbb{F}_q^\Omega$. $Aut\,(C)$ is defined as $Aut\ (C) = \{\delta \in S_n \big| C^\delta = C\}$ *if* $C \subseteq \mathbb{F}_q^n$. This is the set of all permutations which map C to itself and it is a group. The automorphism group of C is a subgroup of S_n and its existence provides a rich structure for the code and permits the use of deeper results from group theory.

Definition 2.2.11. ***Dual of Code*** C

Given an [n, k, d] linear code C, the dual of C denoted by $C^\perp$*, is defined as*
$C^\perp = \{\, a| < a, b > = 0 \ for\ all\ b \in C\ \}$.

In this case we consider C as a vector space endowed with the standard inner product $<,>$, such that given $a = (a_1,\ a_2,\ \ldots,\ a_n)$ *and* $b = (b_1,\ b_2,\ \ldots,\ b_n) \in C$, we have $< a, b > = a_1b_1 + a_2b_2 + \ \ldots\ + a_nb_n$.
The dual $C^\perp$ is an $n - k$ dimensional code.

Proposition 2.2.1. *Let* C *be a code and* $C^\perp$*its dual. Then* $Aut\,(C) = Aut\left(C^\perp\right)$*. An implication of this result is that if a code* C *is* G *- invariant for some permutation group* G*, then* $C^\perp$ *is also* G *– invariant.*

Definition 2.2.12. ***Hull of a code*** C

An intersection of a code and its dual is known as the Hull of the linear code C.

Definition 2.2.13. ***Self Orthogonal Code***

If the code C is contained in its dual, then the code is said to be self orthogonal.

For a self orthogonal [n, k, d] code C, then $k \leq n - k$, *that is* $k \leq \frac{n}{2}$ and C is an even code. If $C = C^\perp$, then the code C is said to be self dual. If C is a self – dual $[n,\ k]$ code, then n is even, the all 1 vector is in C and the distribution of the weights of the codewords in C is symmetric.

Definition 2.2.14. ***Generator Matrix of a code***

Given an [n, k] code C, a $k \times n$ *matrix E whose rows are made up of any k linearly independent vectors of C is called the generator matrix of C.*

Definition 2.2.15. ***Parity Check Matrix***

The generator matrix for the dual code is called the ***parity check*** *matrix for C.*

Definition 2.2.16. ***Projective two weight codes***

An $[n,\ k,\ d]_q$ *code C over* $\mathbb{F}_q$ *is called a projective two weight code if it has only two non – zero weights* w_1 *and* w_2 *and its dual has dimension greater than 3.*

2.3 Design Theory

Codes and designs have many links. Designs turn up in the study of codes and vice versa. This section gives some elementary ideas of design theory that will be used in the sequel. An incidence structure is a triple $(\mathcal{P},\ \mathcal{B},\ \mathcal{I})$ consisting of points $\mathcal{P}$, a collection of blocks $\mathcal{B}$ and an incidence relation $\mathcal{I}\ \subseteq\ \mathcal{P}\ \times\ \mathcal{B}$ between the points and blocks.

Definition 2.3.1. $t-(v,k,\lambda)$***design***

An incidence structure $D=(\mathcal{P},\ \mathcal{B},\ \mathcal{I})$*, with point set* $\mathcal{P}$*, block set* $\mathcal{B}$ *and incidence* $\mathcal{I}$ *is called a* $t-(v,\ k,\ \lambda)$ *design if*

i) $|\mathcal{P}|=v$

ii) Every block $B\ \in\ \mathcal{B}$ *is of cardinality k. that is , every block* $B\ \in\ \mathcal{B}$ *is incident with precisely k points*

iii) Every t distinct points of $\mathcal{P}$ *are contained in exactly* λ *blocks of* $\mathcal{B}$*.*

A $t-(v,k,\lambda)$ design is also referred to as a t – design with the assumption that all the parameters are positive integers and that $t\ \leq k\ <v$ (to avoid trivial cases). Repeated blocks are not allowed, hence members of $\mathcal{B}$ must be different. A design is **symmetric** if it has the same number of points and blocks. A design D is **self dual** if it is isomorphic to its dual.

Theorem 2.3.1. *A t design D is also an s design for* $1\ \leq s\leq t$*. If D has parameters* $t-(v,\ k,\ \lambda)$*, then its parameters as an s design are* $s-(v,\ k,\ \lambda_s)$ *where*

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

Proof: [22, Theorem 3. 2. 2] □

Definition 2.3.2. ***Incidence Matrix of a Design***

Let $D = (\mathcal{P},\ \mathcal{B},\ \mathcal{I})$ *be a* $t-(v,\ k,\ \lambda)$ *design where* $\mathcal{P} = \{p_1,\ p_2,\ \ldots, p_v\}$ *is the point set of the design,* $\mathcal{B} = \{B_1,\ B_2,\ \ldots, B_b\}$ *is the set of blocks of the design and* $\mathcal{I} \subseteq\ \mathcal{P}\ \times \mathcal{B}$. *The incidence matrix of* D *is defined to be the* $v\ \times b$ *matrix*

$A = [a_{ij}]$ *where*

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

A $q-ary$ code of the design $D = (\mathcal{P},\ \mathcal{B},\ \mathcal{I})$ denoted by $C_p(D)$, is the subspace of the function space $\mathbb{F}_q^{\mathcal{P}}$ generated by the characteristic function of the blocks of D. The dimension of the code $C_p(D)$ over a finite field $\mathbb{F}_p$ is the rank of the generating matrix of the code, called the p – rank of D. In general the minimum weight of the code $C_p(D)$ is less than the block size of D.

Lemma 2.3.1. *If* C *is a linear* $[n,\ k]$ *code of an incidence structure* $\mathcal{I}$ *over a finite field* $\mathbb{F}$, *then the automorphism group of* C *is the full symmetric group if and only if* $C =\ \mathbb{F}^n$.

Proof: See[14]. □

A design is trivial if every k set of points is incident with a block and simple if distinct blocks are not incident with the same set of k points. In this thesis all the designs constructed and discussed, are simple and non trivial. The dual structure of D is $D^T\ = \left(\mathcal{B}^T,\ \mathcal{P}^T,\ \mathcal{I}^T\right)$ *where* $\mathcal{B}^T\ =\ \mathcal{P}\ ,\ \mathcal{P}^T\ =\ \mathcal{B}\ ,\ \mathcal{I}^T\ =\ \{\ (B,\ p) : (p,\ B)\ \not\in\in\ \mathcal{I}\}$. The transpose of an incidence matrix for D is an incidence matrix for D^T . The **complement** of D is the structure $\overline{D} = \left(\overline{\mathcal{P}},\ \overline{\mathcal{B}},\ \overline{\mathcal{I}}\right)$ where $\overline{\mathcal{P}} = \mathcal{P}\ ,\ \overline{\mathcal{B}} = \mathcal{B}\ ,\ \overline{\mathcal{I}} = \mathcal{P}\ \times\ \mathcal{B}- \mathcal{I}$. If D is a $t-(v,\ k,\ \lambda)$ design, $t\ \leq v-k$, then $\overline{D}$ is a $t-(v,\ v-k,\ \overline{\lambda}\ )$ where

$$\overline{\lambda} = \lambda \frac{(v-k)(v-k-1)\ldots(v-k-t+1)}{k\ (k-1)\ldots(k-t-1)}\ .$$

Proof: see [22] Theorem 1.3.1 □

Definition 2.3.3. ***Automorphism of a design***

An automorphism of a design $D = (\mathcal{P},\ \mathcal{B},\ \mathcal{I})$ *is a permutation* ϑ *of* $\mathcal{P}$ *such that for* $B\ \in\ \mathcal{B}$, $\vartheta(\mathcal{B}) \in\ \mathcal{B}$. *The automorphisms of D form a group under composition which acts*

on $\mathcal{P}$. Since the automorphisms takes blocks to blocks, the group also has a permutation representation on the set $\mathcal{B}$.

Theorem 2.3.2. *Let C be a $[n,\ k]$ code of a symmetric $1-(v,\ k,\ k)$ design D over a finite field $\mathbb{F}_q$, then the automorphism group of the design is contained in the automorphism group of the code.*

Proof. See [23]
Suppose G is a finite group acting t – transitively on a finite set. We can construct a $t-(v,\ k,\ \lambda)$ design using theorem 2.3.3. □

Theorem 2.3.3. *Let G be a group acting t – transitively on a set Ω of size n and let B be the k – subset of Ω with $1\ <k\ <n-1$. then the set $\mathcal{B}=\{\ B^g\ :g\ \in G\}$ is the set of blocks of a $t-(v,\ k,\ \lambda)$ design with $|G\ :\ G_B|$ blocks. Furthermore G is a group automorphism of the design acting transitively on $\mathcal{B}$.*

Proof: Consider S and S' as t – subsets of Ω. There exists a $g\in G$ such that $S'=S^g$. If B is a block containing S, then B^g will be a block containing S'. Thus g is a bijection between the set of blocks containing S and the set of blocks containing S'. This means any t points will belong to the same number of blocks λ. The number of blocks of the design is the size of the orbit B^g which is $|G:G_B|$. □

Definition 2.3.4. ***Balanced Incomplete Block Design (BIBD)***
A balanced incomplete block design (BIBD) is a pair $(\Omega,\ \mathcal{B})$ where $|\Omega|=v$, and $\mathcal{B}$ is a collection of $b\ \ k-$ subsets of Ω (blocks) such that each element of Ω is contained in exactly r blocks and any two subsets of Ω is contained in exactly $\lambda\ \ $ blocks.

The numbers $v,\ b,\ r,k,\ \lambda$ are the parameters of the BIBD. The trivial and necessary conditions for the existence of a $v,\ b,\ r,k,\ \lambda$ BIBD are $vr\ =\ bk$ *and* $r\ \ (k-1)\ =\ \lambda\ \ (v-1)$.$v,\ k$ *and* λ determine b and r, hence a $(v,\ k,\ \lambda)$ design.

Lemma 2.3.2. ***Fischers Inequality***
If a $v,\ b,\ r,k,\ \lambda$ BIBD exists with $2\ \leq k\ \leq v,\ \ $ then $b\ \geq v$.

The existence question for BIBD's with small k is such that given k *and* λ, for what values of v does the above conditions and Fischer's inequality hold?
The problem has been addressed for all λ when $k \leq 9$. For $k \geq 10$, much less is known.

Definition 2.3.5. ***Steiner System***
A $t-(v,\ k,\ 1)$ *design is called a Steiner system customarily denoted by* $S(t,\ k,\ v)$.

The concept of a code being a vector space leads to a description of codes as spaces spanned by some $q-ary$ vectors, where $\mathbb{F} = \mathbb{F}_q$, is the base field over which the vector space is defined. In such circumstances, one may consider codes as subspaces of vector spaces spanned by sets. Often such considerations arise in the study of codes obtained from combinatorial designs. Similarly, given a code, we can establish a design generated by that code and prove whether it exists or not. In this thesis we are concerned mostly with symmetric $1-(v,\ k,\ k)$ designs and other $1-(v,\ k,\ \lambda)$ designs. In chapter 3, two methods of constructing such designs are given. In both methods, the 1- designs result from the primitive permutation representations of the simple group $G = S_8(2)$.

2.4 Representation and Module Theory

In this section we show how G – invariant linear codes can be viewed as $\mathbb{F}G$ modules. The concept of modules is a generalization of the notion of vector spaces over arbitrary rings. If $\mathbb{F}$ is a field and G is a finite group, the study of $\mathbb{F}G$ – modules is key in the study of linear codes.

2.4.1 Representation of modules

Definition 2.4.1. ***Right R – module***
Let R be a ring. Then G_R *is a right R – module if G is an abelian group additively and there exists a map* $\theta : G \times R \to G,\ \ \theta((g,r)) = gr,\ \ g \in G$ *and* $r \in R$ *satisfying*

i) $(g_1 + g_2)r = g_1r + g_2r$

ii) $g(r+s) = gr + gs$

iii) $g(rs) = (gr)s$

iv) $ge = g$ where e is the identity in G

Definition 2.4.2. ***Group Homomorphism*** .

Let G be a finite group and let $\mathbb{F}$ be a commutative ring of coefficients. A representation of G over $\mathbb{F}$ is a group homomorphism $G \rightarrow GL(n, \mathbb{F})$ for some n.

Definition 2.4.3. ***Faithful Representation***

A representation $\rho : G \rightarrow GL(V)$ is called faithful if $\ker(\rho) = \{e_g\}$. This representation is normally referred to as F – representation of G on V.

Definition 2.4.4. ***FG - Group Algebra*** .

The $\mathbb{F}G$ - group algebra comprises linear combinations of elements of G with coefficients in $\mathbb{F}$. Addition and multiplication in the FG algebra are defined as follows:-

$$\left(\sum_{g\in G} \alpha_g g\right) + \left(\sum_{g\ \in G} \beta_g g\right) = \sum_{g\ \in G} (\alpha_g + \beta_g)\, g \tag{2.1}$$

$$\left(\sum_{g\in G} \alpha_g g\right) . \left(\sum_{g\in G} \beta_g g\right) = \sum_{g\in G} \left(\sum_{hh'=g} \alpha_h \beta'_h\right) g \tag{2.2}$$

$\mathbb{F}G$is a ring and also an $\mathbb{F}$ algebra.

2.4.2 Link between codes and $\mathbb{F}G-$ modules

Given a permutation group G, a finite set Ω and a finite field $\mathbb{F}$, it is of great significance to study the structure of the permutation module $\mathbb{F}\Omega$. The G-invariant sub modules of $\mathbb{F}\Omega$ can be considered as linear codes in $\mathbb{F}\Omega$ and one may therefore enumerate and characterize these codes. Nevertheless, when considering large groups, the chance of finding all the codes invariant under the group diminishes due to the large degree of their representation and the large dimension of the sub modules of the permutation module associated with the given permutation representation. Hence one may be satisfied with minimal representations, or at least with the degree of the smallest irreducible (and hence faithful) representation. Given a representation $\vartheta : G \rightarrow GL\ (n,\ \mathbb{F})$, $V = \mathbb{F}^n$ is converted into an $\mathbb{F}G$ – module by:-

$$\left(\sum_{g\ \in G} \alpha_g\ g\right).\ v\ =\ \sum_{g\ \in G} \alpha_g\ g\vartheta\left(g\right)\left(v\right),\quad v\ \in V \tag{2.3}$$

From the definition of linear codes as subspaces of $\mathbb{F}^n$ for a finite field $\mathbb{F}$, it follows that linear codes are simply $\mathbb{F}G-$ submodules.
Hence for any permutation group G, the G – invariant codes are exactly the $\mathbb{F}G-$ submodules of $\mathbb{F}^n$. For a field $\mathbb{F}$, the representations of G correspond to the finite dimensional $\mathbb{F}G-$ modules. In [10], applying the modular representation theoretic method on the primitive permutation representation of degree 98280 of the simple group Co_1 of Conway, the irreducible faithful representation of dimension 24 was obtained as a binary code. A summary of the results is given in the following theorem.

Theorem 2.4.1. *Let G be a simple Conway group Co_1 and C_{24} be a sub module of dimension 24 obtained from the permutation module of degree 98280. Then the following hold:*

i) C_{24} is the smallest non – trivial Co_1 – invariant irreducible $\mathbb{F}_2$ – module

ii) C_{24} is a self – orthogonal doubly – even two – weight code

iii) the supports of the minimum words define uniquely a self-dual, point – primitive and flag – transitive symmetric 1 – (98280, 47104, 47104) design invariant under Co_1.

iv) $Aut\ (C_{24})\ \cong\ Co_1$

v) The non – trivial codewords of C_{24} define a strongly regular (16777216, 98280, 4600, 552) graph $\Gamma\left(C_{24}\right)$ [24].

It was also established that $C_{24}^{\perp}$, the dual code of C_{24} is a uniformly packed $[98280,\ 98256,\ 3]$ binary code, and that the stabilizer of the codewords of minimum weight in the dual code is a maximal subgroup of Co_1. The link between linear codes and $\mathbb{F}G-$ modules is very important in the sequel.

2.5 Finite Geometries

Given a vector space V over a finite field $\mathbb{F}$ and let $PG(V)$ denote the projective geometry defined by V. Given that V is of dimension n over $\mathbb{F}$, then the projective geometry PG(V) is an $n-1$ projective dimensional space. PG(V) is also abbreviated by $PG_{n-1}(\mathbb{F})$, whose elements are the non – trivial subspaces of V. Hence the points of PG(V) are the 1 – dimension subspaces of V, the lines are the 2 – dimension subspaces of V and the hyper planes are the $n-1$ dimension subspaces of V. If $\mathbb{F} = \mathbb{F}_q$, a point of the projective geometry $PG_{n-1}(\mathbb{F}_q)$ is given in homogeneous coordinates by the non – zero vector $(y_1,\ y_2,\ \ldots, y_n) \in {\mathbb{F}_q}^n$. The number of points in the projective plane $PG_{n-1}(\mathbb{F}_q)$ is $\frac{q^n-1}{q-1}$. The number of m – 1 dimension subspaces of $PG_{n-1}(\mathbb{F}_q)$ is given by

$$\frac{(q^n-1)(q^n-q)\ldots(q^n-q^{m-1})}{(q^m-1)(q^m-q)\ldots(q^m-q^{m-1})}. \tag{2.4}$$

To generate a design from $PG_{n-1}(\mathbb{F}_q)$ where $n \geq 3$, we take the set of points of the plane as the design's point set. The blocks of the design are all subspaces of the same fixed dimension. Suppose the block set is the set of all s – dimension subspaces of $PG_{n-1}(\mathbb{F}_q)$. Then the design is denoted by $PG_{n-1,\ s}(\mathbb{F}_q)$. The 2 – transitivity of the projective groups on points assures that we are dealing with 2 - designs. Thus the designs of points and planes can be considered, designs of the points and lines and the designs of points and hyper planes of a geometry and be guaranteed of a 2 - design. Since the structure of the design is dependent on both the dimension of the plane and the number of elements of the finite field, by fixing any one of these, we can obtain several infinite classes of designs. A $PG_{n-1,\ r}(\mathbb{F}_q)$ projective geometry is a $2-(v,\ k,\ \lambda)$ design with

$$v = \frac{q^n-1}{q-1},\quad k = \frac{q^{r+1}-1}{q-1},\quad \lambda = \frac{(q^{n-2}-1)\ldots(q^{n-r}-1)}{(q^{r-1}-1)\ldots(q-1)} \qquad [5].$$

The codes over $\mathbb{F}_q$ of any of the designs defined by a projective geometry over a field of characteristic p, where $q = p^t$ are some of the generalized Reed – Muller codes.

Remark 2.5.1. *In the projective dimensional space, any point is of zero - dimension, any line is of 1 - dimension and a plane is of 2 - dimension. A projective plane of order u satisfies the following conditions:*

i) The plane has u^2+u+1 points and u^2+u+1 lines

ii) Distinct points determine a unique line and distinct lines intersect in a unique point.

iii) Every line contains exactly $u+1$ points and every point is exactly on $u+1$ lines.

Given a set of points and lines, it is a finite projective plane if and only if it is a $2-(v,\ k,\ 1)$ symmetric design with $v\ \geq 4$. A projective plane of order u is a $S(2,\ u+1,\ u^2+u+1)$ Steiner system. That is, $2-(\ \ u^2+u+1, u+1,\ 1)$ design.

Most designs occur as the supports of codewords associated with a given weight in the code. Given the number of blocks as b and $b=v$, then the t- design is symmetric of order $k-\ \lambda$. The symmetric $2-(v,\ k,\ 1)$ design is a projective plane of order $k-1$.

2.6 Graphs

The terminology used on our graphs in the write up is standard and the graphs considered are undirected.
Graph theory is mainly concerned about general relations on a set. A graph $\Gamma\ (V,\ E)$ comprises a finite set of vertices V together with a set E of edges. An edge is an unordered pair (u, v) representing a line from vertex u to vertex v.

Definition 2.6.1. ***Valency***
The valency of a vertex is the number of edges adjacent with the vertex.

Definition 2.6.2. ***Girth***
The girth in a graph is the length of the smallest cycle (circuit) in the graph.

Definition 2.6.3. ***Diameter***
This is the length of the longest path in a graph.

Definition 2.6.4. ***Regular graph***
A graph is regular if all the vertices have the same valency. A regular graph is ***strongly regular*** *of type $(n,\ k,\ \lambda,\ \mu)$ if it has n vertices, valency k, and if any two adjacent vertices are together adjacent to λ verices, while any two non – adjacent vertices are together adjacent to μ vertices.*

The complement of a strongly regular graph with parameters $(n,\ k,\ \lambda,\ \mu)$ is also a strongly regular graph with parameters $(v,\ v-k-1,\ v-2k+\ \mu-2,\ v-2k+\ \lambda)$ [7]. Calderbank and Kantor in [5] proved the equivalence of two weight projective codes and strongly regular graphs. They defined a construction of the strongly regular graph from a two projective weight code. They determined the graphs parameters from the parameters of the code. In this construction, the points of the vector space space of dimension k, ${\mathbb{F}_q}^k$ is taken as the set of vertices.

Theorem 2.6.1. *([5] Theorem 2)*
Let w_1 and w_2 ($w_1 <\ w_2$) be 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 $v =\ q^k$ codewords and two vertices corresponding to a and b are adjacent if and only if $d\,(a,\ b) =\ w_1$. Then $\Gamma\ (C)$ is a strongly regular graph. From a projective two weight $[n,k]$code C, we obtain a strongly regular graph $\Gamma(C)$ with parameters $(N,\ K,\ \lambda,\ \mu)$ such that $N =\ q^k$, $K = n\,(q-1)\,, \lambda =\ K^2+\ 3K-q\,(w_1+\ w_2)-kq\,(w_1+\ w_2)+\ q^2w_1w_2$ and $\mu =\ \frac{q^2w_1w_2}{q^k}$. If $C^{\perp}$ is the projective dual of the projective two weight code C, the graphs $\Gamma(C)$ and $\Gamma(C^{\perp})$ are isomorphic. Hence for projective self- dual codes, the constructions lead to isomorphic graphs.

Chapter 3

Codes and Designs from finite simple groups

This chapter provides the techniques that are used throughout this thesis to construct linear codes from the finite group $G = S_8(2)$ of order $2^{16}.3^5.5^2.7.17$. In section 3.1 we show how G – invariant linear codes can be viewed as irreducible FG - submodules. This approach is advantageous in that it provides an explicit basis of the code unlike most other methods. However, the method meets apparent computational and algebraic limitations when the permutation module has a considerably large dimension. Section 3.2 provides the techniques that are used to construct 1 – designs and regular connected graphs from the primitive actions of finite groups. From the 1 - designs, we get the associated codes. The algorithms involved are implemented using the MAGMA software package. This method is applicable to any simple group and for some considerably high dimensional permutation representations.

3.1 FG - Modules and G - Invariant codes

Our interest is to find all the G - invariant codes from the primitive permutation representations. In so doing we consider the permutation module obtained from the coset action of its maximal submodules. Given a permutation group G acting on a set Ω, over a finite field $\mathbb{F}$, the vector space over $\mathbb{F}$ with basis Ω is considered as an $\mathbb{F}G$ - module. The G - invariant submodules of $\mathbb{F}\Omega$ are the linear codes in $\mathbb{F}\Omega$. This approach provides the determination of all binary codes invariant under a given group G more directly since we obtain an explicit basis of the code. For every primitive representation of the given permutation group G, we have developed a series of computer programs in MAGMA to search for modules under the group and also used the recursive searches in MEAT-AXE to help determine the irreducibility of the module, subsequently obtaining a chain of maximal submodules which constitute the binary codes invariant under G. An in-depth use

of the database of irreducible faithful representations available in MAGMA and Wilson's webpage together with the Brauer character tables and the ATLAS of finite groups is widely used. Once the isomorphic copies are eliminated, a lattice of submodules is obtained. This in a way answers to the problem of enumeration and classification mentioned earlier.

Provided a representation $\vartheta : G \rightarrow GL(n, \mathbb{F})$, $V = \mathbb{F}^n$ is made into an $\mathbb{F}G$ – module by

$$\left(\sum_{g \in G} \alpha_g \, g \right) . \, v = \sum_{g \in G} \alpha_g \, g\vartheta(g)(v), \quad v \in V$$

By the definition of linear codes as subspaces of $\mathbb{F}^n$ for a finite field $\mathbb{F}$, it follows that linear codes are simply $\mathbb{F}G-$ submodules. Hence for any permutation group G, the G – invariant codes are exactly the $\mathbb{F}G-$ submodules of $\mathbb{F}^n$. For a field $\mathbb{F}$, the representations of G correspond to the finite dimensional $\mathbb{F}G-$ modules.

Lemma 3.1.1. [9, 11] *Given a finite group G and Ω a finite G - set, the FG - submodules of $\mathbb{F}\Omega$ are the G – invariant codes. That is, the G – invariant subspaces of $\mathbb{F}\Omega$.*

In this thesis, we have used Lemma 3.1.1 to construct codes and associated combinatorial structures for representations of degree 120, 136 and 255 (see chapter 4, 5 and 6 respectfully).

3.2 Designs and Graphs from Primitive groups

We consider the action of the primitive permutation group G on a finite set Ω of size n. This method is applicable to any simple group and any representation to obtain a symmetric 1 - design and the respective regular connected graph. From the design, we hence determine the associated linear code. Any t - design is a 1 - design. The converse is not always true. However some of the designs constructed this way are 2 - designs. Theorem 3.2.1 stated below, described by Key and Moori in [18] and later corrected in [30] gives an algorithm for construction of symmetric 1 - designs and regular connected graphs. See also [31]

Theorem 3.2.1. [18] *Let G be a finite primitive permutation group acting on a set Ω of size n. Let $\alpha \in \Omega$, and let $\Delta \neq \{\alpha\}$ be an orbit of G_α, the stabilizer of α. If $\mathcal{B} = \{ \Delta^g : g \in G\}$, and given $\delta \in \Delta$, $\mathcal{E} = \{ \{\alpha, \delta\}^g : g \in G\}$, then $D = (\Omega, \mathcal{B})$ is a self - dual $1 - (n, |\Delta|, |\Delta|)$ design and $\mathcal{E}$ forms the edge set of a regular connected graph of valency $|\Delta|$ with G acting as an automorphism group on each of these structures, primitive on points and blocks of the design.*

Proof: The order of G, $|G| = |\Delta^G||G_\alpha|$, clearly $G_\alpha \subseteq G_\Delta$. Since G is primitive on Ω, G_α is maximal in G. Hence $G_\alpha = G_\Delta$ and $|\Delta^G| = |B| = n$. This proves that we have a $1 - (n, |\Delta|, |\Delta|)$ design. For the graph the vertices adjacent to α are the vertices in Δ. As we orbit these pairs under G, we obtain nk ordered pairs and thus $\frac{nk}{2}$ edges, where $k = \Delta$. The graph is regular since it has G acting and its valency is k. that is, the only vertices incident to α are those contained in the orbit of Δ. The graphs's adjacency matrix is an incidence matrix for the 1 - design, so that the 1 - design is self dual. □

In Theorem 3.2.1, if Δ is the combination of some orbits of the stabilizer that includes the orbit of size 1, and $\mathcal{B} = \{\Delta^g : g \in G\}$, then $D = (\Omega, \mathcal{B})$ is a symmetric $1 - (n, |\Delta|, |\Delta|$ design whose automorphism group is G, primitive on points and blocks of the design. Also, the blocks of any symmetric 1- designs with an automorphism group G acting primitively on points can be constructed as a union of orbits of the G stabilizer.

Lemma 3.2.1. *i) Given $\mathcal{D}$ as a self dual symmetric 1 - design obtained by taking every image under G of all non trivial orbit Δ of the point stabilizer in any of the primitive representations of G, and on which G acts primitively on points and blocks, then the automorphism group of $\mathcal{D}$ contains G.*

ii) If C is a linear code of length n of a symmetric self dual $1 - (n, |\Delta|, |\Delta|)$ design $\mathcal{D}$ over a finite field $\mathbb{F}_q$, then the automorphism group of C contains the automorphism group of $\mathcal{D}$.

We applied the method described by Key and Moori (Theorem 3.2.1) to each of the primitive representations of degree 2295, 5355, 5440 and 11475 to construct the 1 - designs and the respective connected graphs. Computationally, it was not possible to work with primitive representations of higher degrees.

Let G be a finite primitive permutation group acting on a set Ω of cardinality n with $\alpha \in \Omega$ and $\Delta \neq \{\alpha\}$ as an orbit of the stabilizer G_α of α, then images of these orbits under the action of G form the blocks of a self - dual symmetric 1 - design. The point stabilizer is maximal in G, therefore there is only a single orbit of length 1. For suppose G is a simple group and suppose that G_α also fixes x. Then $G_\alpha = G_x$. With the transitivity of G, there exists $g \in G$, such that $\alpha^g = x$. Then $(G_\alpha^g) = G_{\alpha g} = G_x = G_\alpha$. Thus $g \in M_G(G_\alpha) = M$, the normalizer of G_α in G. Since G_α is maximal in G, $M = G$ or $M = G_\alpha$. But G is simple, so $M = G_\alpha$, so that $g \in G_\alpha$ and so $x = \alpha$

The 1 - designs by their parameters do not give any suggestion of what primes may produce meaningful codes, however we concentrate on $p = 2$ to generate binary codes. However, from the order of the group G, we can get q - ary codes invariant under G in F_q where q is a prime divisor of $|G|$.

We chose to find binary codes since most computer processor instructions and any data transmission and storage schemes use a two symbol system.

Chapter 7 of this thesis gives detailed results of the symmetric self - dual 1 - designs of the 2295, 5355, 5440 and 11475 permutation representations.

Chapter 4

The Primitive Representations of the group $G = S_8(2)$

In this chapter using the first method discussed in the previous chapter, we will construct some codes from the projective symplectic group $S_8(2)$ and generate the associated designs. The first section briefly describes the projective symplectic group of order n.

4.1 The projective Symplectic Groups

The linear, unitary, symplectic and orthogonal groups generalize the familiar classical groups, whose description involves immense use of the properties of finite fields. The general linear group $GL_n(q)$ comprises all the invertible $n \times n$ matrices with entries in $\mathbb{F}_q$. $GL_n(q)$ is the group of all linear automorphisms of an n - dimensional vector space over $\mathbb{F}_q$. The subgroup of all $n \times n$ matrices with determinant 1 is called the special linear group denoted by $SL_n(q)$.
The projective symplectic group $PSp_{2n}(q)$ is the factor group $Sp_{2n}(q)/Z(Sp_{2n}(q))$. The projective symplectic groups are simple except for $PSp_2(2) \cong PSL_2(2)$, $PSp_2(3) \cong PSL_2(3)$ and $PSp_4(2)$ [11, 2]. The order of $PSp_{2n}(q)$ is

$$|PSp_{2n}(q)| = \frac{1}{(2,\ q-1)} \cdot |Sp_{2n}(q)| = \frac{q^{n^2}}{(2,\ q-1)} \prod_{j=1}^{n} (q^{2j}-1)[11]. \qquad (4.1)$$

If P is a point of the projective space $PG(2n-1,\ \mathbb{F}_q)$, then the affine subgroup of $G = PSp_{2n}(q)$ is the stabilizer G_p of the form $M : PSp_{2n-2}(q)$, a split extension where M is a p group of order q^{2n-1} [11]. If $q = p^s$ where p is an odd prime, M is a non- abelian special p- group of order q^{2n-1}. If p = 2, then M is an abelian 2 – group.

The $PSp_{2n}(q)$, $n \geq 2$, $q = p^s, p\ prime$, $s \in \mathbb{N}$ acts as a primitive rank 3 group of degree $\frac{q^{2n}-1}{q-1}$ on the points of the projective space $PG(2n-1,\ \mathbb{F}_q)$. The orbits of the stabilizer of a point r consist of $\{r\}$, of length 1, one of length $\frac{q^{2n-1}-1}{q-1} - 1$ and the other of length q^{2n-1}. The symplectic groups defined over $\mathbb{F}_2$ have two different actions which

are 2 – transitive. For more classical background on the symplectic forms and symplectic groups, see [15, 16, 17, 18]. For $n \geq 2$, the group $S_{2n}(q)$ acts 2- transitively on $\Omega^{\pm}$. In these actions, we have

i) The point stabilizer is the group $GO_{2n}{}^{\pm}(2)$ with $\left|S_{2n}(2) : GO_{2n}{}^{\pm}2\right| = 2^{n-1}(2^n \pm 1)$

ii) The two point stabilizer is $2^{2n-2} : GO_{2n}{}^{\pm}(2)$.

Given V as a vector space over a finite field $\mathbb{F}_q$, a function $f(x, y)$ defined $\forall \ x, \ y \in V$ and taking values in $\mathbb{F}_q$ which satisfies:

i) $f(\alpha_1 A + \alpha_2 B, \ y) = \alpha_1 f(A, y) + \alpha_2 f(B, y)$

ii) $f(B, \ A) = -f(A, \ B)$

iii) $f(A, A) = 0$

is called a skew symmetric, bilinear and non degenerate form or symplectic form. The kernel of such a form is the subspace of V such that $f(A, B) = 0 \ \forall \ B$. The nullity and rank of f are the dimension and codimension of its kernel. A form is called nonsingular if its nullity is zero. The rank of a symplectic form is necessarily an even number. For an even number the symplectic group $Sp_{2n}(q)$ is defined as the group of all elements of $GL_n(q)$ that preserve a nonsingular form $f(A, B)$. Any such matrix has determinant 1 so that the general and the special symplectic groups coincide.

Let

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

The symplectic group of rank n over $\mathbb{F}$ is defined to be; $Sp_m(q) = \{g \in M_{2n}(F) \ : \ g^t J g = J\}$. It is evident that $Sp_{2n}(q)$ is a subgroup of $GL_{2n}(q)$. If the bilinear form is skew symmetric and non-degenerate, then dim$V$ must be even, since the matrix of the bilinear form relative to any basis of V is skew symmetric and has a non-zero determinant.

Given that m = 2n, the projective symplectic group of order m in a finite field $\mathbb{F}_q$ is denoted by $S_m(q)$, which is the standard ATLAS notation. This is the notation used throughout this thesis.

4.2 The group $\mathbf{S}_8(2)$

Let G be the projective symplectic group $S_8(2)$. The order of G is 47377612800 = $2^{16}.3^5.5^2.7.17$. Using the ATLAS, G has 11 distinct primitive representations of degree 120, 136, 255, 2295, 5355, 5440, 11475, 13056, 24192, 45696 and 19353600. G is isomorphic to the orthogonal $O_9(2)$, a group of all 9 $\times$ 9 matrices over $\mathbb{F}_2$ and the Chevalley group $B_4[8]$. G is a maximal subgroup of the Fisher group Fi_{23}. G acts naturally on the points of the projective geometry $PG(7,\ 2)$. The number of points in the projective space $(n-1,\ q)$ is $\frac{q^n\ -\ 1}{q-1}$. Hence $PG(7,2)$ has 255 points. The number of $(m-1)$ dimensional subspaces of $PG(n-1,\ q)$ is

$$\frac{(q^n-\ 1)(q^n-\ q)\dots(q^n-\ q^{m-1}\ )}{(q^m-1)(q^m-q)\dots(q^m-\ q^{m-1})}. \tag{4.2}$$

Hence $PG(7,2)$ has 10, 795 lines since the lines are 1 dimensional in the projective plane. The representations and orbit lengths are shown in Table 4.1. Column one gives the maximal subgroups as given by the ATLAS [8], column two gives the degree i.e, the number of cosets of the point stabilizer, column three gives the number of orbits and column four gives the size of the orbits of the point stabilizer.

Due to computational limitations, only up to the 7^{th} representation as presented in MAGMA was considered.

Maximal subgroups	Degree	Number	Orbits
$\mathrm{O}_8^-(2)$: 2	120	2	1,119
$\mathrm{O}_8^+(2)$: 2	136	2	1,135
$2^7 : S_6(2)$	255	3	1,126,128
$2^{10} : A_8$	2295	5	1,30,280,960,1024
$2^{3+8} : (S_3 \times S_6)$	5355	6	1,90,96,240,2048,2880
$\mathrm{S}_3 \times S_6$ (2)	5440	5	1,189,336,1890,3024
$2^{6+6} : (S_3 \times L_3(2))$	11475	7	1,42,56,896,1008,4096,5376

Table 4.1: Maximal subgroups of $S_8(2)$ of degree $\leq$ 11475

4.3 The representation of degree 120

From Table 4.1, G acts two transitively on the cosets of ${O_8}^-(2) : 2$ with orbits of length 1 and 119 respectively, from which we obtain a permutation representation of degree 120. Using this action, we form a permutation module of dimension 120 invariant under G. From the ATLAS, the elements being permuted by G are copies of ${O^-}_8(2)$. The permutation module breaks into 4 absolutely irreducible components of dimensions 1, 8, 26 and 48 with multiplicities 4, 2, 2, 1 respectively. There is only one irreducible submodule of dimension 1. The permutation module has only one maximal submodule of dimension 119. The 119 – dimension module, breaks into one maximal submodule of dimension 111. The 111 – dimension module, breaks into one maximal submodule of dimension 85. The 85- dimension module, breaks into one maximal submodule of dimension 84. The 84 - dimension module breaks into one maximal submodule of dimension 36. The 36 - dimension module breaks into one maximal submodule of dimension 35. The 35 – dimension module breaks into one maximal submodule of dimension 9. The 9 – dimension module breaks into one irreducible maximal submodule of dimension 1. Hence the permutation module has submodules of dimensions 119, 111, 85, 84, 36, 35, 9 and 1.

For any permutation representations of degree n, we denote the constructed codes by $C_{n,\,1}$, $C_{n,\,2}$, ... , $C_{n,\,r}$ if r codes are obtained and by C_n if we only have one code up to isomorphism. Therefore we obtain 6 non-trivial codes of dimensions 9, 35, 36, 84, 85 and 111. The lattice of the sub modules is shown in Figure 4.1.

Taking G to be a permutation group of degree n and $V = \mathbb{F}\Omega$ the corresponding $\mathbb{F}_q$ permutation module, the sub modules of V can be regarded as q - ary linear codes in V, and it is significant we find the weight distribution of the codes. From the above we got 6 non- trivial codes $C_{120,1}, C_{120,2}, \cdots, C_{120,6}$ from the permutation representations of

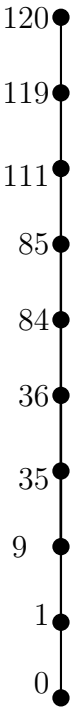

Figure 4.1: 120 Lattice diagram

degree 120. Their respective parameters are listed in Table 4.2. Let the hull of $C_{n,r}$ be denoted by $H_{n,r}$. The weight distribution of the codes $C_{120,1}, C_{120,2}$ and $C_{120,3}$ obtained using MAGMA are shown below:

Weight Distribution for $\mathbf{C}_{120,1}$

$[< 0, 1 >, < 56, 255 >, < 64, 255 >, < 120, 1 >]$

Weight Distribution for $\mathbf{C}_{120,2}$

$[< 0, 1 >, < 24, 5355 >,$

$< 28, 16320 >, < 32, 16065 >,$

$< 36, 3089920 >, < 40, 14676984 >,$

$< 44, 289255680 >, < 48, 1794267720 >,$

$< 52, 7041968640 >, < 56, 14999707155 >,$

$< 60, 20433469056 >, < 64, 14999707155 >,$

$< 68, 7041968640 >, < 72, 1794267720 >,$

$< 76, 289255680 >, < 80, 14676984 >,$

$< 84, 3089920 >, < 88, 16065 >,$

$< 92, 16320 >, < 96, 5355 >,$

$< 120, 1 >]$

Weight Distribution for $\mathbf{C}_{120,3}$

$[< 0, 1 >, < 24, 5355 >,$

$< 32, 16065 >, < 36, 1370880 >,$

$< 40, 8096760 >, < 44, 145313280 >,$

$< 48, 884003400 >, < 52, 3566142720 >,$

$< 56, 7413648915 >, < 60, 10322543616 >,$

$< 64, 7413648915 >, < 68, 3566142720 >,$

$< 72, 884003400 >, < 76, 145313280 >,$

$< 80, 8096760 >, < 84, 1370880 >,$

$< 88, 16065 >, < 96, 5355 >,$

$< 120, 1 >]$

For more weight distributions for the codes and their duals for this representation, see the appendix.

Code $C_{n,r}$	Parameters	Dual $C_{n,r}^{\perp}$	Hull $C_{n,r}$	Aut($C_{n,r}$)
$C_{120,1}$	[120, 9, 56]	[120, 111, 4]	[120, 9, 56]	$S_8(2)$
$C_{120,2}$	[120, 35, 24]	[120, 85, 8]	[120, 35, 24]	$S_8(2)$
$C_{120,3}$	[120, 36, 24]	[120, 84, 8]	[120, 36, 24]	$S_8(2)$
$C_{120,4}$	[120, 84, 8]	[120, 36, 24]	[120, 36, 24]	$S_8(2)$
$C_{120,5}$	[120, 85, 8]	[120, 35, 24]	[120, 35, 24]	$S_8(2)$
$C_{120,6}$	[120, 111, 4]	[120, 9, 56]	[120, 9, 56]	$S_8(2)$

Table 4.2: The parameters of the non - trivial codes

Proposition 4.3.1. *Let G be a permutation module of degree 120, the set $M = \{1, 2, 3\}$ and the set $N = \{4, 5, 6\}$. Then the following hold:*

i) For $r \in M, C_{n,r}$ is a self-orthogonal, doubly even code.

ii) For $r \in N, C_{n,r}$ is an even code.

iii) All the non - trivial codes are projective

Proof:

i) From the weight distribution for these three codes shown above, the containment is clearly seen.

ii) The dimension of $H_{n,r}$ is equal to the dimension of the code $C_{n,r}$. This implies that $C_{n,r} \subset C^{\perp}$, thus $C_{n,r}$ is self orthogonal.
The weight of every codeword in $C_{n,r}$ for $r \in M$ is divisible by 4, thus $C_{n,r}$ for $r \in M$ is doubly even.

iii) The weight of every codeword in $C_{n,r}$ for $r \in N$ is divisible by 2, thus $C_{n,r}$ for $r \in N$ is even.

iv) All the dual codes have weight greater than 3 and thus the codes are projective. □

Proposition 4.3.2. *The codes $C_{120,1}$ and $C_{120,6}$ are optimal codes.*

Proof:

The optimality of the codes $C_{120,1}$ and $C_{120,6}$ is given by MAGMA and also from Grassl online tables [19]. □

Remark 4.3.1. *Optimal codes are instantaneous codes with minimum word length and sufficiently long enough to allow effective decoding and at the same time are economical. That is, the minimum weight of the code attains the theoretical upper bound on the minimum.*

Remark 4.3.2. *The code $C_{120,1}$ has 255 codewords with minimum weight. The action of $G = S_8(2)$ on the 255 points of the projective space $PG(7,2)$ yields a point stabilizer isomorphic to the group $2^7 : S_6(2)$ which is maximal in G. Hence the action of G on the*

cosets of $2^7 : S_6(2)$ *is primitive and of index 255. Therefore, the number of codewords with minimum weight represent the points of the projective space PG (7, 2) and also the index of the coset action, that is* $[G : 2^7 : S_6(2)] = 255$.

From MAGMA, the code $C_{120,1}$ *is also a quasi cyclic linear code of degree 8. The group action of* $G = S_8(2)$ *on* $O_8^-(2)$*, or the orthogonal elliptic form of order 8 gives a point stabilizer* $O_8^-(2) : 2$ *which is maximal in G.*

Proposition 4.3.3. *The codes* $C_{120,2}, C_{120,3}, C_{120,4}$ *and* $C_{120,5}$ *are new best known linear codes.*

Proof: For example, $C_{120,2}$ is a [120,35,24] linear code. The BKLCUpperBound is 56 and the BKLCLowerBound is 40. Since the code $C_{120,2}$ has minimum distance 24, outside the bounds, we conclude that it is a new code of length 120 and dimension 35. Table 4.3 shows the bounds for the other codes. □

Remark 4.3.3. *Given an [n, k, d] linear code , it is said to be a best known linear code if it has the highest minimum weight among all the known [n, k] codes.*

Code	Parameters	BKLCUpperBound	BKLCLowerBound
$C_{120,2}$	[120, 35, 24]	56	40
$C_{120,3}$	[120, 36, 24]	40	32
$C_{120,4}$	[120, 84, 8]	14	12
$C_{120,5}$	[120, 85, 8]	14	11

Table 4.3: Bounds for other codes

Remark 4.3.4. *There are 5355 words with minimum weight in the codes* $C_{120,2}$ *and* $C_{120,3}$*. The codewords of minimum weight in* $C_{120,2}$ *and* $C_{120,3}$ *represent the action of G on the set of isotropic lines of the projective space PG (7, 2) and the stabilizer of a point in this set is a group isomorphic to* $2^{3+8} : S_3 \times S_6$*, where* $[G : (2^{3+8} : S_3 \times S_6)] = 5355$.

There are 11475 words with minimum weight in the codes $C_{120,4}$ *and* $C_{120,5}$*. The codewords of minimum weight in* $C_{120,4}$ *and* $C_{120,5}$ *represent the action of G on the set of isotropic*

planes of the projective space PG (7, 2) and the stabilizer of a point in this set is a group isomorphic to $2^{6+6} : S_3 \times L_3(2)$*, where* $[G : (2^{6+6} : (S_3 \times L_3(2))] = 11475$.

The codewords with minimum weight in the code $C_{120,6}$ *have no geometrical meaning.*

Proposition 4.3.4. *The automorphism group of the code* $C_{120,i}$ *for* $i = 1, 2, \cdots, 6$ *is* $G = S_8(2)$.

Proof: Suppose $\bar{G}$ is the automorphism group of the code $C_{120,i}$ for $i = 1, 2, \cdots, 6$. $\bar{G}$ is of order $2^{16} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 17 \cdot$. Using MAGMA, the composition series for $\bar{G}$ is $1_{\bar{G}} \lhd M \lhd \bar{G}$ which is actually a chief series for $\bar{G}$. Hence M is a non abelian chief factor of $\bar{G}$. The order of M is the same as the $|S_8(2)|$. Therefore $M \cong S_8(2)$. Hence the automorphism group of the code $C_{120,i}$ for $i = 1, 2, \cdots, 6$ is $S_8(2)$ □

4.4 Designs $\mathcal{D}_{n,r}$ held by the support of codewords with minimum weight in $C_{120,r}$ for r = 1, 2, . . . 6

A codeword is a vector. A q -ary vector$u$ of weight w determines the block of w points associated to the support of u. This means that the vectors of a fixed weight w in a q - ary code of length n hold a t- design and if the blocks determined by these vectors are the blocks of a t- design on n points, then that means there exists a t and λ such that every set of t coordinate positions occurs as non - zero positions in exactly λ vectors of weight w. Hence the knowledge of the number of vectors of each weight existing in a code is crucial in determining whether or not the supports of these vectors may form a design. For $q = 2$, the supports are in a 1 - 1 correspondence with the codewords. The Assmus - Mattson theorem gives conditions on the weight enumerators of a code and its dual that are sufficient to ensure that the support of the minimum weight codewords (and other weights also) give a t - design where t is a positive integer less than the minimum weight.

In this section, we describe designs held by the support of codewords with minimum weight.

Let $\mathcal{D}_{n,r}$ denote the 2 - design and $D_{n,r}$ denote the 1 - design held by the support of the minimum codewords in the code $C_{n,r}$. Table 4.4 and Table 4. 5 shows a suumary of the 1 - design and 2 - designs held by the codewords of minimum weight in $C_{n,r}$. Column one indicates the design $\mathcal{D}_{n,r}$, column two shows the parameters of the design, column three gives the number of blocks of the design and column four shows the automorphism group of the design.

$S_8(2)$ acts 2 - transitively on the set of coordinates of $C_{120,r}$ and hence we have that the support of a codeword of any fixed non - zero weight in $C_{120,r}$ will yield a 2 - design. From a 2 - design, computationally we can get a 1 - design.

We consider the action of $S_8(2)$ on the codewords of minimum weight. Let w_m denote a codeword of minimum weight in $C_{120,r}$ for $r = 1, 2, ..., 6$. Let $M = \{255, 5355, 11475\}$. If we take $m \in M$ for $C_{120,r}$ for r = 1, 2, 4 respectively, we get that $w_m^{S_8(2)}$ forms a single orbit and so $S_8(2)$ is transitive on the code coordinates. From the orbit stabilizer theorem we have $[S_8(2) : (S_8(2)_{w_m})] \in \{255, 5355, 11475\}$. This implies that $(S_8(2)_{w_m}) \in \{2^7 : S_6(2), 2^{3+8} : S_3 \times S_6, 2^{6+6} : S_3 \times L_3(2)\}$ respectively. Since $S_8(2)$ is transitive on code coordinates, the codewords with minimum weight forms designs 2 - (120, 56, 55), 2 - (120, 24, 207) and 2 - (120, 8, 45) respectively. The number of blocks is equal to the indices of $(S_8(2)_{w_m})$ in $S_8(2)$. Thus $S_8(2)$ acts primitively on the designs.

Using the above information, we can give a geometric interpretation of codewords with minimum weight.

Remark 4.4.1. *Codewords of weight 56 in $C_{120,1}$ represent the point of the projective space PG (7, 2) and the stabilizer of a point is a group isomorphic to $2^7 : S_6(2)$. They are also blocks of the 2 - (120, 56, 55) design.*

$\mathcal{D}_{n,r}$	2 - Design	Blocks	Aut ($\mathcal{D}_{n,r}$)
$\mathcal{D}_{n,1}$	2 - (120, 56, 55)	255	$S_8(2)$
$\mathcal{D}_{n,2}$	2 - (120, 24, 207)	5355	$S_8(2)$
$\mathcal{D}_{n,3}$	2 - (120, 24, 207)	11475	$S_8(2)$
$\mathcal{D}_{n,4}$	2 - (120, 8, 45)	11475	$S_8(2)$
$\mathcal{D}_{n,5}$	2 - (120, 8, 45)	11475	$S_8(2)$
$\mathcal{D}_{n,6}$	2 - (120, 4, 27)	11475	$S_8(2)$

Table 4.4: 2 - Designs for the 120 Representation

$\mathcal{D}_{n,r}$	1 - Design	Blocks	Aut ($\mathcal{D}_{n,r}$)
$\mathcal{D}_{n,1}$	1- (120, 56, 119)	255	$S_8(2)$
$\mathcal{D}_{n,2}$	1 - (120, 24, 1071)	5355	$S_8(2)$
$\mathcal{D}_{n,3}$	1 - (120, 24, 1071)	5355	$S_8(2)$
$\mathcal{D}_{n,4}$	1 - (120, 8, 765)	11475	$S_8(2)$
$\mathcal{D}_{n,5}$	1 - (120, 8, 765)	11475	$S_8(2)$
$\mathcal{D}_{n,6}$	1 - (120, 4, 1071)	32130	$S_8(2)$

Table 4.5: 1 - Designs for the 120 Representation

Proposition 4.4.1. *The automorphism group of the 1 - designs and the 2 - design $\mathcal{D}_{120,i}$ for $i = 1, 2, \cdots, 6$ is $G = S_8(2)$.*

Proof: Suppose $\bar{G}$ is the the automorphism group of the design $\mathcal{D}_{120,i}$ for $i = 1, 2, \cdots, 6$. $\bar{G}$ is of order $2^{16} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 17 \cdot$. Using MAGMA the composition series for $\bar{G}$ is $1_{\bar{G}} \lhd M \lhd \bar{G}$ which is actually a chief series for $\bar{G}$. Hence M is a non abelian chief factor of $\bar{G}$. The order of N is the same as the $|S_8(2)|$. Therefore $M \cong S_8(2)$. Hence the automorphism group of the design $\mathcal{D}_{120,i}$ for $i = 1, 2, \cdots, 6$ is $S_8(2)$ □

Chapter 5

The 136 Permutation Representation

5.1 Introduction

From Table 4.1, G acts two - transitively on the cosets of ${O_8}^+(2) : 2$ with orbits of length 1 and 135 in that order, from which we obtain a permutation representation of degree 136. Using this action, we form a permutation module of dimension 136 invariant under G. From the ATLAS, the elements being permuted by G are copies of ${O^+}_8(2)$.

The permutation module breaks into 5 absolutely irreducible components of dimensions 1, 8, 16, 26 and 48 with multiplicities 4, 2, 1, 2, and 1 respectively. We find only one irreducible submodule that is 1 dimensional . We obtain only one maximal submodule of dimension 135 in the permutation module. The 135 - dimension module breaks into one maximal submodule of dimension 127. The 127 - dimension module breaks into one maximal submodule of dimension 101. The 101- dimension module breaks into a pair of maximal submodules of dimension 85 and 100. The 85 – dimension module breaks into one maximal submodule of dimension 84. The 84 -dimension sub module breaks into one maximal sub module of dimension 36. The 36 - dimension module breaks into one maximal submodule of dimension 35. The 35 - dimension module breaks into one maximal submodule of dimension 9. The 9 - dimension module breaks into one irreducible maximal submodule of dimension 1. The 100 - dimension module breaks into a pair of maximal submodules of dimension 52 and 84. The 52 - dimension module breaks into one maximal submodule of dimension 51. The 51 - dimension module breaks into one maximal submodule of dimension 35. From the other 84 -dimension sub module, we obtain one maximal sub module of dimension 36. Thus the permutation module splits into submodules of dimensions 135, 127, 101, 100, 85, 84, 52, 51, 36, 35, 9 and 1. Thus we

obtain 10 non-trivial codes of dimensions 9, 35, 36, 51, 52, 84, 85, 100, 101, and 127.

The lattice of the sub modules is shown in figure 5.1.

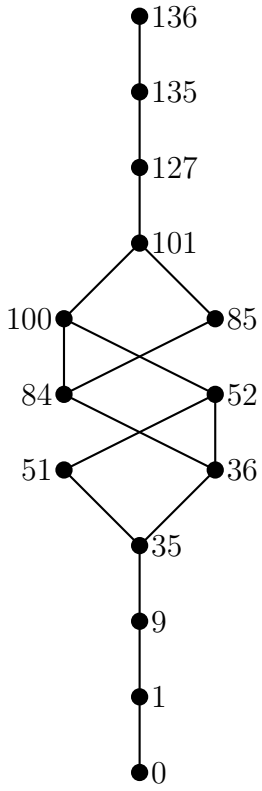

Figure 5.1: Lattice diagram for Representation 136

There are 10 non isomorphic codes of length 136. For the permutation representation of degree 136, we denote the constructed codes by $C_{136,r}$ for r = 1, 2,. . ., 10. The codes and their respective parameters are shown in Table 5.1. Column 1 shows the code $C_{136,r}$, column 2 indicates the parameters of the code, Column 3 provides the parameters of the dual code $C^{\perp}$ and column 4 shows the hull.

Due to computational limitations, we list the weight distributions of the first three codes of small dimension.

Weight distribution for $C_{136,1}$

$< 0, 1 >, < 64, 255 >, < 72, 255 >, < 136, 1 >$

Weight distribution for $C_{136,2}$

$< 0, 1 >, < 32, 16065 >,$

$< 36, 45696 >, < 40, 5355 >,$

$< 44, 4112640 >, < 48, 13494600 >,$

$< 52, 230307840 >, < 56, 1127322360 >,$

$< 60, 3755388672 >, < 64, 7164932115 >,$

$< 68, 9768487680 >, < 72, 7164932115 >,$

$< 76, 3755388672 >, < 80, 1127322360 >,$

$< 84, 230307840 >, < 88, 13494600 >,$

$< 92, 4112640 >, < 96, 5355 >,$

$< 100, 45696 >,$

$< 104, 16065 >,$

$< 136, 1 >$

Weight distribution for $C_{136,3}$

$< 0, 1 >, < 28, 5440 >, < 32, 16065 >,$

$< 36, 62016 >, < 40, 5355 >, < 44, 9253440 >,$

$< 48, 24461640 >, < 52, 456503040 >, < 56, 2290141944 >,$

$< 60, 7413581952 >, < 64, 14494048275 >, < 68, 19343318400 >,$

$< 72, 14494048275 >, < 76, 7413581952 >, < 80, 2290141944 >,$

$< 84, 456503040 >, < 88, 24461640 >, < 92, 9253440 >,$

$< 96, 5355 >, < 100, 62016 >, < 104, 16065 >,$

$< 108, 5440 >, < 136, 1 >$

Code $C_{136,r}$	**Parameters(n, k, d)**	**Dual** $C_{n,r}^{\perp}$	**Hull** $C_{n,r}$
$C_{136,\ 1}$	[136, 9, 64]	[136,127, 4]	[136, 9, 64]
$C_{136,\ 2}$	[136, 35, 32]	[136, 101,8]	[136, 35]
$C_{136,\ 3}$	[136, 36, 28]	[136,100,28]	[136, 36]
$C_{136,\ 4}$	[136, 51, 16]	[136, 85, 16]	[136, 35]
$C_{136,\ 5}$	[136, 52, 16]	[136, 84, 16]	[136, 36]
$C_{136,\ 6}$	[136, 84, 16]	[136, 52, 16]	[136, 52]
$C_{136,\ 7}$	[136, 85, 16]	[136, 51, 16]	[136, 51]
$C_{136,\ 8}$	[136, 100, 28]	[136, 36, 28]	[136,36, 28]
$C_{136,\ 9}$	[136, 101, 8]	[136, 35, 32]	[136, 35, 32]
$C_{136,\ 10}$	[136, 127, 4]	[136, 9, 64]	[136, 9, 64]

Table 5.1: The Code $C_{136,r}$ for $r = 1, 2, \cdots, 10$

.

Proposition 5.1.1. *Given a permutation module of dimension 136 of* $S_8(2)$*, let the set* $M = \{1, 2, 3\}$ *and the set* $N = \{4, 5, 6, 7, 8, 9, 10\}$*. Then the following hold:*

i) There are 10 non - isomorphic and non - trivial codes

ii) The code $C_{136,\ 1} = [136,\ 9,\ 64]$ *is an optimal code.*

iii) For $r \in M$*, the codes* $C_{136,r}$ *are self-orthogonal and doubly even codes with minimum weights 64, 32 and 28 respectively.*

iv) For $r \in N$ *the codes* $C_{136,\ r}$ *are even projective codes.*

Proof:

i) The permutation module splits into 14 non - isomorphic irreducible submodules which constitute the linear codes. Clearly, from figure 5.1, we have 10 non - trivial codes.

ii) The optimality of the code is given by MAGMA and also from Grassl online tables [19].

iii) The Hull $= C \cap C^{\perp}$. For all $r \in M$ the hull has the same dimension as the code. This implies that $C \subset C^{\perp}$ and thus the codes are self orthogonal.

Let w be the weight of a codeword. Using MAGMA, for all $r \in M$, the codes $C_{136,r}$ have $w \equiv 0 \bmod 4$. Thus the codes are doubly even.

iv) Let w be the weight of a codeword. Using MAGMA, for all $r \in N$, the codes $C_{136,r}$ have $w \equiv 0 \bmod 2$. Thus the codes are even.

All the dual codes have minimum distance $d \geq 3$. Thus the codes are projective.

Remark 5.1.1. *The words of minimum weight of the code represent the points of the projective plane PG(7,2) or the isotropic points in the orthogonal space. Dimension 9 of the $C_{136,\ 1}$ code illustrates the isomorphism between $S_8(2)$ and $O_9(2)$. The point stabilizer is the group isomorphic to the group $O_8^+ : 2$. Codewords of minimum weight form a 2 – (136, 64, 56) design with 255 blocks on which $S_8(2)$ acts primitively. The codewords of minimum weight in $C_{136,\ 1}$ represent the isotropic lines. The stabilizer of an isotropic line is a group isomorphic to $2^{3+8} : S_3 \times S_6$. With similar arguments applied to the proof of proposition 4.3.4 , the 2 - design has $S_8(2)$ as the automorphism group.*

The code $C_{136,\ 1}$ also generates a 1 - (136, 64, 120) design with 255 blocks on which $S_8(2)$ acts primitively. The code $C_{136,\ 1}$ is generated by row vectors of the point block incidence matrix of the corresponding design.

Proposition 5.1.2. *The autormophism group of the code $C_{136,r}$ for $r = 1,\ 2,\ 3,\ 4$ is $S_8(2)$.*

Proof

Suppose $\overline{G}$ is the automorphism group of the code $C_{136,\ i}$ for $i = 1,\ 2,\ 3, 4$. $\overline{G}$ is of order $2^{16}.3^5.5^2.7.17..$ By using MAGMA the composition series for $\overline{G}$ is $1_{\overline{G}} \trianglelefteq M \trianglelefteq \overline{G}$ of which it is a chief series for $\overline{G}$. Hence M is a non commutative chief factor of $\overline{G}$. The order of M is the same as the$|S_8(2)|$. Therefore $M \cong S_8(2)$. Hence the automorphism group of the code $C_{136,\ i}$ for $i = 1,\ 2,\ 3, 4$. is $S_8(2)$ □

5.2 Designs associated with the support of codewords for the Permutation Representation 136

Due to computational limitations, we describe the designs associated to codewords of minimum weight in $C_{136,1}, C_{136,2}$, $C_{136,3}$ and $C_{136,4}$. Let $\mathcal{D}_{n,r}$ be the design held by the codeword of minimum weight in $C_{136,r}$. Table 5.2 shows a summary of the designs held by the codewords of minimum weight for the codes $C_{136,1}, C_{136,2}$, $C_{136,3}$ and $C_{136,4}$. Column 1 lists the designs, column 2 gives the parameters of the 2 - design (1 - design) and column 3 shows the number of blocks. Given a 2- design, we can computationally obtain a 1 - design and not vice versa.

$\mathcal{D}_{n,r}$	2 - Design	Blocks	1 - Design	Blocks
$\mathcal{D}_{n,1}$	2 - (136, 64, 56)	255	1 - (136, 64, 120)	255
$\mathcal{D}_{n,2}$	2 - (136, 32, 868)	16065	1 - (136, 32, 3780)	16065
$\mathcal{D}_{n,3}$	2 - (136, 28, 224)	5440	1 - (136, 28, 1120)	5440
$\mathcal{D}_{n,4}$	2 - (136, 16, 30)	2295	1 - (136, 16, 270)	2295

Table 5.2: Some Designs held by codewords of minimum weight

5.2.1 The 2 - designs associated to codewords of minimum weight for the 136 representation

$S_8(2)$ acts 2 - transitively on the code co ordinates of $C_{136,r}$, thus the support of every fixed non - zero weight codeword in $C_{136,r}$ yields a 2 - design.

Taking the support of the 255 codewords with minimum weight in $C_{136,1}$ and orbiting them under $S_8(2)$, we get a 2 – (136, 64, 56) design with 255 blocks. The number of blocks is exactly equal to the number of codewords with minimum weight which implies that the codewords span the code.

Taking the support of the 5440 codewords with minimum weight in $C_{136,3}$ and orbiting them under $S_8(2)$, we get a 2 - (136, 28, 224) design with 5440 blocks. The number of blocks is exactly equal to the number of codewords with minimum weight which implies that the codewords span the code.

Taking the support of the 2295 codewords with minimum weight in $C_{136,\ 4}$ and orbiting them under $S_8(2)$, we get a 2 - (136, 16, 30) design with 2295 blocks. The number of blocks is exactly equal to the number of codewords with minimum weight which implies that the codewords span the code.

Proposition 5.2.1. *The automorphism group of the 2 - designs $\mathcal{D}_{136,r}$ for $r = 1, 2, 3, 4$ is the group $S_8(2)$.*

Proof: Let G = $S_8(2)$ and G_1 be the automorphism group of the 2 - design $\mathcal{D}_{136,1}$. The order of $G_1 \equiv |G|$ and by our construction $G \subset Aut(C)$. And since $Aut(C) = S_8(2)$, then $G_1 = S_8(2)$ and by induction it is true for r = 2, 3, 4. □

Remark 5.2.1.

i) The code $C_{136,1}$ holds a 2 - (136, 64, 56) design with 255 blocks. Therefore the words with minimum weight of the code forms a basis for the incidence matrix of the design. Also the blocks are primitive on the points of the projective space PG(7, 2) and on the action of G on the point stabilizer isomorphic to $2^7 : S_6(2)$.

ii) The number of blocks of 2 - (136, 32, 868) design held by the $C_{136,2}$ code is exactly the same as the number of words with minimum weight. Therefore the words with minimum weight in the code are the rows of the incidence matrix of the block design.

iii) The 2 - (136, 28, 224) design held by the code $C_{136,3}$ has 5440 blocks. Thus the words of minimum weight are exactly the same as the number of blocks of the design which implies that the codewords span the code. The words of minimum weight of

the code $C_{136,3}$ and the block size of the 2 - (136, 28, 224) design held by the code are isomorphic to the group $S_3 \times S_6(2)$ which is maximal in $S_8(2)$. The group $S_3 \times S_6(2)$ is a point stabilizer of the action of G on the non isotropic lines of the projective space PG (7, 2) and [G: $S_3 \times S_6(2)$] = 5440.

iv) The 2 - (136, 16, 30) design held by the code $C_{136,4}$ has 2295 blocks. Thus the codewords of minimum weight are equal to the blocks of the associated design. The words of minimum weight of the code $C_{136,4}$ and the block size of the 2 - design held by the code $C_{136,4}$ are isomorphic to the group 2^{10}: A_8 which is maximal in the group $G = S_8(2)$. The group $2^{10} : A_8$ is a point stabilizer of the action of $S_8(2)$ on the set of maximal isotropic subspaces of the projective space PG (7, 2) and [G: $(2^{10} : A_8)$] = 2295.

Similar remarks apply for the 1 - designs.

Combining all the propositions proved in this chapter and the description of the properties of the codes we hence have proved the following theorem:

Theorem 5.2.1. *Given that G is the simple projective symplectic group $S_8(2)$. In its natural action as a primitive rank - 2 group of permutation representation 136 on the copies of $O^+{}_8(2)$, a permutation module of dimension 136 invariant under G is formed. The permutation module splits into 14 submodules of which we obtain 10 non - trivial and non isomorphic binary linear codes. Let $\mathcal{D}_{136,r}$ be the design obtained by orbiting the codewords with minimum weight under G in the code $C_{136,r}$. Let $\mathcal{D}_{136,r}$ be the design associated to the words of minimum weight in $C_{136,r}$. Then*

i) There are 10 non - isomorphic and non - trivial codes

ii) The code $C_{136,1} = [136,\ 9,\ 64]$ is an optimal code.

iii) For $r \in M$, the codes [136, 9, 64], [136, 35, 32] and [136, 36, 28] are self-orthogonal and doubly even codes.

iv) For $r \in N$ the codes [136, 51, 16], [136, 52, 16], [136, 84, 16], [136, 85, 16], [136, 100, 28], [136, 101, 8] and [136, 127, 4] are even projective codes.

v) The automorphism group of the 2 -(136, 64, 56), 2 - (136, 32, 868), 2 - (136, 28, 224) and 2 - (136, 16, 30) designs is $S_8(2)$.

5.2.2 Graph of the of the 136 primitive representation

Let Γ be the graph of the 2 - (136, 64, 56) design. The graph is regular of valence 254. $\Gamma = (255, 32385)$. The number of vertices of the graph is equal to the block size of the combinatorial design. The words of minimum weight in $C_{136,1}$ represent the rows of the adjacency matrix of Γ.

Proposition 5.2.2. *The $Aut(\Gamma) = 2 : A_{255} \cong S_{255}$.*

Proof: Using MAGMA, the automorphism group of the graph is simple and its order is equal to the order of $2 : A_{255}$. □

Chapter 6

The Representation of Degree 255

6.1 Introduction

The point stabilizer of the coset action of $G = S_8(2)$ on the 255 point set of the projective plane PG(7, 2) is the group $2^7 : S_6(2)$ which is maximal in G. We get a permutation representation of degree 255. From Table 4.1 the group G acts primitively as a rank 3 group of degree 255 on the cosets of $2^7 : S_6(2)$ with orbits of lengths 1, 119 and 135. Using this action we form a permutation module of dimension 255 invariant under G. The permutation module breaks into absolutely irreducible components of dimension 1, 8, 16, 26 and 48 with multiplicities 7, 4, 1, 4 and 2 respectively. Working recursively and filtering out isomorphic copies of maximal submodules, the permutation module has a total of 80 submodules of dimensions 0, 1, 8, 9, 10, 35, 36, 37, 44, 45, 84, 85, 86, 92, 93, 94, 118, 119, 120, 121, 134, 135, 136, 137, 161, 162, 163, 169, 170, 171, 210, 211, 218, 219, 220, 245, 246, 247, 254 and 255. The lattice of the submodules is shown in Figure 6.1. From this we obtain in total 76 non - trivial binary codes of length 255 whose dimensions are 8, 9, 10, 35, 36, 37, 44, 45, 84, 85, 86, 92, 93, 94, 118, 119, 120, 121, 134, 135, 136, 137, 161, 162, 163, 169, 170, 171, 210, 211, 218, 219, 220, 245, 246 and 247 summarized in Table 6.1.

Dimension	#	Dimension	#	Dimension	#
8	1	93	3	163	1
9	3	94	1	169	1
10	1	118	1	170	3
35	1	119	7	171	1
36	3	120	7	210	1
37	1	121	1	211	1
44	1	134	1	218	1
45	1	135	7	219	3
84	1	136	7	220	1
85	3	137	1	245	1
86	1	161	1	246	3
92	1	162	3	247	1

Table 6.1: Dimensions of 76 non-trivial and non-isomorphic codes

6.2 The Binary Linear Codes $\mathrm{C}_{255,i}$

The permutation module splits into 80 submodules which gives us 76 non-trivial and non isomorphic codes of length 255 and dimensions as shown in the Table 6.1 where # represents the number of codes with the given dimension.
For any permutation representations of degree n, we denote the constructed codes by $\mathrm{C}_{n,1}, C_{n,2}, \cdots, C_{n,r}$ if r codes are obtained and by C_n if we only have one code up to isomorphism.

In this section we discuss the first five codes with small dimension shown in the Table 6.2. Due to computational limitations, we could only get the weight distribution of these 5 codes shown in Table 6.3.

Remark 6.2.1. *From Table 6.3, it is clear that all the codes are indecomposable.*

Proposition 6.2.1. *Given G as a permutation module of degree 255 with an irreducible submodule of dimension 8, the following holds:*

i) the code $C_{255,1}$ is a $[255, 8, 128]_2$ self orthogonal, doubly even, projective and optimal code. Its dual $C_{255,1}^{\perp}$ is a $[255, 247, 3]_2$ code.

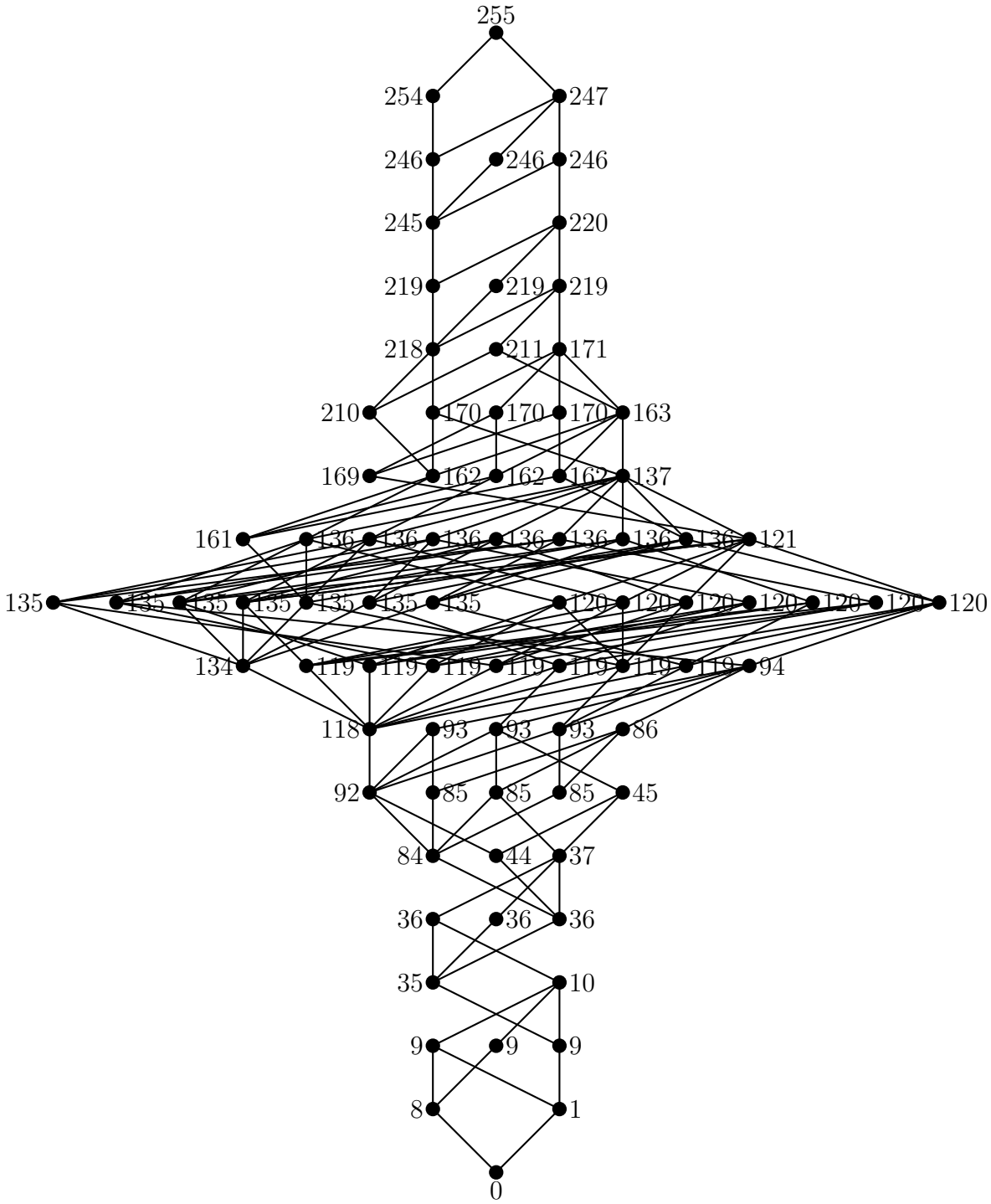

Figure 6.1: Lattice diagram for Representtion 255

Code	Parameters	Dual Code Parameters
$C_{255,1}$	$[255,8,128]_2$	$[255,247,3]_2$
$C_{255,2}$	$[255,9,119]_2$	$[255,246,3]_2$
$C_{255,3}$	$[255,9,127]_2$	$[255,246,4]_2$
$C_{255,4}$	$[255,9,120]_2$	$[255,246,3]_2$
$C_{255,5}$	$[255,10,119]_2$	$[255,245,4]_2$

Table 6.2: Parameters of codes of small dimension

Name	Dim	0	119	120	127	128	135	136	255
$C_{255,1}$	8	1				255			
$C_{255,2}$	9	1		136		255			
$C_{255,3}$	9	1	120	136		255	136	120	
$C_{255,4}$	9	1			255	255			1
$C_{255,5}$	10	1	120	136	255	255	136	120	1

Table 6.3: The weight distribution of some codes from a 255 dimensional representation

ii) The $Aut(C_{255,1}) = L_2(8)$.

Proof:

i) Computations by MAGMA shows the hull of $C_{255,1}$ has dimension 8 which is precisely the dimension of the code. This implies that $C \subseteq C^{\perp}$ this shows that the code is self orthogonal. The code $C_{255,1}$ is a one weight code whose weight enumerator is $1 + 255x^{128}$. Since $128 \equiv 0 \bmod 4$, the code is clearly doubly even. $C^{\perp}$ has minimum weight 3, therefore the code is projective. The optimality of the code is given by MAGMA and also from Grassl online tables.

ii) The code $C_{255,1}$ is spanned by its minimum weight codewords and these form the blocks of a symmetric 1 - (255, 128, 128) design $\mathcal{D}$, and we have that $Aut(\mathcal{D}) \leq Aut(C_{255,1})$. By the fundamental theorem of projective geometry, the automorphism group of $\mathcal{D}$ is $P\Gamma L_8(2)$ and the order $|Aut(\mathcal{D})| = 2^{28}.3^5.5^2.7^2.17.31.127 = |Aut(C_{255,1})|$. Therefore $Aut(C_{255,1}) = P\Gamma L_8(2)$.

Let $Aut(C_{255,1})$ be denoted by $\overline{G}$. By construction, all codes have $S_8(2) \leq \overline{G}$. Using MAGMA, the composition series for $\overline{G}$ is $1_{\overline{G}} \trianglelefteq N \trianglelefteq \overline{G}$ which is the only series for

$\overline{G}$. Thus N is a non abelian factor of $\overline{G}$. The order of N is the same as the $|L_8(2)|$. Therefore $N \cong L_8(2)$. Hence the automorphism group of the code $C_{255,1}$ is $L_8(2)$. $\square$

Remark 6.2.2.

i) The codewords with minimum weight in $C_{255,1}$ represent the points in the projective space PG (7, 2). The stabilizer of a point is a group isomorphic to the group $2^7 : S_6(2)$. The codewords with minimum weight in $C_{255,1}^{\perp}$ represent the points in the projective space PG (7, 2).

ii) The $C_{255,1}$ code has 255 codewords with minimum weight. Since $C_{255,1}$ is a [255, 8, 128] code, the words of minimum weight generate the code.

Proposition 6.2.2. *The code $C_{255,2}$ is a $[255, 9, 119]_2$ projective code. The dual code $C_{255,2}^{\perp}$ is a $[255, 246, 3]_2$ code. The automorphism group of the code $C_{255,2}$ is $S_8(2)$.*

Proof: Let $\overline{G}$ be the automorphism group of the code. $\overline{G}$ is of order $2^{16} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 17 \cdot$. The composition series for $\overline{G}$ found using MAGMA is $1_{\overline{G}} \trianglelefteq N \trianglelefteq \overline{G}$ which is actually a chief series for $\overline{G}$ Hence N is a non abelian chief factor of $\overline{G}$. The order of N is the same as the $|S_8(2)|$. Therefore $N \cong S_8(2)$. Hence the automorphism group of the code $C_{255,2}$ is $S_8(2)$.

Remark 6.2.3.

i) Given a linear code of length 255 and dimension 9, the best known linear code upper boundary with these parameters has minimum distance 127 and lower boundary minimum diatance 127. Therefore from MAGMA the code $C_{252,2}$ is a new code.

ii) The weight enumerator of $C_{255,2}$ is $1 + 120x^{119} + 255x^{128} + 136x^{135}$. Thus $C_{255,2}$, has 120 codewords with minimum weight while its dual has 5440 codewords with minimum weight. The group $G = S_8(2)$ acts on the cosets of $O_8^-(2) : 2$ with orbits

of length 1 and 119. From table 4.1 and the ATLAS, the elements being permuted by G are copies of $O_8^-(2)$. The number of codewords with minimum weight for the code $C_{255,2}$ is equal to the number of cosets of the point stabilizer for this group action. The dual code $C_{255\cdot 2^\perp}$ has 5440 codewords with minimum weight. The group $G = S_8(2)$ acts on the cosets of $S_3 \cdot S_6(2)$ with orbits of length 1,189, 336, 1890 and 3024. From ATLAS, the elements being permuted by G are the non isotropic lines. The number of codewords with minimum weight for the dual code $C_{255\cdot 2^\perp}$ is equal to the number of cosets of the point stabilizer for this group action.

Proposition 6.2.3. *The code $C_{255,3}$ is a [255,9,127]$_2$ optimal code and its dual $C_{255,3}^\perp$ is a [255,246,4]$_2$ even and code. The automorphism group of the code $C_{255,3}$ is $L_8(2)$.*

Proof The optimality of the code is given by MAGMA and also from Grassl online tables. The dual code has minimum weight at least 3, hence the code $C_{255,3}$ is projective. Let $\overline{G}$ be the automorphism group of the code. G is of order $2^{28} \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 17 \cdot 31 \cdot 127$. The composition series for G found using MAGMA is $1_{\overline{G}} \trianglelefteq N \trianglelefteq \overline{G}$ which implies that N is a non-abeian main factor of $\overline{G}$. Since $|N| = 2^{28} \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 17 \cdot 31 \cdot 127 = |L_8(2)|$ we have that $N \cong L_8(2)$. Hence the result. □

Remark 6.2.4. *The weight enumerator of the code $C_{255,3}$ is $1 + 255x^{127} + 255x^{128} + x^{255}$ and has 255 codewords with minimum weight. The number of codewords with minimum weight is precisely the number of points in the projective space PG(7,2). $G = S_8(2)$ acts primitively on the points of PG(7,2).*

Proposition 6.2.4. *The code $C_{255,4}$ is a [255,9,120]$_2$ self orthogonal, doubly even and projective code and its dual $C_{255,4^\perp}$ is a [255,246,3]$_2$ code. The automorphism group of the code $C_{255,4}$ is $S_8(2)$.*

Proof The weight enumerator for $C_{255,4}$ is $1 + 136x^{120} + 255x^{128} + 120x^{136}$. Clearly all the weights of the codewords are $0 \equiv \text{mod } 4$. Thus the code is doubly even and self orthogo-

nal. The proof of the automorphism is excatly as it is in the proof of proposition 6.2.2. □

Remark 6.2.5. *The code $C_{255,4}$ has 136 codewords with minimum weight. The codewords of minimum weight represent copies of $O_8^+(2)$ which is the plus hyperplane in the orthogonal space. The dual code $C_{255\cdot 4}^{\perp}$ has 5355 codewords with minimum weight. The group $G = S_8(2)$ acts on the cosets of $2^{3+8} : (S_3 \times S_6)$ with orbits of length 1, 90, 96, 240, 2048, 2880. From ATLAS, the elements being permuted by G are the 10795 isotropic lines of PG(7,2). The number of codewords with minimum weight for the dual code $C_{255\cdot 4}^{\perp}$ is equal to the number of cosets of the point stabilizer for this group action.*

Proposition 6.2.5. *The code $C_{255,5}$ is a $[255,10,119]_2$ code. The dual $C_{255,5}^{\perp}$ is a $[255,245,4]_2$ code. The automorphism group of the code $C_{255,5}$ is $S_8(2)$.*

Proof: Similar arguments as in the proof of proposition 6.2.2 could apply here.

Remark 6.2.6. *The code $C_{255,5}$ has 120 codewords with minimum weight. The weight enumerator for the code $C_{255,5}$ is $1 + 120x^{119} + 136x^{120} + 255x^{127} + 255x^{128} + 136x^{135} + 120x^{136} + x^{255}$. The codewords with minimum weight and codewords with weight 136 represent copies of $O_8^-(2)$ which is the elliptic form hyperplane in the orthogonal space. The codewords with weight 120 and 135 represent copies of $O_8^+(2)$ which is the quadratic form hyperplane in the orthogonal space. The codewords with weight 127 and 128 represent the points in the projective space PG (2, 7).*

6.3 Designs

Coding theory has been used to extend designs. In [16] Kennedy extended designs held by vectors of a code. A binary vector u of weight$w$ is said to determine a block of w points corresponding to the support of u. Hence, the vectors of a fixed weight w in a binary code of length$n$, hold at design if the blocks determined by these vectors are the t blocks of a t design on n points [8]. This means that every set of t coordinate positions occurs

as non- zero positions for exactly λ vectors of weight w. The knowledge of the number of vectors of each weight existing in a code is vital in the determination of whether or not the supports of these vectors could form a design.If S is the support of a vector in a code over $\mathbb{F}_q$, then it is the support of at least q - 1 such vectors and if the minimum weight of the code is $|S|$, then S is the support of precisely q - 1 vecors [22]. For q = 2, the supports are in a one to one correspondence with the codewords. The Assmus Mattson theorem [2], establishes the connection between codes and designs, in that codes of certain weight in a q-ary code hold a design and that we can determine the number of codes of such weight. The theorem provides conditions on the weight enumerators of a code and its dual that are sufficient to ensure that support of the minimum weight codes and other codes, yield a t design, where t is a positive integer less than the minimum weight.

We denote the 1 - designs by $\mathcal{D}_{255,r}$ for $r = 1, 2, \cdots, 5$ associated with the code $\mathrm{C}_{255,r}$ in the same range. From the weight distributions of the five codes, we found all the 1 - designs held by the supports of the codewords and also the 2 - designs in cases where they existed.

By a series of propositions that follow, we prove the following theorem:

6.3.1 Designs held by the support of the codewords in $\mathbf{C}_{255,i}$ for $i = 1, 2, \cdots, 5$

Let w_m be a codeword of non zero weight in $C = C_{255,r}$ for $r = 1, 2, \cdots, 5$. We determine the structure of the stabilizer of w_m in $\mathrm{Aut}(C)$, denoted by $\mathrm{Aut}(C)_{w_m}$ and form the designs D_{w_m} from the orbits. We examine the action of $\mathrm{Aut}(C) = L_8(2)$ or $\mathrm{Aut}(C) = S_8(2)$ on the set W_m of non trivial codewords of C and describe their nature. Let $M = \{119, 120, 127, 128, 135, 136\}$ for codes $C = C_{255,r}$ for $r = 1, 2, \cdots, 5$.For $m \in M$, we define $W_m = \{w_m \in C_{255,r} | wt(w_m) = m\}$. For $w_m \in W_m$, we take the image of the support of w_m under the action of $G = S_8(2)$ or $G = L_8(2)$ to form the blocks of the $t - (255, m, k_m)$ designs $D = D_{w_m}$ where $k_m = |(w_m)^G| \ . \ \frac{m}{255}$ and show that $\mathrm{Aut}(C)$ acts primitively on

D_{w_m}. In lemma 1, we show that for all $m \in M$, the stabilizer $Aut(C)_{w_m} = H$ where $H < \mathrm{Aut}(C)$ is a maximal subgroup of $\mathrm{Aut}(C)$.

Lemma 6.3.1. *Let $C = C_{255,r}$ for $r = 1, 2, \cdots, 5$ and $0 \neq w \in C$. Then $Aut(C)_w$ is a maximal subgroup of $Aut(C)$. Also, the design D obtained by orbiting the images of the support of any non trivial codeword in C is primitive.*

Proof

All the codes $C = C_{255,r}$ for $r = 1, 2, \cdots, 5$ have either $S_8(2)$ or $L_8(2)$ as the automorphism group. We consider the action of these two groups on the codewords of weight $m \in M$ separately.

Case I: Suppose $\mathrm{Aut}(C) = S_8(2)$ which we denote by $\overline{G}$. Let C be the codes $\mathrm{C}_{255,r}, r = 2, 4, 5$ and $M = \{119, 120, 127, 128, 135, 136\}$. In all cases of $m \in M, W_m$ is invariant under the action of $\overline{G}$. Thus every W_m is a single orbit under this action implying that $\overline{G}$ is transitive on each W_m. By the orbit stabilizer theorem, we conclude that $|\overline{G} : \overline{G}_{w_m}| \in \{119, 120, 128, 135, 136\}$. From Table 4.1, the table of maximal subgroups of $S_8(2), (S_8(2))_{w_m} \in \{O_8^-(2) : 2, O_8^+(2) : 2, 2^7 : S_6(2)\}$. Since $S_8(2)$ is transitive on the code coordinates.The codewords of W_m form a 1 - design D_{w_m} where the number of blocks comprise the indices of $(S_8(2))_{w_m}$ in $S_8(2)$. This means that $S_8(2)$ is transitive on the blocks of D_{w_m} for each W_m. Since $S_8(2)_{w_m}$ is a maximal subgroup of $S_8(2)$ for $m \in M$, we conclude that $S_8(2)$ acts primitively on D_{w_m}.

Case II: Suppose $\mathrm{Aut}(C) = L_8(2)$. In this case $\mathrm{C}_{255,r}, r = 1, 3$ and $M = \{119, 120, 127, 128, 135, 136, 255\}$. For all the choices of $m \in M$, we have $(w_m)^{L_8(2)} = W_m$. Thus W_m is a single orbit of $L_8(2)$. Similar arguments as in the first case, show that $L_8(2)_{w_m}$ is a maximal subgroup of $L_8(2)$ and that $L_8(2)$ acts primitively on the designs $\mathcal{D}_{w_m}$. □

In Table 6.4, the column one represents the codewords of weight m (the sub index of m represents the codes from where the codeword is obtained), the column two shows the parameters of the t - designs $\mathcal{D}_{w_m}$ as defined in sub - section 6.1, column three lists the

number of blocks of $\mathcal{D}_{w_m}$ and column four shows whether or not a design D_{w_m} is primitive under the action of $\mathrm{Aut}(C)$. This information is useful in giving a geometrical interpretation to the codewords of minimum weight.

Taking the supports of the codewords of non - zero weights in $\mathrm{C}_{255,r}$ and orbit them under the action of $S_8(2)$ to form the blocks of designs $\mathcal{D}_{w_m}$ on which $S_8(2)$ acts primitively on points and blocks. Our results are summarized in table 6.4.

m	D_{w_m}	Number of blocks	Primitive
$119_{3,5}$	1 - (255, 119, 56)	120	Yes
$120_{4,5}$	1 - (255, 120, 64)	136	Yes
$127_{2,5}$	1 - (255, 127, 127)	255	Yes
	2 - (255, 127, 63)	255	Yes
$128_{1,2,3,4,5}$	1 - (255, 128, 128)	255	Yes
	2 - (255, 128, 64)	255	Yes
$135_{3,5}$	1 - (255, 135, 72)	136	Yes
$136_{4,5}$	1 - (255, 136, 64)	120	Yes

Table 6.4: Primitive t - designs invariant under $\mathrm{Aut}(C)$

Proposition 6.3.1. *Let $M = \{127, 128\}, N = \{119, 120, 136, 137\}$. Let $\mathcal{D}_{w_m}$ be the design held by the codewords of weight m. Then the following hold:*

i) For $m \in M$ the automorphism group of the 1 - design $\mathcal{D}_{w_m}$ is $L_8(2)$.

ii) For $m \in M$ the automorphism group of the 2 - design $\mathcal{D}_{w_m}$ is $L_8(2)$.

iii) For $m \in N$ the automorphism group of the 1 - design $\mathcal{D}_{w_m}$ is $S_8(2)$.

Proof:

i) Let $\mathcal{D}_{w_m}$ be the symmetric 1 - design. By construction $S_8(2) \subseteq \mathrm{Aut}(C_{255,r})$ and $S_8(2)$ is a primitive group of degree 255. It follows that $\mathrm{Aut}(C_{255,r})$ is a primitive group of degree 255. Since there are exactly 255 codewords of weight 127 and 128, we use this fact to determine the automorphism group of the design as a set of permutations that preserve the set of the weight of codewords. Let $\overline{G}$ be the automorphism group of the $\mathcal{D}_{w_m}$ 1 - design. Using MAGMA $|\overline{G}| = 2^{28} \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 17 \cdot 31 \cdot 127$. The

composition series for $\overline{G}$ is $1_{\overline{G}} \trianglelefteq N \trianglelefteq \overline{G}$ which is the main series for $\overline{G}$ and implies that N is a non abelian factor of $\overline{G}$. Since $|N| = |\overline{G}|$ then $N \cong L_8(2)$ and hence $\overline{G} = L_8(2)$.

ii) We consider the action of $Aut(C_{255,r}) = L_8(2)$ for r = 1, 3. G acts 2 - transitively on the set of coordinates of $C_{255,r}$ and the support of a codeword of any fixed non zero weight in $C_{255,r}$ will yield a 2 - design. Since $C_{255,r}$ is spanned by the codewords of weight 128 and 127 respectively, and these codewords form the blocks of a symmetric 2 - (255, 127, 63) and 2 -(255, 128, 64) designs $\mathcal{D}_{w_m}$, we have that Aut ($\mathcal{D}_{w_m}$) $\subseteq Aut(C_{255,5})$. By the fundamental theorem of projective geometry, the automorphism group of the designs is $P\Gamma L_8(2)$ and by order $|Aut(mathcalD_{w_m})| = 2^{28} \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 17 \cdot 31 \cdot 127 = |Aut(C_{255,5})|$. Therefore $|Aut(\mathcal{D}_{w_m})| = P\Gamma L_8(2)$. The composition series for$Aut(\mathcal{D}_{w_m})$ shows that it is a simple group and by the classification of simple groups we get that $Aut(\mathcal{D}_{w_m}) = L_8(2)$.

iii) Similar arguments hold as in the proof of i) in proposition 6.3.1. □

.

Remark 6.3.1.

i) The codewords of minimum weight in $C_{255,1}$ represent the points of the projective space PG (7, 2) or the isotropic points of the orthogonal space. They also represent the blocks of the 1 - (255, 128, 128) symmetric design and the 2 - (255, 128, 64) designs of the points and hyperplanes of PG (7, 2). Thus the minimum weight codewords are the incident vectors of the blocks of the designs D and hence spanning vectors of the code. $S_8(2)$ acts primitively as a rank 3 group on the points of the projective space PG (7, 2) and the stabilizer of a point is $2^7 : S_6(2)$ which is maximal in $S_8(2)$. The primitive action of $S_8(2)$ on $2^7 : S_6(2)$ gives three orbits of length 1, 126 and 128. The codewords of minimum weight in $C_{255,1}$ represent the index of this coset action. That is, $[S_8(2) : (2^7 : S_6(2))] = 255$.

NB: there are 255 codewords with minimum weight 128 in $C_{255,1}$. *In* $C_{255,i}$ *for* $i = 2, 3, 4, 5$, *there are 255 codewords with weight 128 and thus represent the blocks of the same designs.*

Codewords of weight 127 (which is minimum in $C_{255,2}$*) represent the blocks of the 1 - (255, 127, 127) symmetric design and 2 - (255, 127, 63) design. Codewords of weight 119 (which is minimum in* $C_{255,3}$ *and* $C_{255,5}$*) represent the blocks of the 1 - (255, 119, 56) design. Codewords of weight 120 (which is minimum in* $C_{255,4}$*) represent the blocks of the 1 - (255, 120, 64) design. Codewords of weight 135 represent the blocks of the 1 - (255, 135, 72) design and codewords of weight 136 represent the blocks of the 1 - (255, 136, 64) design.*

ii) The symplectic group $S_8(2)$ *acts as a primitive rank-3 group of degree 255 on the points of the projective space PG (7, 2). The orbits of the point stabilizer are of length 1, 126 and 128. The point* $\propto$ *together with the points of the orbit of length 126 form a hyperplane which is the image of the absolute point under the symplectic polarity [14]. The symmetric 1 - (255, 128, 128) design* $\mathcal{D}$ *formed by orbiting the orbit of length 128 is the complement of the design of points and hyperplanes obtained by taking the union of the other 2 orbits. The union of the orbit of length 1 and length 126 give a 2 - (255, 126, 126) symmetric design and its complement is also a 2 - (255, 128, 64) design.*

iii) By the fundamental theorem of projective geometry, the automorphism group of the design of the points and planes and hence the complementary design is the full projective semi linear group $P\Gamma L_8(2)$.

iv) Let G be the simple symplectic group $S_n(q), n > 4$ *and q any prime power, acting as a rank 3 group of degree* $\frac{q^n-1}{q-1}$ *and let* $\mathcal{D}$ *be the* $1 - \left(\frac{q^n-1}{q-1}, q^{n-1}, q^{n-1}\right)$ *symmetric design. Then* $\mathcal{D}$ *is a symmetric 2 design with automorphism group* $P\Gamma L_n(q)$ *which properly contains the automorphism group of* $S_n(q)$ *and* $Aut(\mathcal{D}) \not< Aut(G)$ *[14].*

v) By taking the action on the symmetric design of the points and hyperplanes of the PG(7,2) space or its complementary design, the symplectic group $S_8(2)$ in its natural primitive rank 3 action on the points of the projective space PG(7,2) does not satisfy the conjecture of Key and Moori (section 7 in [11]). For the purpose of completeness of this thesis, we state the conjecture here: any design $\updownarrow\mathcal{D}$ obtained from a primitive permutation representation of a simple group G will have the automorphism group Aut(G) as its full automorphism group unless the design is isomorphic to another one constructed in the same way in which case the automorphism group of the design will be a proper subgroup of Aut(G) containing G.

Combining all the propositions proved in this chapter and the description of the properties of the first five codes with minimum dimension, we have thus proved the following theorem:

Theorem 6.3.1. *Let G be the simple projective symplectic group $S_8(2)$. In its natural action as a primitive rank 3 group of degree 255 on the points of the projective space PG(7, 2), a permutation module of dimension 255 invariant under G is formed. The permutation module splits into 80 submodules of which we obtain 76 non - trivial and non isomorphic binary linear codes. Let $\mathcal{D}_{w_m}$ be the design held by orbiting the codewords of weight w_m under G in the code $C_{255,r}$. Let $M = \{127, 128\}, N = \{119, 120, 136, 137\}$.*

i) The codes [255, 8, 128] and [255, 9, 127] are optimal codes.

ii) The codes [255, 8, 128] and [255, 9, 120] are doubly even and self orthogonal.

iii) The codes [255, 8, 128] and [255, 9, 119] are projective codes whose duals are 1 error correcting codes.

iv) The automorphism group of the codes [255, 8, 128] and [255, 9, 127] is the group $L_8(2)$ and the automorphism group of the codes [255, 9, 119], [255, 9, 120] and [255, 10, 119] is $S_8(2)$.

v) For $m \in M$ the automorphism group of the 1 - design $\mathcal{D}_{w_m}$ is $L_8(2)$.

vi) For $m \in M$ the automorphism group of the 2 - design $\mathcal{D}_{w_m}$ is $L_8(2)$.

vii) For $m \in N$ the automorphism group of the 1 - design $\mathcal{D}_{w_m}$ is $S_8(2)$.

viii) The minimum weight of the code $C_{255,r}$ for $i = 1, 2, \cdots, 5$ is the block size of the geometrical 1 design. Thus a basis of minimum words exists.

6.4 Graphs of the design $\mathcal{D}_{255,r}$

All the graphs of the designs are regular and the vertices are primitive on the points of the blocks. In Table 6.5, the column one gives the supports of codewords w in $\mathrm{C}_{255,r}$ orbited under the action of $S_8(2)$ to form the blocks of the designs$\mathcal{D}_{w_m}$, the column two gives the number of vertices of the graph , column three lists the number of edges of the graph and the column four shows the valency of the graph.

w	Vertices (V)	Edges (E)	Valency
119	120	7140	119
120	136	9180	135
127	255	32385	254
128	255	32385	254
135	136	9180	135
136	120	7140	119

Table 6.5: Parameters of the graph $\Gamma = (V, E)$

Remark 6.4.1. *From a $C_{255,1}$ [255,8,128]$_2$ code with 255 codewords with minimum weight, we get a symmetric 1 - (255, 128, 128) design with 255 blocks whose graph is* $\Gamma = (255, 128, 64, 64)$. *This graph is a symplectic graph* $\Gamma = (2^{2m} - 1, 2^{2m-1}, 2^{2m-2}, 2^{2m-2})$,*with* $m = 4$. *This graph is a known strongly regular graph with spectrum* $[128]^1, [8]^{119}, [-8]^{135}$. *The complement of this graph is also a strongly regular graph* $\overline{\Gamma} = (255, 126, 61, 63)$ *with spectrum* $[126]^1, [7]^{135}, [-9]^{119}$.

Chapter 7

Designs and codes from the Primitive permutation representations of degree 2295, 5355, 5440 and 11475

7.1 Introduction

For each of the primitive representation of the group $S_8(2)$ of degree 2295, 5355, 5440 and 11475, using MAGMA, we formed the orbits of the stabilizer of a point and for each of the non - trivial orbits and their unions, we orbited them under the full group, thus forming the symmetric 1 - design and the corresponding regular connected graph as described in Theorem 3.2.1.

Where computationally possible, we established the interplay between the various combinatorial objects.

In Table 7.1, the first column gives the degree (the number of cosets of the point stabilizer), the second column gives the number of orbits #, and the remaining columns give the length of the orbits of length greater than 1.

Degree	#	Length					
2295	5	30	280	960	1024		
5355	6	90	96	240	2048	2880	
5440	5	189	336	1890	3024		
11475	7	42	56	896	1008	4096	5376

Table 7.1: Some permutation representation of $S_8(2)$

7.2 The Representation of Degree 2295

Let $G = S_8(2)$ be a finite primitive permutation group acting on a set Ω (the maximal isotropic subspace of the projective space PG (7, 2)). The stabilizer of a point $\alpha \in \Omega$ in

this representation is a maximal subgroup isomorphic to the group $2^{10} : A_8$. We consider the rank - 5 primitive representation of degree 2295 on the cosets of $2^{10} : A_8$, with orbits of length 1, 30, 280, 960 and 1024. Due to the maximality of the point stabilizer, there is only one orbit of length 1. For each of the non - trivial orbits, we orbit them under the full group to form the symmetric 1 - designs as described in Theorem 3.2.1.

By Theorem 3.2.1 $\varepsilon = \{\{\alpha, \sigma\}^g : g \in G\}$, forms the edge set of a regular connected graph of valency $|\Delta|$. The vertices adjacent to α are the vertices in $\Delta \neq \{\alpha\}$, the orbit of the stabilizer G_α of α. As we orbit these pairs under G, we get nk ordered pairs and hence $\frac{nk}{2}$ edges where k = Δ. The group G acts on the graph and thus the graph is regular and its valency is k.

The rows of the incidence matrix of the design $\mathcal{D}$ form the q - ary linear code C of $\mathcal{D}$.

Let $\mathcal{D}_k, \Gamma_k$ and C_k denote the 1 - design, graph and the code of the design from the orbit of length i respectively. By the construction in theorem 3.2.1, table 7.2 shows the 1 - designs and the regular connected graphs of the primitive representation 2295 from the single non - trivial orbits.

Orbit length	1-design	Graph Γ
30	1 - (2295, 30, 30)	(2295, 34425)
280	1 - (2295, 280, 280)	(2295, 321300)
960	1 -(2295, 960, 960)	(2295, 1101600)
1024	1 - (2295, 1024, 1024)	(2295, 1175040)

Table 7.2: Designs and graphs of the primitive representation 2295

Lemma 7.2.1. *If G is the simple group $S_8(2)$, then it consists 4 non - isomorphic self -*

dual 1 - designs obtained by taking all the images under G of the non - trivial orbits of the point stabilizer in the 2295 primitive representation of G, on which G acts primitively on points and blocks. The code of the design is the row vectors of the incidence matrix of the design.

Theorem 7.2.1. *Let G be the simple projective symplectic group $S_8(2)$ and Ω the primitive G- set of size 2295 defined by the action on the cosets of $2^{10} : A_8$. Let $\alpha \in \Omega$ and $\Delta \neq \{\alpha\}$ be an orbit of G_α, the point stabilizer of α. Let $\mathcal{B} = \{\Delta^g : g \in G\}$, then $\mathcal{D}_k = (\Omega, \mathcal{B})$ with $k = |\Delta|$. Let the set $M = \{30, 280, 960, 1024\}$. Then the following hold:*

i) $\mathcal{D}_k$ is a symmetric $1 - (2295, |\Delta|, |\Delta|)$ design.

ii) Up to isomorphism there are 4 symmetric 1 - designs.

iii) If $k = 30, 280, 960$ then $Aut(\mathcal{D}_k) \cong S_8(2)$ and if $k = 1024$, then $Aut(\mathcal{D}_k) \cong O_{10}^+(2)$.

Proof

i) The proof of (i) and (ii) is quite clear by the construction method described in theorem 3.2.1.

ii) It is enough to prove for k = 30. Let $\bar{G}$ be the automorphism group of the design $\mathcal{D}_{30}$. $\bar{G}$ is of order $2^{16} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 17 \cdot$. The composition series for $\bar{G}$ found using MAGMA is $1_{\bar{G}} \trianglelefteq N \trianglelefteq \bar{G}$ which is actually a chief series for $\bar{G}$. Hence N is a non - abelian chief factor of $\bar{G}$. The order of N is the same as the $|S_8(2)|$. Therefore $N \cong S_8(2)$. Thus the automorphism group of the design $\mathcal{D}_{30}$ is $S_8(2)$.

By theorem 3.2.1, the automorphism group of the design contains the automorphism group of G. Thus $G = S_8(2) \subseteq Aut(\mathcal{D}_{1024}) \subseteq S_{2295}$ (the symmetric group on 2295 points), thus $Aut(\mathcal{D}_{1024})$ is a primitive permutation group on Ω of degree 2295. Let $\overline{G}$ be the automorphism group of the design $\mathcal{D}_{1024}$. $\overline{G}$ is of order $2^{20} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 17 \cdot 31$. The composition series for $\overline{G}$ found using MAGMA is $1_{\overline{G}} \trianglelefteq N \trianglelefteq \overline{G}$ which is actually

a chief series for $\overline{G}$. Hence N is a non abelian chief factor of $\overline{G}$. The order of N is the same as the $|O_{10}^{+}(2)|$. Therefore $N \cong O_{10}^{+}(2)$. Hence the automorphism group of the code $Aut(\mathcal{D}_{1024}) \cong O_{10}^{+}(2)$. □

.

7.2.1 Codes of the designs from single orbits of the representation 2295

Let C_k denote the code of the design $\mathcal{D}_k$. C_k consists of the row vectors of the incidence matrix of the block design $\mathcal{D}_k$. Table 7.3 shows the parameters of the codes of the designs. Column 1 indicates the orbit length, column 2 shows the codes of the designs and column 3 gives the automorphism group of the code.

k	C_k	Aut (C_k)
30	[2295, 2294]	$S_8(2)$
280	[2295, 728]	$S_8(2)$
960	[2295, 132]	$S_8(2)$
1024	[2295, 16, 1024]	$O_{10}^{+}(2)$.

Table 7.3: Some codes of the 1 - designs of the 2295 representation

Remark 7.2.1. *i) Due to computational limitations, the minimum weight of the codes C_{30}, C_{280} and C_{960} is not provided.*

ii) The code C_{30} is trivial.

Proposition 7.2.1. *Let C_k be the code of the design D_k, then the following hold:*

i) C_{280} is a $[2295, 728]$ even code. It's dual is a $[2295, 1567]$ code and the hull is $[2295, 596]$ code.

ii) C_{960} is a $[2295, 132]$ doubly even, self orthogonal and projective binary code.

iii) C_{1024} is a self orthogonal, doubly even projective $[2295, 16, 1024]$ code with 2295 words of minimum weight 1024. The dual code $C_{1024}^{\perp}$ is a $[2295, 2279, 3]$ uniformly packed code with 118575 words of minimum weight 3.

iv) $AutC_{960} \cong S_8(2)$.

Proof

i) we proved i) and ii) using MAGMA

ii) A code C is self orthogonal if $C \subseteq C^{\perp}$. The hull of the code $C(\mathcal{D}_{960})$ is a$[2295, 132]$ binary code. Since the dimension of the hull is equal to the dimension of the code, then the code is self orthogonal. Self orthogonal codes are doubly even.

iii) The code C_{1024} is a two weight code whose weight enumerator is $1 + 2295x^{1024} + 63240x^{1152}$. Clearly the weights $1024 \equiv 0 mod 4$ and $1152 \equiv 0 mod 4$. Thus the code is doubly even. The hull of the C_{1024} is of dimension 16, therefore $C_{1024} \subseteq C_{1024}^{\perp}$ and the code C_{1024} is self orthogonal. By Corollary 4.3 in [10], if $C^{\perp}$ is a 1 error correcting code, then $C^{\perp}$ is uniformly packed if and only if C is a two weight code. From MAGMA, the number of words with minimum weight is 118575. □

Proposition 7.2.2. *Let $Aut(C_k)$ be the automorphism group of the code C_k, then for k = 30, 280 and 960, $Aut(C_k) = S_8(2)$ and for k = 1024, $Aut(C_k) = O_{10}^{+}(2)$.*

Proof By the construction method described in theorem 3.2.1 and lemma 3.2.1, the automorphism group of the code contains the automorphism group of the design. Using MAGMA, the composition series for the automorphism group of the codes is given, and hence the result. □

Let Γ_k denote the regular connected graph of the design D_k. Table 7.2 shows the parameters (V, E) of the graph of valence k.
However C_{1024} of the design D_{1024} is a two weight code and a connection can be established between the code and a strongly regular graph which we discuss next.

7.2.2 A strongly Regular Graph on 65536 vertices related to $S_8(2)$

The code C_{1024} is a two weight code whose weight enumerator is $1+2295x^{1024}+63240x^{1152}$. Since C_{1024} is a two - weight code, a connection can be established with strongly regular graphs. Let w_1 and w_2 (where $w_1 < w_2$) be the weights of the q - ary two - weight code C_{1024}. A graph Γ_{1024} is associated as follows: the vertices of the graph are identified with the codewords and two vertices corresponding to the codewords u and v are adjacent if $d(u, v) = w_1$. Thus from the code C_{1024} we obtain a new strongly regular graph Γ_{1024} associated to C_{1024} whose properties are given in:

Lemma 7.2.2. *Γ_{1024} is a strongly regular (65536,2295,310,72) graph with spectrum* $[2295]^1, [247]^{2295}, [-9]^{63240}$. *The complementary graph $\overline{\Gamma}(C_{1024})$ of Γ_{1024} is a strongly regular (65536, 63240, 61016, 61256) graph with spectrum* $[63240]^1, [8]^{2295}, [-248]^{63240}$.

Proof The first part of the lemma follows using [10, Corollary 3.7]. Observe from above, the eigenvalues of an adjacency matrix A of Γ_{1024} are $\theta_0 = 2295, \theta_1 = 247$,and $\theta_2 = -9$ with corresponding multiplicities $f_0 = 1, f_1 = 2295$ and $f_2 = 63240$. □

Remark 7.2.2. *The group action of $G = S_8(2)$ on the set of maximal isotropic subspace of the projective space PG(7,2) yields a point stabilizer isomorphic to $2^{10} : A_8$ which is maximal in G. There are 2295 cosets of the point stabilizer, that is $[G : (2^{10} : A_8)] = 2295$. By orbiting the orbit of length 1024 under the full group, we get a symmetric 1 - (2295, 1024, 1024) self - dual design with 2295 blocks. The code of the $\mathcal{D}_{1024}$ design has 2295 codewords with minimum weight 1024. This implies that the words of minimum weight are the row vectors of the incidence matrix of $\mathcal{D}_{1024}$ or span the incidence matrix of the design.*

Length	Design	Aut(D_b)	code
31	1-(2295, 31 , 31)	$O^+_{10}(2)$	[2295, 729]
281	1-(2295, 281, 281)	$S_8(2)$	Trivial code
310	1-(2295, 310, 310)	$O^+_{10}(2)$	Trivial code
311	1-(2295, 311, 311)	$O^+_{10}(2)$	[2295, 133]
961	1-(2295, 961, 961)	$S_8(2)$	Trivial code
990	1-(2295, 990, 990)	$S_8(2)$	Trivial code
991	1-(2295, 991, 991)	$S_8(2)$	[2295, 729]
1025	1-(2295, 1025, 1025)	$S_8(2)$	Trivial code
1054	1-(2295, 1054, 1054)	$S_8(2)$	Trivial code
1055	1-(2295, 1055, 1055)	$O^+_{10}(2)$	[2295, 729]
1240	1-(2295, 1240, 1240)	$O^+_{10}(2)$	[2295, 728]
1241	1-(2295, 1241, 1241)	$S_8(2)$	Trivial code
1270	1-(2295, 1270, 1270)	$S_8(2)$	Trivial code
1271	1-(2295, 1271, 1271)	$O^+_{10}(2)$	[2295, 17, 1024]
1304	1-(2295, 1304, 1304)	$S_8(2)$	[2295, 728]
1305	1-(2295, 1305, 1305)	$S_8(2)$	Trivial code
1334	1-(2295, 1334, 1334)	$S_8(2)$	Trivial code
1335	1-(2295, 1335, 1335)	$S_8(2)$	[2295, 133]
1984	1-(2295, 1984, 1984)	$O^+_{10}(2)$	[2295, 132]
1985	1-(2295, 1985, 1985)	$O^+_{10}(2)$	Trivial code
2014	1-(2295, 2014, 2014)	$S_8(2)$	Trivial code
2015	1-(2295, 2015, 2015)		Trivial code
2264	1-(2295, 2264, 2264)	$O^+_{10}(2)$	[2295, 728]
2265	1-(2295, 2265, 2265)	$S_8(2)$	Trivial code
2294	1-(2295,2294, 2294)		Trivial code

Table 7.4: 1 - Designs formed by union of orbits of the point stabilizer

7.2.3 Designs for Union of Orbits of the point stabilizer of the 2295 representation

Let G be a finite primitive permutation group acting on a set Ω. It follows from Theorem 3.2.1 that if we form any union of orbits of the stabilizer of a point, and take their images under the action of the full group, we obtain the blocks of a symmetric 1 - design with the group G acting as an automorphism group.

Considering G to be the simple group $S_8(2)$, in this section we examine all the designs invariant under G, in particular designs constructed from unions of the orbits of the rank - 5 permutation representation of degree 2295. Let Ω be the primitive G - set of degree

2295 and Ω_1, Ω_2, Ω_3, Ω_4 and Ω_5 with subdegrees 1, 30, 280, 960 and 1024 respectively denote the sub orbits of G on Ω with respect to the point stabilizer $2^{10} : A_8$.

We consider the s - element subsets $\{i_1, ...i_s\}$ of the set $\{1, 2, 3, 4, 5\}$ to form $\begin{pmatrix} 5 \\ s \end{pmatrix}$ disinct unions of s suborbits Ω_i. To avoid trivial cases we exclude s = 0, 5. Subsequently we form the multiset R which represents the possible coordinates k of the block. Thus $R = \{31, 281, 310, 311, 961, 990, 991, 1025, 1054, 1055, 1240, 1241, 1270, 1271, 1304, 1305, 1334, 1335, 1984, 1985, 2014, 2264, 2294\}$. For $k \in R$ using lemma 4.1, we take the images of these unions under the action of G and form the 1 - designs D_k whose properties we examine in the sequel. Observe that $k = \left| \bigcup_{i=1}^{s} \Omega_{i_j} \right|$ where $1 \leqslant s \leqslant 4$ and $1 \leqslant k \leqslant 2294$ is the distinct union of s suborbits Ω_i.

For every k, using theorem 3.2.1 we take the images of these unions under the action of $S_8(2)$ and form the blocks of the self - dual symmetric 1 - designs D_k whose properties we examine in the sequel.

In table 7.3 column 1 gives the length of the joint orbits, that is $k = \left| \bigcup_{i=1}^{s} \Omega_{i_j} \right|$, column 2 shows the parameters of the union of orbits, column three represents the automorphism group of the design and column 4 shows the parameters of the code of the design.

Remark 7.2.3. *For some constructed designs we were not able to compute the full automorphism group of the design. Whenever the automorphism group of the code is not given, it is the consequence of computational limitations.*

Theorem 7.2.2. *Let G be the simple projective symplectic group $S_8(2)$ and Ω the primitive G - set of size 2295 defined by the action on the cosets of $2^{10} : A_8$. Let $\alpha \in \Omega$ and $\Delta = \bigcup_{i=1}^{s} \Omega_{i_j}$, $1 \leq s \leq 4$ be union of orbits of $(2^{10} : A_8)$ - orbits. Let $\mathcal{B} = \{ \Delta^g : g \in G\}$ and $\mathcal{D}_k = (\Omega, \mathcal{B})$ with $k = |\Delta|$. Define the sets M and N such that $M = \{281, 961, 990, 991, 1025, 1054, 1241, 1270, 1304, 1305, 1334, 1335, 2014, 2265\}$ and $N = \{31, 310,$*

$311, 1055, 1240, 1271, 1984, 1985, 2264\}$. *Then the following hold:*

i) $\mathcal{D}_k$ *is a symmetric* $1-(2295, |\Delta|, |\Delta|)$ *design.*

ii) Up to isomorphism there are 25 symmetric 1 - designs on 2295 points.

iii) If $k \in M$ *then* $Aut(\mathcal{D}_k) \cong S_8(2)$ *and if* $k \in N$*, then* $Aut(\mathcal{D}_k) \cong O_{10}^+(2)$.

Proof

i) The definition of Ω and $\mathcal{B}$ is clearly defined from the construction method described in theorem 3.2.1.

ii) First we consider the case when $k = 281$. Since $\mathcal{D}_{281}$ is a symmetric 1 - design, we need only show that $G = Aut(\mathcal{D}_{281})$. Now $G \subseteq Aut(\mathcal{D}_{281} \subseteq S_{2295}$, so $Aut(\mathcal{D}_{281})$ is a primitive permutation group on Ω of degree 2295. Let $\overline{G}$ be the automorphism group of the design $\mathcal{D}_{281}$. $\overline{G}$ is of order $2^1 6 \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 17 \cdot$. The composition series for $\overline{G}$ found using MAGMA is $1_{\overline{G}} \trianglelefteq N \trianglelefteq \overline{G}$ which is actually a chief series for $\overline{G}$ Hence N is a non abelian chief factor of $\overline{G}$. The order of N is the same as the $|S_8(2)|$. Therefore $N \cong S_8(2)$ and $Aut(\mathcal{D}_{281}) = S_8(2)$.

Now consider the case when k = 31. Since $\mathcal{D}_{31}$ is a symmetric 1 - design, it is enough to show that $Aut(\mathcal{D}_{31}) \cong O_{10}^+(2)$. Now $G \subseteq Aut(\mathcal{D}_{31}) \subseteq S_{2295}$, so $Aut(\mathcal{D}_{31})$ is a primitive permutation group on Ω of 2295 points. Also $Aut(\mathcal{D}_{31})_\alpha$ must fix $\Phi = \Omega_1 \cup \Omega_2$ setwise and thus $Aut(\mathcal{D})_{31}$ has an orbit of length 31 in Ω. The point stabilizer of the action of $O_{10}^+(2)$ on the maximal isotropic subspace $PG(9, 2)$ is the group $2^{10} : L_5(2)$. The only primitive group of degree 2295 that has a sub orbit of length 31 is $2^{10} : L_5(2)$. That is, the coset action of $O_{10}^+(2)$ on $2^{10} : L_5(2)$ has an orbit of length 31. Thus $Aut(\mathcal{D}_{31}) \cong O_{10}^+(2)$. □

7.2.4 Binary codes of the Designs of the union of orbits

Let C_k denote the binary code of the design $\mathcal{D}_k$, $L = \{1240, 1304, 2264\}$, $M = \{31, 991, 1055\}$, $N = \{281, 310, 961, 990, 1025, 1054, 1241, 1270, 1305, 1334, 1985, 2014, 2015, 2265, 2294\}$. Then the following hold:

Proposition 7.2.3. *i) If $k \in L$, then C_k is a [2295, 728] code.*

ii) If $k \in M$, then C_k is a [2295, 729] code.

iii) If $k \in N$, then C_k is trivial.

iv) C_{1984} is a [2295, 132] even, doubly even and self - orthogonal code.

v) C_{311} and C_{1335} are [2295, 133] codes.

vi) C_{1275} is a [2295, 17, 1024] code.

Proof

iv) Since the dimension of C_{1984} equals the dimension of the hull, it follows that $C \subseteq C^{\perp}$ and so C is self - orthogonal. □

Remark 7.2.4. *i) The constructed codes are of large dimension and we were not able to compute the minimum distance. In our results whenever the minimum distance is not given, is is a consequence of computational limitation.*

ii) The weight enumerator of the code C_{1275} is $1+2295x^{1024}+63240x^{1143}+63240x^{1152}+2295x^{1271}+x^{2295}$. The codewords of minimum weight in C_{1275} and those of weight 1271 represent the blocks of the symmetric $1-(2295, 1275, 1275)$ design. The words of minimum weight represent the length of the longest orbit of the coset action of G on the point stabilizer $2^{10} : A_8$.

7.3 The Representation of degree 5355

Let $G = S_8(2)$. The point stabilizer of the action of G on the isotropic lines of the projective space PG (7, 2) is the group $2^{3+8} : S_3 \times S_6$. As shown in table 4.1, there are 6 orbits of the action of G on $2^{3+8} : S_3 \times S_6$ of lengths 1, 90, 96, 240, 2048 and 2880, that is, $[G : (2^{3+8} : S_3 \times S_6)] = 5355$. The point stabilizer is maximal in G, hence there is only 1 orbit of length 1. As described in theorem 3.2.1, we form the symmetric 1 - designs by taking all the images under G of the non - trivial orbits of the point stabilizer and on which G acts primitively on points and blocks.

A summary of the 1 - designs and the regular connected graphs from single orbits is shown in Table 7.4. The column one shows the orbit length, the column two indicates the 1 - design, column three shows the parameters of the regular connected graphs and column four shows the parameters of the code of the design.

Due to computational limitations, we provide the number of edges for only the first two graphs.

Orbit length	1-design	Graph Γ	Code
90	1 - (5355, 90, 90)	(5355, 240975)	[5355, 5354]
96	1 - (5355, 96, 96)	(5355, 257040)	[5355, 1074]
240	1 -(5355, 240, 240)		[5355, 1230]
2048	1 -(53555, 2048, 2048)		[5355, 26, 2048]
2880	1 - (5355, 2880, 2880)		[5355, 1112]

Table 7.5: Designs of the primitive representation of degree 5355

Proposition 7.3.1. *Let G be the simple projective symplectic group $S_8(2)$ and Ω the primitive G - set of of size 5355 defined by the action of G on the cosets of $2^{3+8} : (S_3 \times S_6)$. Let $\alpha \in \Omega$ and $\Delta \neq \{\alpha\}$. Let $\mathcal{B} = \{\Delta^g : g \in G\}$ and $\mathcal{D}_k = (\Omega, \mathcal{B})$ with $k = |\Delta|$. Define the set $M = \{90, 96, 240, 2048, 2880\}$. Then, for $k \in M, \mathcal{D}_k$ is a symmetric $1-(5355, |\Delta|, |\Delta|)$ self - dual design.*

Proof

This result is inferred by the construction method described in theorem 3.2.1. For the

representation of degree 5355 we have 5 symmetric self - dual 1 - designs as shown in table 7.4 column 2. □

Let D_k, Γ_k, and C_k denote the 1 - design, graph and the code of the design from the orbit of length k respectively. Due to computational limitations we are not able to provide the automorphism group of the designs except for the $\mathcal{D}_{1024}$ design.

Proposition 7.3.2. *The* $Aut\,(D_{2048})$ *is* $G = S_8\,(2)$.

Proof

By the construction method described in theorem 3.2.1, the automorphism group of the design contains the automorphism group of the group. $G = S_8(2) \subseteq Aut(D_{2048}) \subseteq S_{2295}$ thus, $Aut(D_{2048})$ is a primitive permutation group on Ω of degree 5355. Let $\overline{G}$ be the automorphism group of the design D_{2048}. $\overline{G}$ is of order $2^{16} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot \cdot 17$. The composition series for $\overline{G}$ found using MAGMA is $1_{\overline{G}} \trianglelefteq N \trianglelefteq \overline{G}$ which is actually a chief series for $\overline{G}$. Hence N is a non abelian chief factor of $\overline{G}$. The order of N is the same as the $|S_8(2)|$. Therefore $N \cong S_8(2)$. Hence $Aut(D_{2048}) = S_8(2)$. □

Remark 7.3.1. *The group action of* $G = S_8(2)$ *on the isotropic lines of the projective space yields a point stabilizer isomorphic to* $2^{3+8} : S_3 \times S_6$ *which is a maximal subgroup of G. There are 5355 cosets of the point stabilizer, that is,* $[G : (\, 2^{3+8} : S_3 \times S_6\,)] = 5355$. *From the orbit of length 2048 of the point stabilizer a symmetric 1 – (5355, 2048, 2048) design is constructed. The design holds a binary code with 5355 codewords of minimum weight 2048. This means that the words of minimum weight of the code span the incidence matrix of the design.*

7.3.1 Designs for Union of Orbits of the point stabilizer of the 5355 Representation

Given a finite primitive permutation group G acting on a set Ω, we form any union of orbits of the stabilizer of a point and take their images under the action of the full group, we obtain the blocks of a symmetric 1 - design with the group G acting as an automorphism group.

Considering G to be the simple group $S_8(2)$, in this section we examine all the designs invariant under G, in particular designs constructed from unions of the orbits of the rank - 6 permutation representation of degree 5355. Let Ω be the primitive G - set of degree 2295 and Ω_1, Ω_2, Ω_3, Ω_4, Ω_5 and Ω_6 with subdegrees 1, 90, 96, 240, 2048 and 2880 respectively denote the sub orbits of G on Ω with respect to the point stabilizer $2^{3+8} : (S_3 \times S_6)$.
We consider the s - element subsets $\{i_1, ...i_s\}$ of the set $\{1, 2, 3, 4, 5, 6\}$ to form $\begin{pmatrix} 6 \\ s \end{pmatrix}$ disinct unions of s suborbits Ω_i. To avoid trivial cases we exclude s = 0, 6. Let $k = \left| \bigcup_{i=1}^{s} \Omega_{i_j} \right|$ where $1 \leqslant s \leqslant 5$ and $1 \leqslant k \leqslant 5354$.

For every k, using Theorem 3.2.1 we take the images of these unions under the action of $S_8(2)$ and form the blocks of the self - dual symmetric 1 - designs D_k whose properties we examine in the sequel.

In Table 7.5 column one gives the length of the joint orbits, that is $k = \left| \bigcup_{i=1}^{s} \Omega_{i_j} \right|$, column two shows the parameters of the designs of the union of orbits and column three shows the parameters of the code of the design.
Let D_k, C_k represent the symmetric 1 - design obtained by taking the image of the orbit of size k under the group G and the code of the design respectively.

Proposition 7.3.3. *Let G be the simple projective symplectic group* $S_8(2)$ *and* Ω *the*

Length	Design	Codes	Length	Design	Codes
91	1-(5355, 91, 91)	[5355, 1239]	2971	1-(5355, 2971, 2971)	[5355, 491]
97	1-(5355, 97, 97)	Trivial code	2976	1-(5355, 2976, 2976)	[5355, 356]
186	1-(5355, 186, 186)	Trivial code	2977	1-(5355, 2977, 2977)	Trivial code
187	1-(5355, 187, 187)	[5355, 237]	3066	1-(5355, 3066, 3066)	Trivial code
240	1-(5355, 240, 240)	[5355, 1230]	3067	1-(5355, 3067, 3067)	[5355, 1231]
241	1-(5355, 241, 241)	Trivial code	3120	1-(5355, 3120, 3120)	[5355, 236]
330	1-(5355, 330, 330)	Trivial code	3121	1-(5355, 3121, 3121)	Trivial code
331	1-(5355, 331, 331)	[5355, 357]	3210	1-(5355, 3210, 3210)	Trivial code
336	1-(5355, 336, 336)	[5355, 490]	3211	1-(5355, 3211, 3211)	[5355, 1073]
337	1-(5355, 337, 337)	Trivial code	3216	1-(5355, 3216, 3216)	[5355, 1238]
426	1-(5355, 426, 426)	Trivial code	3217	1-(5355, 3217, 3217)	Trivial Code
427	1-(5355, 427, 427)	[5355, 1113]	3306	1-(5355, 3306, 3306)	Trivial Code
2048	1-(5355, 2048, 2048)	[5355, 26]	3307	1-(5355, 3307, 3307)	[5355, 27, 2048]
2049	1-(5355, 2049, 2049)	Trivial code	4928	1-(5355, 4928,4928)	[5355, 1112]
2234	1-(5355, 2234, 2234)	Trivial code	4929	1-(5355, 4929, 4929)	Trivial code
2235	1-(5355, 2235, 2235)	[5355, 237]	5018	1-(5355, 5018, 5018)	Trivial code
2881	1-(5355, 2881, 2881)	Trivial code	5019	1-(5355, 5019, 5019)	[5355, 491]
2138	1-(5355, 2138, 2138)	Trivial code	5024	1-(5355, 5024, 5024)	[5355, 356]
2139	1-(5355, 2139, 2139)	[5355, 1239]	5025	1-(5355, 5025, 5025)	Trivial Code
2144	1-(5355, 2144, 2144)	[5355, 1072]	5168	1-(5355, 5168, 5168)	[5355, 236]
2145	1-(5355, 2145, 2145)	Trivial code	5114	1-(5355, 5114, 5114)	Trivial Code
2288	1-(5355, 2288, 2288)	[5355, 1230]	5115	1-(5355, 5115, 5115)	[5355, 1231]
2289	1-(5355, 2289, 2289)	Trivial code	5258	1-(5355, 5258, 5258)	Trivial Code
2378	1-(5355, 2378, 2378)	Trivial code	5259	1-(5355, 5259, 5259)	[5355, 1073]
2379	1-(5355, 2379, 2379)	[5355, 357]	5264	1-(5355, 5264, 5264)	[5355, 1238]
2384	1-(5355, 2384, 2384)	[5355, 490]	5265	1-(5355, 5265, 5265)	Trivial Code
2385	1-(5355, 2385, 2385)	Trivial Code	5354	1-(5355, 5354, 5354)	Trivial Code
2474	1-(5355, 2474, 2474)	Trivial Code	5355	1-(5355, 5355, 1)	[5355, 1, 5355]
2475	1-(5355, 2475, 2475)	[5355, 1235]			
2880	1-(5355, 2880, 2880)	[5355, 1239]			
2970	1-(5355, 2970, 2970)	Trivial code			

Table 7.6: Symmetric 1 - designs for union of orbits of the 5355 Representation

primitive G - set of size 5355 defined by the action on the cosets of $2^{3+8} : S_3 \times S_6$. Let $\alpha \in \Omega$ and $\Delta = \bigcup_{i=1}^{s} \Omega_{i_j}$, $1 \leq s \leq 5$ be union of orbits of $(2^{3+8} : S_8 \times S_6)$ - orbits. Let $\mathcal{B} = \{ \Delta^g : g \in G\}$ and $\mathcal{D}_k = (\Omega, \mathcal{B})$ with $k = |\Delta|$. Then the following hold:

i) $\mathcal{D}_k$ is a symmetric $1 - (5355), |\Delta|, |\Delta|)$ design.

ii) Up to isomorphism there are 61 non - trivial symmetric 1 - designs on 5355 points.

Proof

Result i and ii are inferred from the construction method described by Key and Moori in section 3.2. □

7.3.2 The binary Code C_{2048} of the 5355 Rrpresentation

Due to computational limitations, we describe the properties of only one code of the 1 - (5355, 2048, 2048) symmetric design. C_{2048} is a [5355, 26, 2048] binary code. The weight distribution of C_{2048} is :

$[< 0, 1 >, < 2048, 5355 >, < 2400, 45696 >, < 2528, 1370880 >, < 2560, 1349460 >,$

$< 2635, 11999232 >, < 2656, 21248640 >, < 2667, 31089600 >, < 2688, 31089600 >,$

$< 2699, 21248640 >, < 2720, 11999232 >, < 2795, 1349460 >, < 2827, 1370880 >,$

$< 2955, 45696 >, < 3307, 5355 >, < 5355, 1 >]$.

Proposition 7.3.4. *The code C_{2048} is doubly even and self - orthogonal and $Aut(C_{2048}) = S_8(2)$.* .

Proof Let w_i be the weight of all codewords in C_{2048}. Clearly, from the weight distribution of $C_{2048}, w_i \equiv 0 mod 4$, thus the code is doubly even. The hull of C_{2048} has dimension 26. This implies that $C \subseteq C^{\perp}$, thus the code is self- orthogonal.

The automorphism group of the code contains the automorphism group of the design by the construction method described in theorem 3.2.1. $G = S_8(2) \subseteq Aut(D_{2048}) \subseteq Aut(C_{2048}) \subseteq S_{5355}$, thus $Aut(C_{2048})$ is a primitive permutation group on Ω of degree 5355. Let $\overline{G}$ be the automorphism group of the design C_{2048}. $\overline{G}$ is of order $2^{16} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot \cdot 17$. The composition series for $\overline{G}$ found using MAGMA is $1_{\overline{G}} \trianglelefteq N \trianglelefteq \overline{G}$ which is actually a chief series for $\overline{G}$. Hence N is a non abelian chief factor of $\overline{G}$. The order of N is the same as the $|S_8(2)|$. Therefore $N \cong S_8(2)$. Hence $Aut(C_{2048}) = S_8(2)$. □

Remark 7.3.2. *i) The code C_{2048} is spanned by its minimum weight codewords and these form the blocks of the symmetric 1 - (5355, 2048, 2048) design.*

ii) The codewords of minimum weight of the code C_{2048} and the codewords of weight 3307 are the row vectors of the incident matrix of the design D_{2048}.

iii) The point stabilizer of the action of G on the set of isotropic lines of the projective space PG (7, 2) is the group isomorphic to $2^{3+8} : S_3 \times S_6$. The coset action of G on $2^{3+8} : S_3 \times S_6$ is such that $[G : (2^{3+8} : S_3 \times S_6)] = 5355$.

7.4 The representation of degree 5440

Let $G = S_8(2)$. The point stabilizer of the action of G on the non isotropic lines of the projective space PG (7, 2) is the group $S_3 \times S_6(2)$. As shown in table 4.1, there are 5 orbits of the action of G on $S_3 \times S_6(2)$ of lengths 1, 189, 336, 1890, and 3240, that is, $[G : S_3 \times S_6(2)] = 5440$. The point stabilizer is maximal in G, thus there is only 1 orbit of length 1. As described in theorem 3.2.1, we form the symmetric 1 - designs by taking all the images under G of the non - trivial orbits of the point stabilizer and on which G acts primitively on points and blocks.

A summary of the 1 - designs and the regular connected graphs from single orbits is shown in Table 7.6. Column one shows the orbit length and column two shows the parameters of the 1 - designs.

Orbit length	1-design	Code
189	1 -(5440, 189, 189)	[5440, 5440]
336	1 - (5440, 336, 336)	[5440, 366]
1890	1 - (5440, 1890, 1890)	[5440, 238]
3024	1 - (5440, 3024, 3024)	[5440, 366]

Table 7.7: Designs of the primitive representation of degree 5440

Let D_k, and C_k denote the 1- design and the code of the design from the orbit of length

Length	Design	Code	Length	Design	code
189	1-(5440, 189, 189)	Trivial code	3025	1-(5440, 3025, 3025)	Trivial code
190	1-(5440, 190, 190)	[5440, 238]	3213	1-(5440, 3213, 3213)	Trivial code
336	1-(5440, 336, 336)	[5440, 366]	3214	1-(5440, 3214, 3214)	Trivial code
337	1-(5440, 337, 337)	Trivial code	3360	1-(5440, 3360, 3360)	[5440, 28]
525	1-(5440, 525, 525)	Trivial code	3361	1-(5440, 3361, 3361)	Trivial code
526	1 -(5440,526,526)	[5440, 434]	3549	1-(5440, 3549, 3549)	Trivial code
1890	1-(5440, 1890, 1890)	[5440, 238]	3550	1-(5440, 3550, 3550)	[5440, 238]
1891	1-(5440, 1891, 1891)	Trivial code	4914	1-(5440, 4914, 4914)	[5440, 484]
2079	1-(5440, 2079, 2079)	Trivial code	4915	1-(5440, 4915, 4915)	Trivial code
2080	1-(5440, 2080, 2080)	[5440, 28]	5103	1-(5440, 5103, 5103)	Trivial code
2226	1-(5440, 2226, 2226)	[5440, 484]	5104	1-(5440, 5104, 5104)	[5440, 366]
2227	1-(5440, 2227, 2227)	Trivial code	5250	1-(5440, 5250., 5250)	[540,238]
2415	1-(5440, 2415, 2415)	Trivial code	5251	1-(5440, 5251, 5251)	Trivial code
2416	1-(5440, 2416, 2416)	[5440, 366]	5439	1-(5440, 5439, 5439	trivial code
3024	1-(5440, 3024, 3024)	[5440, 366]	5440	1-(5440, 5440, 1)	[5440, 1, 5440]

Table 7.8: Designs of the union of orbits of the primitive representation of degree 5440

k respectively.

Theorem 7.4.1. *Let G be the simple projective symplectic group $S_8(2)$ and Ω the primitive G - set of of size 5440 defined by the action of G on the cosets of $S_3 \times S_6(2)$. Let $\alpha \in \Omega$ and $\Delta \neq \{\alpha\}$. Let $\mathcal{B} = \{\Delta^g : g \in G\}$ and $\mathcal{D}_k = (\Omega, \mathcal{B})$ with $k = |\Delta|$. Define the set $M = \{189, 366, 1890, 3024\}$. Then, for $k \in M, \mathcal{D}_k$ is a symmetric $1 - (5440, |\Delta|, |\Delta|)$ self - dual design.*

Proof

This result is inferred by the construction method described in theorem 3.2.1. For the representation of degree 5440 we have 4 symmetric self - dual 1 - designs as shown in table 7.6 column 2. □

Proposition 7.4.1. *Let $N = \{336, 1890, 3024\}$, then for $k \in N, C_k$ is self - orthogonal and doubly even.*

Proof: The hull of C_k has the same dimension as the code C_k . This implies that $C \subseteq C^{\perp}$. Hence the code is self orthogonal and by using MAGMA the code is doubly even. □

7.4.1 Designs for Union of orbits of the point stabilizer of the 5440 Representation

Considering G to be the simple group $S_8(2)$, we examine all the designs invariant under G, in particular designs constructed from unions of the orbits of the rank - 5 permutation representation of degree 5440. Let Ω be the primitive G - set of degree 5440 and Ω_1, Ω_2, Ω_3, Ω_4, and Ω_5 with subdegrees 1, 189, 366, 1890 and 3240 respectively denote the orbits of G on Ω with respect to the point stabilizer $S_3 \times S_6(2)$.

We consider the s - element distinct subsets $\{i_1, ...i_s\}$ of the set $\{1, 2, 3, 4, 5\}$ to form $\begin{pmatrix} 5 \\ s \end{pmatrix}$ disinct unions of s suborbits Ω_i. To avoid trivial cases we exclude s = 0, 5. Let $k = \left| \bigcup_{i=1}^{s} \Omega_i \right|$ where $1 \leqslant s \leqslant 5$ and $1 \leqslant k \leqslant 5439$.

For every k, using theorem 3.2.1 we take the images of these unions under the action of $S_8(2)$ and form the blocks of the self - dual symmetric 1 - designs D_k whose properties we examine in the sequel.

In table 7.7 column 1 gives the length of the joint orbits, that is $k = \left| \bigcup_{i=1}^{s} \Omega_i \right|$, column 2 shows the parameters of the designs of the union of orbits and column 3 shows the parameters of the code of the design.

Theorem 7.4.2. *Let G be the simple projective symplectic group $S_8(2)$ and Ω the primitive G - set of size 5440 defined by the action on the cosets of $S_3 \times S_6(2)$. Let $\alpha \in \Omega$ and $\Delta = \bigcup_{i=1}^{s} \Omega_{i_j}$, $1 \leq s \leq 5$ be union of orbits of $S_8 \times S_6(2)$ - orbits. Let $\mathcal{B} = \{ \Delta^g : g \in G\}$ and $\mathcal{D}_k = (\Omega, \mathcal{B})$ with $k = |\Delta|$. Then the following hold:*

i) $\mathcal{D}_k$ is a symmetric $1 - (5440), |\Delta|, |\Delta|)$ design.

ii) Up to isomorphism there are 25 non - trivial symmetric 1 - designs on 5440 points.

Proof

Result i and ii are inferred from the construction method described by Key and Moori in section 3.2. 1 □

7.4.2 Binary codes of the 1 - designs from union of orbits in the 5440 representation

The row vectors of the incidence matrix of the design D_k form the code C_k.

Proposition 7.4.2. *Let* $L = \{1890\}, M = \{190, 336, 2080, 2226, 2416, 3024, 3360, 5104\}$, $N = \{526, 3214, 3550, 4914, 5250\}$. *Then:*

i) For $k \in L$, *the code* C_k *is even.*

ii) For $k \in M$, *the code* C_k *is doubly even and self - orthogonal.*

iii) For $k \in N$, *the code* C_k *is even and self - orthogonal.*

Proof

Due to computational limitations, the weight distribution of the codes could not be obtained. By using MAGMA, the codes are even. The dimension of the hull of the codes C_k is the same as the dimension of the code. Since $C \subseteq C^{\perp}$, it implies that the codes are self orthogonal.

7.5 The representation of degree 11475

Let $G = S_8(2)$. The point stabilizer of the action of G on the isotropic planes of the projective space PG (7, 2) is the group $2^{6+6} : (S_3 \times L_3(2))$. As shown in table 4.1, there are 7 orbits of the action of G on $2^{6+6} : (S_3 \times L_3(2))$ of lengths 1, 42, 56, 896, 1008,4096 and 5376, that is, $[G : 2^{6+6} : (S_3 \times L_3(2)] = 11475$. Due to the maximality of the point

stabilizer, there is only 1 orbit of length 1. As described in theorem 3.2.1, we form the symmetric 1 - designs by taking all the images under G of the non - trivial orbits of the point stabilizer and on which G acts primitively on points and blocks.

A summary of the 1 - designs from single orbits is shown in table 7.8. The first column shows the orbit length, the second shows the parameters of the 1 - designs and third column shows the parameters of the codes of the design. .

Orbit length	1-design	Code
42	1 - (11475, 42, 42)	Trivial code
56	1 -(11475, 56, 56)	[11475, 2824]
896	1 - (11475, 896, 896)	[11475, 612]
1008	1 - (11475, 1008, 1008	
4096	1 - (11475, 4096, 4096)	
5376	1 - (11475, 5376, 5376)	

Table 7.9: Designs of the primitive representation of degree 11475

Let D_k, andC_k denote the 1- design, graph and the code of the design from the orbit of length k.

Remark 7.5.1. *For most of the constructed designs we were not able to compute the codes of the designs. This is a consequence of computational limitations.*

7.5.1 Designs for union of orbits of the point stabilizer of the 11475 representation

Considering G to be the simple group $S_8(2)$, in this section we examine all the designs invariant under G, in particular designs constructed from unions of the orbits of the rank - 7 permutation representation of degree 11475. Let Ω be the primitive G - set of degree 11475 and Ω_1, Ω_2, Ω_3, Ω_4, Ω_5, Ω_6, and Ω_7 with subdegrees 1, 42, 56, 896, 1008, 4096 and 5376 respectively denote the orbits of G on Ω with respect to the point stabilizer

$2^{6+6} : (S_3 \times L_3(2))$.

We consider the s - element subsets $\{i_1, ...i_s\}$ of the set $\{1, 2, 3, 4, 5, 6, 7\}$ to form $\begin{pmatrix} 7 \\ s \end{pmatrix}$ disinct unions of s suborbits Ω_i. To avoid trivial cases we exclude s = 0, 7. Let $k = \left| \bigcup_{i=1}^{s} \Omega_i \right|$ where $1 \leqslant s \leqslant 5$ and $1 \leqslant k \leqslant 5439$.

For every k, using Theorem 3.2.1 we take the images of these unions under the action of $S_8(2)$ and form the blocks of the self - dual symmetric 1 - designs D_k whose properties we examine where possible due to the large degree of the representation.
In Table 7.9, we list the 1 - designs for $k = \left| \bigcup_{i=1}^{s} \Omega_i \right|$.

7.6 Conclusions and Recommendations for Further Research

We have used coding theory to try and understand the internal structures of the group $S_8 2$. We enumerated and characterized all the codes held by the group for the permutation representation 120, 136 and 255 using the modular theoretic method. We were able to display the lattice structures for these codes. For higher permutation representations:- 2295, 5355, 5340 and 11475 we did not get all the codes due to computational limitations with MAGMA capabilities.
We recommend for further research to devise a method or a tool to overcome the computational limitations experienced using MAGMA in its current state.

Designs	Designs	Designs	Designs
1-(11475, 42, 42)	1-(11475, 4097, 4097)	1-(11475, 6000, 6000)	1-(11475, 9473, 9473)
1-(11475, 43, 43)	1-(11475, 4138, 4138)	1-(11475, 6001, 6001)	1-(11475, 9514, 9514)
1-(11475, 56, 56)	1-(11475, 4139, 4139)	1-(11475, 6042, 6042)	1-(11475, 9515, 9515)
1-(11475, 57, 57)	1-(11475, 4152, 4152)	1-(11475, 6043, 6043)	1-(11475, 9528, 9528)
1-(11475, 98, 98)	1-(11475, 4153, 4153)	1-(11475, 6056, 6056)	1-(11475, 9529, 9529)
1-(11475, 99, 99)	1-(11475, 4194, 4194)	1-(11475, 6057, 6057)	1-(11475, 9570, 9570)
1-(11475, 896, 896)	1-(11475, 4195, 4195)	1-(11475, 6098, 6098)	1-(11475, 9571, 9571)
1-(11475, 897, 897)	1-(11475, 4992, 4992)	1-(11475, 6099, 6099)	1-(11475, 10368, 10368)
1-(11475, 938, 938)	1-(11475, 4993, 4993)	1-(11475, 6272, 6272)	1-(11475, 10369, 10369)
1-(11475, 939, 939)	1-(11475, 5034, 5034)	1-(11475, 6273, 6273)	1-(11475, 10410, 10410)
1-(11475, 952, 952)	1-(11475, 5035, 5035)	1-(11475, 6314, 6314)	1-(11475, 10411, 10411)
1-(11475, 953, 953)	1-(11475, 5048, 5048	1-(11475, 6315, 6315)	1-(11475, 10424, 10424)
1-(11475, 994, 994)	1-(11475, 5049, 5049)	1-(11475, 6328, 6328)	1-(11475, 10425, 10425)
1-(11475, 995, 995)	1-(11475, 5090, 5090)	1-(11475, 6329, 6329)	1-(11475, 10466, 10466)
1-(11475, 1008, 1008)	1-(11475, 5091, 5091)	1-(11475, 6370, 6370)	1-(11475, 10467, 10467)
1-(11475, 1009, 1009)	1-(11475, 5104, 5104)	1-(11475, 6371, 6371)	1-(11475, 10480, 10480)
1-(11475, 1050, 1050)	1-(11475, 5105, 5105)	1-(11475, 6384, 6384)	1-(11475, 10481, 10481)
1-(11475, 1051, 1051)	1-(11475, 5146, 5146)	1-(11475, 6385, 6385)	1-(11475, 10522, 10522)
1-(11475, 1064, 1064)	1-(11475, 5147, 5147)	1-(11475, 6426, 6426)	1-(11475, 10523, 10523)
1-(11475, 1065, 1065)	1-(11475, 5160, 5160)	1-(11475, 6427, 6427)	1-(11475, 10536, 10536)
1-(11475, 1106, 1106)	1-(11475, 5161, 5161)	1-(11475, 6440, 6440)	1-(11475, 10537, 10537)
1-(11475, 1107, 1107)	1-(11475, 5202, 5202)	1-(11475, 6441, 6441)	1-(11475, 10578, 10578)
1-(11475, 1904, 1904)	1-(11475, 5203, 5203)	1-(11475, 6482, 6482)	1-(11475, 10579, 10579)
1-(11475, 1905, 1905)	1-(11475, 5376, 5376)	1-(11475, 6483, 6483)	1-(11475, 11376, 11376)
1-(11475, 1946, 1946)	1-(11475, 5377, 5377)	1-(11475, 7280, 7280)	1-(11475, 11377, 11377)
1-(11475, 1947, 1947)	1-(11475, 5418, 5418)	1-(11475, 7281, 7281)	1-(11475, 11418, 11418)
1-(11475, 1960, 1960)	1-(11475, 5419, 5419)	1-(11475, 7336 ,7336)	1-(11475, 11419, 11419)
1-(11475, 1961, 1961)	1-(11475, 5432, 5432)	1-(11475, 7337, 7337	1-(11475, 11432, 11432)
1-(11475, 2002, 2002)	1-(11475, 5433, 5433)	1-(11475, 7378, 7378)	1-(11475, 11433, 11433)
1-(11475, 2003, 2003)	1-(11475, 5474, 5074)	1-(11475, 7379, 7379)	1-(11475, 11474, 11474)
1-(11475, 4096, 4096)	1-(11475, 5475, 5475)	1-(11475, 9472, 9472)	1-(11475, 11475, 11475)

Table 7.10: Designs for union of orbits of the representation 11475

References

[1] E. Artin (1957). *Geometric Algebra*, Wiley Interscience, New York, ISBN-13: 978-0471608394.

[2] E. F Assmus, Jr and J. D. Key (1992). Designs and their codes, *Cambridge University Press, Cambridge tracts in mathematics*, Vol 103, ISBN 9780521413619. .

[3] W. Bosma, J. Cannon, C. Playoust (1997). The Magma algebra system 1, the user language. *Journal of symbolic computations* Vol 24, no. 3-4, 235 - 265.

[4] N.L. Biggs, A. T. White (1979). *Permutation groups and combinatorial structures.* Cambridge University press, London Mathematical Society Lecture Notes Series, First Edition.

[5] R. Calderbank, W. M. Kantor (1986). The geometry of two weight codes. *London Mathematical Society*, Vol 18, Issue 2, 97 - 122.

[6] Y. M. Chee, H. M. Kiah and P. Purkayatsha, (2013). Matrix Codes and Multitone Frequency Shift Keying for Power Line Communications, *2013 IEEE International Symposium of Information Theory*, 2870 - 2874.

[7] L. Chikamai, J. Moori, B. G. Rodrigues (2014), Some irreducible 2 - modular codes invariant under the Symplectic group $S_6(2)$, *Glssnicki Mathematicki*, Vol 49, Issue 69, 235 - 262.

[8] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson (1985). *Atlas of finite groups*, Oxford university press, Oxford, ISBN 0-19-853199-0.

[9] D. Crnkovic, S. Rukavina (2004). On Symmetric (71, 35, 17) design. *Math. Maced.* Vol 2, 51- 58.

[10] D Crnkovic, S. Rukavina, L. Simcic (2013). Binary doubly even self dual codes of length 72 with large automorphism groups. *Mathematical communications*, Vol 18, no. 2, 297 - 308.

[11] P. Delsarte (1972). Weight of linear codes and strongly regular normed spaces. *Discrete Mathematics*, Vol 3, Issues 1 - 3, 47 - 64.

[12] P. Dembowski (2012). *Finite geometries*, Springer Science and Business Media, ISBN 978 364 262 0126 .

[13] Georges Ferdinand R Radohery (2014), Designs and codes from certain finite simple groups, *Msc Thesis*, North West University.

[14] M. Grassl(2007). *Bounds on the minimum distance of linear codes and quantum codes.* Available online at `http://www.codetables.de`. Accessed on 16^{th} June 2018.

[15] D. Jungnickel, A. Pot, K. W. Smith (2007). *Difference Sets. Handbook of Combinatorial Designs*, CRC Press, 2nd Edition.

[16] G. T Kennedy, V. Pless (1995). A coding theoretic approach to extending designs. *Discrete Mathematics*, Vol 142, Issue 1 - 3, 155 - 168.

[17] J . D Key (1998). Codes and finite geometries. *Congress Num.* Vol 131, 85 - 89.

[18] J. D. Key, J. Moori (2002). Designs, codes and graphs from the janko groups J_1 and J_2.*Journal of Combinatorial Mathematics and Combinatorial Computing*, Vol 40, 143 - 153.

[19] G. F. R. Radoheny (2013). Designs and codes from certain Finite simple groups. *Masters thesis*, North west University.

[20] Rauhi I. Elkhatib (2012). The Maximal Subgroups of the Symplectic Group $PSp(8,2)$. *Journal of Systems and Software*, Vol 2, No. 3, 126 - 132.

[21] B.G. Rodriguez (1999). On the theory and examples of group extensions, *Masters thesis*, University of Natal, Pietermaritzburg.

[22] B. G. Rodriguez (2003), Codes of designs and graphs from finite simple groups. *Ph.D thesis*, University of Natal, Pietermaritzburg.

[23] B. G. Rodriguez (2008). Self orthogonal designs and codes from the symplectic groups $S_4(3)$ and $S_4(4)$. *Science Direct, Discrete Mathematics*, Vol 308, 1941 - 1950.

[24] B. G. Rodriguez (2018). A projective two weight code related to the simple group Co_1 of Conway. *Graphs and Combintorics*, Vol 34, Issue 3, 509 - 521.

[25] J. J. Rotman (1994). *An Introduction to the Theory of Groups*. Springer - Verlag New - York, 4^{th} Edition.

[26] D. Seipe (2009). Investigation of binary self dual codes invariant under simple groups, *Masters Thesis*, The University of Arizona.

[27] C. Shannon (1948). A mathematical theory of communication. *Bell system Technical Journal*, Vol 27, Issue 3, 379 - 423.

[28] D. E. Taylor (1992). *The geometry of classical groups*, Sigma Series in Pure Mathematics, Heldermann Verlag Berlin, ISBN 978-3885380092. .

[29] Tendai M. M. Shumba (2014). On the existence of self dual codes invariant under permutation groups. *Masters Thesis*, University of KwaZulu Natal.

[30] J. D. Key, J. Moori (2008). Correction to: Designs, codes and graphs from the janko groups J_1 and J_2 ". *Journal of Combinatorial Mathematics and Combinatorial Computing*, Vol 64, 137 - 153.

[31] J. D. Key, J. Moori and B. G. Rodriguez (2003), On some designs and codes from primitive representations of some finite simple groups. *Journal of Combinatorial Mathematics and Combinatorial Computations*, Vol 45, 3 - 19.

[32] R. A. Wilson, R. A. Parker, J.N. Bray, Online Atlas of Finite Group Representations, Version 3.004, http://brauer.maths.qmul.ac.uk/Atlas/V3/Classic/$S_8(2)$. Accessed on 2^{nd} February 2017.

[33] L. Chikamai, J. Moori, B. G. Rodrigues (2012), 2 - modular representations of the alternating group A_8 as binary codes. *Glssnicki Mathematicki*, Vol 47(67), 225 - 252.

[34] L. Chikamai, J. Moori, B. G. Rodrigues (2014), 2 - modular codes admiting the simple group $L_3(4)$ as an automorphism group, *Utilitas Mathematika*, Vol 95, 357 - 399.

[35] L. Chikamai, J. Moori, B. G. Rodrigues (2014), Binary codes from 2 - (64, 28, 12) designs and their orbit matrices, *JCMCC*, Vol 90, 285 - 298.

[36] L. Rukaria, L. Chikamai, I. Kamuti (2017), Linear codes obtained from the Projective symplectic group PsP (8, 2), 2^{nd} *Interdisciplinary International conference of Kibabii University.*

[37] L. Rukaria, L. Chikamai, I. Kamuti (2018), Binary codes from the Projective symplectic group $S_8(2)$, *International Journal of Engineering and Mathematical Sciences*, Vol 14, Issue 1, 10 - 23.

Appendices

A] Some Magma Routines

i) //Submodules from the Permutation Module//

$g1 := PermutationModule(G, GF(8)); g1;$

$m := Submodules(g1); \#m;$

$[\#m\,[i] : i\ in\ [1..\#m]]\,;$

ii) //Designs of codewords//

$wt := WeightDistribution(A);$

$wt := x; wt;$

$wds := Words(A, wt); \#wds;$

$D := Design < 1, Length(A) | wds >; D;$

$aut := AutomorphismGroup(D);$

$FactoredOrder(aut);$

$cf := CompositionFactors(aut); cf;$

iii) `//moori method 1 for designs// no of orbits`

$st := Stabilizer(G, 1);$

$orbs := Orbits(st); \#orbs;$

$[\#orbs\,[i] : i\ in\ \ [1..\#orbs]]\,;$

$v := Index(G, st);$

$edg := 1, Setseq(orbs[2])[1]^G;$

$blox := Setseq(orbs[2]^G);$

$des := Design < 1, v | blox >; des;$

iv) //code from design//

$A := LinearCode(des, GF(2));$

$Dimension(A);$

$[Length(A), Dimension(A), MinimumWeight(A)]$;

v) //Finding a regular connected graph//

$st := Stabilizer(G, 1); orbs := Orbits(st); \#orbs; [\#orbs\,[i] : i\ in\ [1..\#orbs]]$;

$v := Index(G, st)$;

$edg := \{1, Setseq(orbs\,[2])[1]\}^G$;

$gr := Graph < v|edg >$;

$\#edg$;

$Valence(gr)$;

$Girth(gr)$;

$Diameter(gr)$;

$Vertices(gr)$;

$\#Vertices(gr$;

vi) //Lattice Diagram//

$g1 := PermutationModule(G, GF(2)); g1$;

$SubmoduleLattice(g1)$;

$//Maximalsubgroupsof G//maxes := MaximalSubgroups(G); \#maxes$;

$\left[Index\left(G, maxes\,[i]'\,subgroup\right) :\ i\ in\ [1..\#maxes]\right]$;

$a1, a2, a3 := CosetAction(G, maxes\,[1]'\,subgroup)$;

$st := Stabilizer(a2, 1); st$;

$cf := CompositionFactors(st); cf$;

$orbs := Orbits(st); \#orbs$;

$[\#orbs\,[i] : i\ in\ [1..\#orbs]]$;

`vii) //Accessing other representations from the smallest//using method 1`

$M := MaximalSubgroups\,(G)\,; M$;

$H := M\,[10]'\,subgroup$;

$a1, a2, a3 := CosetAction\,(G, H)\,$;

$st := Stabilizer\,(a2, 1)\,; st;$

$orbs := Orbits\,(st)\,; \#orbs;$

$[\#orbs\,[i] :\ i\ in\,[1..\#orbs]]\,;$

$v := Index\,(a2, st)\,;$

$edg := \{1, Setseq\,(orbs\,[5])\,[1]\}^a 2;$

$blox := Setseq\,(orbs\,[5]^a\,2)\,;$

$des := Design < 1, v|blox >;$

$des;$

$A := LinearCode\,(des, GF\,(2))\,;$

$Dimension\,(A)\,;$

$gr := Graph < v|edg >;$

$\#edg;$

$\#Vertices\,(gr)\,;$

$Valence\,(gr)\,;$

$Girth\,(gr)\,;$

$Diameter\,(gr)\,;$

B] Weight distribution of some Codes

Weight Distribution for $\mathbf{C}_{120,4}$

$[< 0, 1 >, < 8, 11475 >,$

$< 12, 1542240 >, < 14, 23500800 >,$

$< 16, 1014831405 >, < 18, 30799104000 >,$

$< 20, 859154486400 >, < 22, 18368549591040 >,$

$< 24, 316442252860335 >, < 26, 4439687079905280 >,$

$< 28, 51337801937530560 >, < 30, 494022948157777920 >,$

$< 32, 3989050260878100285 >, < 34, 27219364278781409280 >,$

$< 36, 157915538559835116160 >, < 38, 783063385496035338240 >,$

$< 40, 3334043324131083471159 >, < 42, 12236440773079964252160 >,$

$< 44, 3884358980370135495312 0 >, < 46, 1069605975916954996531 20 >,$

$< 48, 2561175604618302375682 65 >, < 50, 5343970648294612163174 40 >,$

$< 52, 9732798402515189957491 20 >, < 54, 1549357941059149437726720 >,$

$< 56, 2158034528228505165615315 >, < 58, 2631940164743945002536960 >,$

$< 60, 2811864096750561877401216 >, < 62, 2631940164743945002536960 >,$

$< 64, 2158034528228505165615315 >, < 66, 1549357941059149437726720 >,$

$< 68, 9732798402515189957491 20 >, < 70, 5343970648294612163174 40 >,$

$< 72, 2561175604618302375682 65 >, < 74, 1069605975916954996531 20 >,$

$< 76, 3884358980370135495312 0 >, < 78, 1223644077307996425216 0 >,$

$< 80, 3334043324131083471159 >, < 82, 783063385496035338240 >,$

$< 84, 157915538559835116160 >, < 86, 27219364278781409280 >,$

$< 88, 3989050260878100285 >, < 90, 494022948157777920 >,$

$< 92, 51337801937530560 >, < 94, 4439687079905280 >,$

$< 96, 316442252860335 >, < 98, 18368549591040 >,$

$< 100, 859154486400 >, < 102, 30799104000 >,$

$< 104, 1014831405 >, < 106, 23500800 >,$

$< 108, 1542240 >, < 112, 11475 >,$

$< 120, 1 >]$

Weight Distribution for $\mathbf{C}_{120,5}^{\perp}$

$[< 0, 1 >, < 8, 11475 >,$

$< 12, 1542240 >, < 14, 23500800 >,$

$< 16, 1014831405 >, < 18, 30799104000 >,$

$< 20, 859154486400 >, < 22, 18368549591040 >,$

$< 24, 316442252860335 >, < 26, 4439687079905280 >,$

$< 28, 51337801937530560 >, < 30, 494022948157777920 >,$

$< 32, 3989050260878100285 >, < 34, 27219364278781409280 >,$

$< 36, 157915538559835116160 >, < 38, 783063385496035338240 >,$

$< 40, 3334043324131083471159 >, < 42, 12236440773079964252160 >,$

$< 44, 3884358980370135495312 0 >, < 46, 1069605975916954996531 20 >,$

$< 48, 2561175604618302375682 65 >, < 50, 5343970648294612163174 40 >,$

$< 52, 9732798402515189957491 20 >, < 54, 1549357941059149437726720 >,$

$< 56, 2158034528228505165615315 >, < 58, 2631940164743945002536960 >,$

$< 60, 2811864096750561877401216 >, < 62, 2631940164743945002536960 >,$

$< 64, 2158034528228505165615315 >, < 66, 1549357941059149437726720 >,$

$< 68, 9732798402515189957491 20 >, < 70, 5343970648294612163174 40 >,$

$< 72, 2561175604618302375682 65 >, < 74, 1069605975916954996531 20 >,$

$< 76, 3884358980370135495312 0 >, < 78, 1223644077307996425216 0 >,$

$< 80, 3334043324131083471159 >, < 82, 783063385496035338240 >,$

$< 84, 157915538559835116160 >, < 86, 27219364278781409280 >,$

$< 88, 3989050260878100285 >, < 90, 494022948157777920 >,$

$< 92, 51337801937530560 >, < 94, 4439687079905280 >,$

$< 96, 316442252860335 >, < 98, 18368549591040 >,$

$< 100, 859154486400 >, < 102, 30799104000 >,$

$< 104, 1014831405 >, < 106, 23500800 >$

$, < 108, 1542240 >, < 112, 11475 >,$

$< 120, 1 >] >$

Weight Distribution for $\mathbf{C}_{120,6}^{\perp}$

$[< 0, 1 >, < 8, 11475 >,$

$< 12, 3065440 >, < 14, 45434880 >,$

$< 16, 2001865005 >, < 18, 62140323840 >,$

$< 20, 1715893070976 >, < 22, 36737072547840 >,$

$< 24, 632911787191215 >, < 26, 8879328482088960 >,$

$< 28, 102675396808125120 >, < 30, 988046965808379904 >,$

$< 32, 7978098219211806525 >, < 34, 54438732758117836800 >,$

$< 36, 315831064398276004480 >, < 38, 1566126818463667353600 >,$

$< 40, 6668086473106355550519 >, < 42, 24472882199005877790720 >,$

$< 44, 7768717737106430657440 >, < 46, 213921201657283426897920 >,$

$< 48, 512235105284831850798345 >, < 50, 106879416183626028521 4720 >,$

$< 52, 194655962279932415494400 >, < 54, 309871597357303636150 2720 >,$

$< 56, 431606892840897303330 4275 >, < 58, 526388048690675596056 5760 >,$

$< 60, 562372802471367096483 1872 >, < 62, 526388048690675596056 5760 >,$

$< 64, 431606892840897303330 4275 >, < 66, 309871597357303636150 2720 >,$

$< 68, 194655962279932415494400 >, < 70, 106879416183626028521 4720 >,$

$< 72, 512235105284831850798345 >, < 74, 213921201657283426897920 >,$

$< 76, 7768717737106430657440 >, < 78, 2447288219900587779 0720 >,$

$< 80, 6668086473106355550519 >, < 82, 156612681846366735 3600 >,$

$< 84, 315831064398276004480 >, < 86, 54438732758117836800 >,$

$< 88, 7978098219211806525 >, < 90, 988046965808379904 >,$

$< 92, 102675396808125120 >, < 94, 8879328482088960 >,$

$< 96, 632911787191215 >, < 98, 36737072547840 >,$

$< 100, 1715893070976 >, < 102, 62140323840 >,$

$< 104, 2001865005 >, < 106, 45434880 >,$

$< 108, 3065440 >, < 112, 11475 >,$

$< 120, 1 >]$

C] Publications

i) **Linear Codes Obtained from the Projective Symplectic Group $PsP(8,2)$**

ISBN: 978 - 9966 -59 - 011 - 4

Abstract

We discuss some binary codes constructed from the primitive representation of degree 120 from the Projective Symplectic Group. Some of these codes have interesting properties. We establish some properties of these codes and nature of codewords.

Mathematics Subject Classification: 05B05, 20D45, 94B05

Key Words: Code, Design, Projective Symplectic Group, Self Orthogonal Codes, Cyclic Code, Block Code, Automorphism Group.

ii) **Binary Codes from the Projective Symplectic Group $S_8(2)$**

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

Abstract

We find all of the binary codes constructed from the primitive permutation representation of the projective symplectic group $S_8(2)$ of degree 255. It is shown that in total we have 76 non - trivial and non - isomorphic codes.The properties of the codes with small dimension are given and links with modular representation theory established. Further from the support of the codewords, we construct the 1 and 2 - designs associated to the code and the graphs of the designs.

Key Words: Code, Design, Graph, automorphism group, projective symplectic group.