2-MODULAR REPRESENTATIONS OF UNITARY GROUP $U_3(4)$ AS LINEAR CODES

Janet Lilian Maina

A thesis submitted in partial fulfilment for the requirements of the award of the degree of Master of Science in Pure mathematics of Kibabii University.

2019

Declaration

The research reported in this thesis was done under the supervision of Dr. Lucy Chikamai, Mathematics Department, Kibabii University and Dr. Lydia Njuguna, Mathematics Department, Kenyatta University and it is the author's original work prepared with no other than the indicated sources and support and has not been presented elsewhere for a degree or any other award.

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

Maina Lilian Janet

MSC/PM/002/15

Declaration and Approval

We the undersigned certify that we have read and hereby recommend for acceptance of Kibabii University a thesis entitled,"2-Modular Representations of the Unitary Group $U_3(4)$ as Linear Codes."

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

Dr. Lucy Chikamai.

Department of Mathematics

Kibabii University.

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

Dr.Lydia Njuguna

Department of Mathematics

Kenyatta University

Copyright

Dedication

I dedicate this thesis to my lovely children Wayne Wekesa and Delight Nangami.

Acknowledgment

I would like to thank the almighty God for giving me life and grace that has enabled me do this work. I wish to register a heartfelt gratitude by acknowledging the support, advice and profound efforts of my supervisors Dr. Lucy Chikamai and Dr. Lydia Njuguna. I sincerely thank my lecturers Prof. Shem Aywa, Dr. Achiles Simiyu and Dr. Benard Okello for course work.

I acknowledge my classmate Yvonne Kariuki for the encouragement and teamwork. I appreciate Kibabii University for offering me a chance to pursue my dream in the institution. I extend my sincere gratitude to my family especially my loving husband Simon Wamalwa for his encouragement, understanding and support during the entire period of study.

Abstract

A monumental achievement in group theory was done with the announcement of the completion of classification of simple finite groups in 2004. The proof of this work which was termed, a theorem, consists of tens of thousands of pages in several hundred journal articles written by about 100 authors, published between 1995 and 2004. Such voluminous work cannot be understood by any single person. Attempts to simplify the proof has already been embarked on. It is thought that a knowledge of internal structures associated with the groups and more so representation theoretic methods, could go along way to help simplify the proof. This has sparked research of combinatorial objects like codes obtained from groups and their interplay. This thesis is a study of linear binary codes obtained from primitive permutation representations of the simple finite classical group $U_3(4)$. Using the established magma databases and the Meataxe software, we consider for each primitive representation over $\mathbb{F}_2$, the permutation module obtained from the action of the group on the cosets of its maximal subgroups and the subsequent maximal submodules. Each submodule constitutes a binary code invariant under the group. In this thesis we study linear binary codes, designs and graphs obtained from the group $U_3(4)$. Using modular theoretic methods , we construct and enumerate all linear binary codes and designs from primitive permutation representations of degrees 208 and 416 and classify most of the codes. Furthermore, we determine their properties and establish the interplay between these codes and other combinatorial objects like designs and graphs. In the process, we have uncovered the lattice structure of the submodules. We have also determined the full automorphism groups of the codes and designs. Codes are applied in many areas particularly in error correction, storage and transmission of data. The properties of a code determines its usage. We found some codes with good parameters. We found some self-orthogonal, doubly even codes, irreducible and decomposable codes.

Symbols and abbreviations

Ω	A set
A^*	Conjugate transpose of A
$\emptyset$	Empty set
$\mathbb{F}$	A Field
$\mathbb{F}q$	The Galois Field of q elements
$\mathbb{F}G$	Group ring of G over F
G	Group
$\|G\|$	Order of a group G
K $\leq\leqslant$ G	K is a subgroup of G
H $\cong$ G	H is Isomorphic to G
$[n, k, d]_q$	A q-ary code of length n and dimension k and minimum distance d
$[n, k]_q$	A q-ary code of length n, dimension k
$(\mathbb{D}, \mathbb{P}, \mathbb{I})$	An incidence structure with P points and B blocks
$GL(V)$	General linear group over V
dim(V)	The dimension of a vector space V
S_n	The symmetric group on n symbols
$Aut(C)$	Automorphism group of a code
$U_3(4)$	Unitary group with the order 62,400
V	Vector space

Table of Contents

Chapter 1

Introduction

This thesis is a study of linear binary codes, designs and graphs obtained from primitive permutation representations of the Unitary group $U_3(4)$. The reliability of a communication system may depend on error-correcting codes and the decoding algorithm being used [19,23]. Codes are used for storage and transmission of data in computer systems. Graphs can be used to measure regularity of events, track events and detect the level of corruption in a system . Designs on the other hand can be used in sampling techniques by Statisticians.

The general objective of this study was to study linear binary codes, designs and graphs preserved by the group $U_3(4)$. The specific objectives of the study were to construct and enumerate G - invariant codes and determine some of their properties, determine t-designs using codewords of the codes and their primitivity and construct symmetric 1-designs and regular connected graphs preserved by the primitive groups using a series of computer programs in Magma.

A lot of studies have been done on the external Structures of Simple groups which was completed in 1981 and documented in 1983 by Daniel Gorenstein. The study of the underlying structures of simple finite groups is little known and thus not complete. Brooke in [4, 5] found all codes from the primitive permutation representations of the simple groups $PSU_4(2)$ and $PSU_3(3)$. In particular they examined all binary codes arising from primitive permutation representations of these groups. The authors in [9] enumerated all

non-trivial codes from the 2-modular representations of simple group A_8 using a chain of maximal submodules of a permutation module induced by the action of A_8 on objects such as points, Steiner S(3, 4, 8) systems, duads, bisections and triads.The results revealed the the underlying structure of A_8.

The group $U_3(4)$ falls under the classical groups. This group has been classified in terms of maximal subgroups. Much information is known on classical groups after the simple finite group classification. The proof of classification theorem consists of tens of thousands of pages in several hundred journal articles written by about 100 authors, published between 1955 and 2004 and is not understood by many people. It is generally understood that the knowledge of internal structures could simplify the proof of this theorem of the classification problem.

This thesis is organised into four chapters. Chapter one is the introduction that gives the general overview of coding theory, statement of the problem, general and specific objectives and significance of the study. In chapter two, preliminary materials and results on groups and combinatorial structures that are used in this thesis are discussed.
In chapter three, two methods of construction of codes and designs are discussed. In the first method, a group G acts on maximal subgroups(from the atlas) over a finite field with two elements to obtain a permutation module. This permutation module decomposes into maximal submodules using meat axe program. These submodules are codes invariant under this group. In the second method, a group G acts on a primitive permutation representation to obtain a maximal subgroup which is a point stabilizer in G. From the orbits of the point stabilizer, symmetric 1- designs and consequently from the designs, the desired codes are constructed.

In chapter four, we constructed and enumerated all G-invariant codes from primitive permutation representation of degrees 208 and 416. We uncovered the lattice structure. Properties of the linear binary codes were studied. We found 10 self orthogonal codes of length 208, 4 doubly even codes of length 208, two irreducible codes [208, 64] and [208 ,16, 72]. We also found 17 decomposable codes of dimensions 91, 90, 90, 90, 81, 80, 79, 78, 78, 78, 67, 66, 66, 66, 65, 55 and 17. There were 7 reducible codes of dimension 89, 77, 65, 54, 54 , 54 and 53 . There were also 6 non-isomorphic self dual [416, 208] codes of length 416. We determined t-designs using weights of codewords of some linear binary codes of length 208. The designs 1-(208, 72, 144), 1-(208, 120, 120), 1-(208, 72, 144 and 1-(208, 136, 272) were primitive. Others were not primitive. Symmetric 1- designs were determined from the primitive permutation representation of degrees 208, 416 and 1600. It was found that the automorphism group was either $2^2 : U_3 4$, $U_3 4$, $2 : U_3 4$ or $2 : A_{208}$.

Chapter 2

Basic Concepts

In this chapter, we discuss basic concepts on groups and combinatorial structures that are used in this thesis. For additional information, [7, 12, 13, 18, 19, 21, 22,23, 29, 30, 31, 33, 34, 37] can be read.

2.1 Groups

Definition 2.1.1. *A group is a set G together with a binary operation*

$(a, b) \mapsto a * b : G \times G \to G$ *satisfying the following conditions:*

$G1$*: (associativity) for all* $a, b, c \in G$,

$(a * b) * c = a * (b * c)$;

$G2$*: (existence of a neutral element) there exists an element* $e \in G$ *such that*

$a * e = a = e * a$

for all $a \in G$,

$G3$*: (existence of an inverse) for each* $a \in G$, *there exists an* $a^{-1} \in G$ *such that*

$a* a^{-1} = e = a^{-1} *a$.

The aim of this section is to bring together a selection of mostly recent results on groups important in subsequent chapters . The background materials and results on groups can be found in [7, 22, 30, 31,35].

2.1.1 Simple groups

A simple group is a non-trivial group whose only normal subgroups are the trivial group and the group itself [34]. A subgroup H of a group G is called normal if $gH = Hg$ for all $g \epsilon G$. Every finite simple group is isomorphic to one of the following groups: A cyclic group with prime order, an alternating group of degree at least 5, a simple group of Lie type and the 26 sporadic simple groups [29].

2.1.2 Permutation Groups

Definition 2.1.2. *The symmetric group on a set Ω is the group S_Ω of all permutations of Ω. If Ω is a finite of cardinality n , then S_Ω is often denoted by S_n . A permutation group G on a set Ω is a subgroup of S_Ω.*

Definition 2.1.3. *Let G be a group and Ω be a set. An action G on Ω is a function which associates to every $\alpha \in \Omega$ and $g \in G$ an element α^g of Ω such that, for all $\alpha \in \Omega$ and all $g, h \in G$, $\alpha^e = \alpha$, $(\alpha^g)^h = \alpha^{gh}$.*

2.1.3 Automorphism Groups

The automorphism of a group G, denoted by Aut (G) is the set of all automorphisms of G, under the operation of composition. i.e It is an isormorphism $G \to G$.

Lemma 2.1.4. *Let g be any element of the group G. Define a map $\phi_g : G \to G$ by $\phi_g(x) = gxg^{-1}$ for all $x \in G$. Then $\phi_g$an automorphism of G , is known as an inner automorphism corresponding to g.*

Proof. ϕ_g is a homomorphism , since

$$\phi_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \phi_g(x)\phi_g(y).$$

The inner automorphism $\phi_{g^{-1}}(x) = g^{-1}xg$ clearly inverts ϕ_g. Since ϕ_g is an invertible homomorphism,it is an automorphism.

The set of inner automorphisms of G is denoted Inn G. □

Remark 2.1.5. *If G is abelian, then*

$$\phi_g(x) = gxg^{-1} = gg^{-1}x = x = id(x).$$

That is, in an abelian group, the inner automorphisms are trivial. More generally, $\phi_g = id.$ if and only if $g \in Z(G)$.

The existence of automorphism for a group G provides rich arrangement of elements in the group and thus allowing the use of deeper results from group theory.

2.1.4 Primitive Groups

If G is a permutation group on a set Ω ; then a partition P of Ω is said to be $G-$invariant (and G is said to preserve P) if the elements of G permute the blocks (elements of P) of P blockwise. The blocks of a $G-$invariant partition are called blocks of imprimitivity for G. If G is transitive on Ω then all blocks of a $G-$invariant partition have the same cardinality and G acts transitively on P . Moreover, every permutation group G on Ω preserves two partitions namely Ω and $\{\{\alpha\}|\alpha \in \Omega\}$; these are called trivial partitions of Ω and their blocks Ω and α are called trivial blocks of imprimitivity. All other blocks of Ω are said to be non-trivial.

A permutation group G is said to be primitive on Ω if G is transitive on Ω and the only $G-$ invariant partitions of Ω are the trivial partitions. Also G is said to be imprimitive on Ω if G is transitive on Ω and G preserves some non-trivial partition of Ω.

Theorem 2.1.6. *(Characterization of primitive permutation groups) Let G be a transitive*

permutation group on a set Ω *. Then* G *is primitive if and only if for each* $\alpha \in \Omega$ *; the stabilizer* G_α *is a maximal subgroup of* G*.*

Proof. See [3] □

By the above theorem it follows that, if we know all the maximal subgroups of a group G then we know all the primitive actions. We have also seen that a transitive action is equivalent to an action on the coset space G/H. In view of this, we conclude that a primitive action is equivalent to the left multiplication action of G on the coset space G/H where H is a maximal subgroup of G. We shall apply this fact to find designs and codes from the primitive permutation representations from finite group in the later chapters.

2.2 Combinatorial Structures

This section focuses on combinatorial structures which are important in subsequent chapters. For more information on codes and combinatorial structures, we see [12, 22].

2.2.1 Linear codes

In order to define codes that we can encode and decode efficiently, we add more structure to the codespace. We are mainly interested in linear codes where we develop the basics of linear codes. We let $\mathbb{F}_q$ be a finite field of order q and its vector space of $n-$tuples of elements by $V = \mathbb{F}_q^n$.

$x \cdot y = xy^t$ where y^t is the transpose of y is the standard dot product of x and y in V. The subspace spanned over $\mathbb{F}_q$ by the subset $\{x_1, x_2, ..., x_n\}$ of V will be denoted by $\langle x_1, x_2, ..., x_n \rangle$ [35].

Definition 2.2.1. *Let* $\mathbb{F}$ *be a set of* q *elements. A* $q-$*ary code* C *is a set of finite sequences*

of the elements of $\mathbb{F}$ *, called codewords. i.e* $C = w_1, ..., w_i \subseteq (\mathbb{F}_q)^n$. *Where* $\mathbb{F}_q$ *is a set of* q *symbols and* n *is the length of each element of the code. If all the codewords are sequences of the same length* n *, then* C *is called a block code of length* n.

The set $(\mathbb{F}_q)^n$ is endowered with the Hamming distance defined as follows:

Definition 2.2.2. *Let* C *be a* q*-ary code and* x *and* y *words in* C. *The Hamming distance between* x *and* y *, denoted by* $d(x, y)$ *, is the number of positions in which the words* x *and* y *differ.*
i.e $d(x, y) = |i : x_i \neq y_i|$.

Definition 2.2.3. *The minimum distance* d *of* C *is the smallest Hamming distance between any two distinct words in* C *, that is* $d = min(x, y)|x, y \in C, x \neq y\}$.

It is important to note that the minimum distance of a code is an important parameter that measures the capacity to detect and to correct errors.

Lemma 2.2.4. *Let* C *be a code with minimum distance* d.*If* $d \geqslant s + 1 \geqslant 2$, *then* C *can be used to detect up to* s *errors.If* $d \geqslant 2t + 1$, *then* C *can be used to correct up to* t *errors.*

Definition 2.2.5. *The Hamming weight* $w(c)$ *of a codeword* c *is the number of nonzero components in the code word.*

Definition 2.2.6. *A linear code* C *of length* n *over the field* $\mathbb{F}_q$ *is a subspace of* $\mathbb{F}_q^n$. *We write* $C = [n, k]_q$ *where* $dim(C) = k$.

Every linear code of length n over $\mathbb{F}_q$ contains the zero vector $0 \in \mathbb{F}_q^n$ whose entries are all the zero elements of the field. If $d(x, y)$ is the Hamming distance of x, y in C, then $x - y$ is in C and $d(x, y) = d(0, x - y)$. This implies that for a linear code, the minimum distance d of the code is the smallest number of non-zero entries of the codewords of the code.

Definition 2.2.7. *A linear binary (n, k) code C is a k -dimensional subspace of the n-dimensional vector space over $G\mathbb{F}(2)$.*

Definition 2.2.8. *Let C be a $[n, k]_q$ code. A generator matrix for C denoted by G is a $k \times n$ matrix obtained from any k linearly independent vectors of C.*

NOTE: The generator matrix can be used for a linear code to encode a message.

Definition 2.2.9. *Let C be a linear code of length n over the field $\mathbb{F}_q$. The weight of a word x in C is defined to be $wt(x) = d(0, x)$.*

It is noted that the minimum distance of a linear code C is the minimum weight of the code. When the minimum weight d of a linear code $C = [n, k]$ is known, we write $C = [n, k, d]_q$. For a linear code $C = [n, k, d]_q$, we have the Singleton bound $d \leq n-k+1$. Let C be a linear $[n, k, d]_q$ code. We let $A_i(c)$ denote the number of codewords at distance i from a codeword $c \in C$. The numbers $A_i(c)$ where $0 \leq i \leq n$, are called the weight distribution of C with respect to c. The weight distribution classifies codewords according to the number of non-zero coordinates.

Definition 2.2.10. *Let C be a $[n, k]_q$ code. The dual code or orthogonal code of C denoted by $C^{\perp}$ is the orthogonal under the standard inner product, that is $C^{\perp} = \{v \in \mathbb{F}_q^n | (v, c) = 0$ for all $c \in C$.*

For $dim(C) + dim(C^{\perp}) = n$, $C^{\perp}$ is simply the null space of a generator matrix for C. Taking G to be the generator matrix for $C = [n, k]_q$, a generator matrix H for $C^{\perp}$ is a $(n - k) \times n$ matrix that satisfy $GH^T = 0$, that is $c \in C$ if and only if $cH^T = 0 \in \mathbb{F}_q^{n-k}$.

Definition 2.2.11. *Any generator matrix H for $C^{\perp}$ is called a parity-check or check matrix for C. If G is written in the standard form $[I_k|A]$, then $H = [-A^T|I_{n-k}]$ is a check matrix for the code with generator matrix G.*

Theorem 2.2.12. *Let H be a check matrix for a $[n, k, d]_q$ code C. Then every choice of $d-1$ or fewer columns of H forms a linearly independent set. Moreover if every $d-1$ or fewer columns of a check matrix for a code C are linearly independent, then the code has minimum weight at least d.*

Proof. See [1,Theorem 2.3.1] □

Theorem 2.2.13. *If C is a $q-$ary linear code of dimension k of $\mathbb{F}^n$, then dual code of C denoted by $C^\perp$ is the orthogonal compliment of C in $\mathbb{F}^n$; that is*
$C^\perp = x \in \mathbb{F}^n | (x, y) = 0 \forall x \in C.$

If $C \subseteq C^\perp$, then C is self-orthogonal and if $C = C^\perp$, then C is self-dual. A binary code is doubly-even if all its codewords have weight divisible by 4. Thus doubly even codes are self orthogonal.

Definition 2.2.14. *An isomorphism of C onto itself is called an automorphism of C if C is a linear code of length n over $\mathbb{F}_q$. An automorphism group of C is the set of all automorphisms of C and is denoted as $Aut(C)$. Any automorphism of the code preserves each weight class of C. If $C \subseteq \mathbb{F}_q^\Omega$, then the automorphism group of C is a subgroup of S_n.*

The existence of automorphism for C can provide a richer structure for the code and allow the use of deeper results from group theory.

2.2.2 Designs

Combinatorial design theory deals with the problem of existence of arrangement of objects into subsets of the same size such that any t of these objects will belong to the same number of common subsets [1,2].

Definition 2.2.15. *An incidence structure is a triple $I = (P, B, I)$, P is called the point set, B is called the block set and I is an incidence relation between P and B. The elements of I are called flags.*

Definition 2.2.16. *The structure $D = (P, B, I)$, where P is the point set, B is the block set and I is the incidence is $a, t-(v, k, \lambda)$ design, where $|P| = v$. When a design D has the same number of points and blocks , it is called symmetric . A $t-(v, k, 1)$ design is called a Steiner System. A $2-(v, 3, 1)$ Steiner system is called a Steiner Triple System. A $t-(v, 2, \lambda)$ design D can be regarded as a graph with ρ as points and β as edges.*

Definition 2.2.17. *$D^t = (B^t, P^t, I^t)$, is the dual structure of D for $P^t = B, B^t = P$ and $I^t = \{(B, p)|(p, B) \in I\}$.*

Note: Given a labelling on the point and block sets of D the transpose of an incidence matrix for D is an incidence matrix for D^t. We will say that the design is symmetric if it has the same number of points and blocks, and self-dual if it is isomorphic to its dual.

We shall be concerned mostly with t- designs and symmetric 1-(v, k, k) designs. Theorem 4.1.1 in [15] justifies the construction of t- designs. In Theorem 3.3.1 we give a method to construct symmetric 1-(v, k, k) designs. These designs will result from the primitive permutation representations of groups.

2.2.3 Graphs

A graph G is an ordered pair (V, E) , where V is a non-empty finite set of vertices and E is a set of pairs of distinct vertices in G , called edges. The valency of a vertex is the number of edges containing the vertex. A graph is regular if all the vertices have the same valence[1,2, 21].

A connected graph on N vertices is said to be strongly regular with parameters (N, K, λ, μ) if it is regular with valency K and if the number of vertices joined to two given vertices is λ or μ according as the two given vertices are adjacent or non-adjacent;we shall always exclude the null and complete graphs. If C is a $[n, k]_q$ code, then the code C is related to a strongly regular (N, K, λ, μ) graph where the Eigen values of the adjacency matrix A of the graph are K, ρ_1, ρ_2; where:-

$$\rho_1, \rho_2 = 1/2[\lambda_2 - \mu] \pm \sqrt{d}$$
$$\text{and } d = (\lambda - \mu)^2 + 4(K - \mu).$$

We shall be concerned with how codes interplay with graphs.

2.3 Representations

In this section, we are interested in preliminary results of representations theory that will be useful in subsequent chapters.

Definition 2.3.1. *A homomorphism $\rho : G \longrightarrow GL(n, \mathbb{F})$ is said to be a matrix representation of G of degree n over the field $\mathbb{F}$ if G is a finite group and V is a vector space of dimension n over the field $\mathbb{F}$. The column space, $\mathbb{F}^{n\times 1}$ of ρ is called module ρ representation. ρ is called an ordinary representation if the characteristic of $\mathbb{F}$ is zero and is called a modular representation if it is a representation over a field of non-zero characteristic.*

Definition 2.3.2. *Let $\rho : G \longrightarrow GL(n, \mathbb{F})$ be a representation of G over the field $\mathbb{F}$. The function $\chi : G \to \mathbb{F}$ dened by $\chi(g) = trace(\rho(g))$ is called the character of ρ.If $\varphi : G \to \mathbb{F}$ is a function that is constant on conjugacy classes of G i.e., $\varphi(g) = \varphi(\alpha g \alpha^{-1})$ for all, $\alpha \in G$ we say that φ is a class function. It is easily shown that any character χ is a class function.*

Definition 2.3.3. *Two matrix representations $\rho 1$ and $\rho 2$ of G are equivalent representations for $P \in GL(n, \mathbb{F})$ such that $\rho 2(g) = P\rho 1(g)P^{-1}$ for all, $g \in G$.*

Note: Whenever we consider a representation, it is only considered up to equivalence.

Definition 2.3.4. *Let $\rho : G \to GL(n, \mathbb{F})$ be a representation of G on a vector space $V = \mathbb{F}^n$. Let $W \subseteq V$ be a subspace of V of dimension m such that $\rho_g(W) \subseteq W$ for all, $g \in G$, then the map $G \to GL(m, \mathbb{F})$ given by $g \to \rho(g)|W$ is a representation of G called a sub representation of ρ. The subspace W is then said to be $G-$invariant or a $G-$subspace. Every representation has $\{0\}$ and V as $G-$ invariant subspaces. These two subspaces are called trivial or improper subspaces.*

Definition 2.3.5. *We define a linear representation V of G over $\mathbb{F}$ as a homomorphism.*
$\emptyset : G \to GL(V)$
if $\mathbb{F}$ is a field of characteristic p , V is an $\mathbb{F}$ vector space and G is a finite group of order n.

We say that the representation is faithful if $\emptyset$ is injective. Representations are similar or equivalent if they correspond to isomorphic $\mathbb{F}G-$ modules. A module M is irreducible or simple if the only submodules are M and 0. If not then M is reducible. M is decomposable if there exist non-zero sub modules M_1 and M_2 such that $M = M_1 \oplus M_2$. M is completely reducible if it can be written as the direct sum of irreducible sub modules [21].

Definition 2.3.6. *A representation $\rho : G \to GL(n, \mathbb{F})$ of G with representation module V is called **reducible** if there exists a proper non-zero $G-$subspace U of V and it is said to be irreducible if the only $G-$subspaces of V are the trivial ones.*

The representation module V of an irreducible representation is called simple and the $\rho-$invariant subspaces of a representation module V are called submodules of V. A

simple subspace U of V is a submodule that is isomorphic to a simple representation module and it is called a composition factor of V.

Definition 2.3.7. *Let $\rho : G \to GL(V)$ be a representation of G on a vector space V. If there exists $G-$invariant subspaces U and W such that $V = U \oplus W$ then ρ is called decomposable. If no such subspaces exist it is called indecomposable.*

Definition 2.3.8. *A completely reducible representation ρ is a direct sum of irreducible representations.*

2.4 $\mathbb{F}G$ - modules

This section describes the relationship between representations of G and $\mathbb{F}G$ - modules. Because of the one-to-one correspondence between them, we study representations via module theory. The results from $\mathbb{F}G$-modules carry over to representations.
$\rho : \mathbb{F}G \to End_{\mathbb{F}}(V)$ is a homomorphism, where $\mathbb{F}G$ is the group ring of G over $\mathbb{F}$, restricts to a representation of G. V can be regarded as a vector space over $\mathbb{F}$ and also as an $\mathbb{F}G$ -module through the homomorphism ρ.

Definition 2.4.1. *The group ring of G over $\mathbb{F}$ is the set of all formal sums of the form*
$\Sigma_{g\in G}\lambda_g g, \lambda_g \in \mathbb{F}$
with componentwise addition and multiplication if G is a finite group and $\mathbb{F}$ is a field.

Theorem 2.4.2. *There is a bijective relationship between finitely generated $\mathbb{F}G$-modules and representations of G on finite-dimensional $\mathbb{F}$-vector spaces if $\mathbb{F}$ is a field and G is a finite group.*

Proof. See [35] □

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

Definition 2.4.3. *A subspace W of V is called an $\mathbb{F}G$-submodule of V if V itself is an $\mathbb{F}G$-module.*

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

Definition 2.4.5. *V is decomposable if it can be written as a direct sum of two $\mathbb{F}G$-submodules where V is an $\mathbb{F}G$-module. V is completely reducible if it can be written as a direct sum of irreducible submodules.*

Definition 2.4.6. *A function $\tau : V \to W$ is said to be an $\mathbb{F}G$-homomorphism if τ is a linear transformation for any $v \in V, g \in G$, $\tau(gv) = g\tau(v)$ i.e., if τ sends v to w then it sends gv to gw.*

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

Proof. See [35,Theorem 3.19] □

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

$0 = V_0 \subset V_1 \subset ... \subset V_t = V$

such that for each $i \geq 1$ the factorV_{i-1}/V_i is irreducible. The integer t is called the length of the module V . If t is infinite then V is said not to have a composition series.

Chapter 3

Construction of codes, designs and graphs from primitive groups

In this chapter, we discuss methods of construction of codes, designs and graphs from primitive groups. Section 3.1 describes how to construct G-invariant codes. In section 3.2, we describe how to construct codes from maximal submodules. Section 3.3 describes how to construct designs from primitive groups. Finally section 3.4 describes how to construct codes from combinatorial designs. From these four methods, we extract algorithms that were implemented with the software package MAGMA [35]. For a more detailed account and additional information the reader is advised to consult [1, 2, 3, 7, 9, 21].

3.1 Construction of G-invariant codes

It is required that all submodules of the permutation module are determined. As such, the permutation module is decomposed into submodules. These constitutes the building blocks for the construction of a lattice of submodules where possible, thereby attaining an answer to the enumeration problem. With the characterization of these codes we get the solution to the problem of classification of the codes.

Accordingly, Maschke's Theorem gives a characterization of decomposition over a field whose characteristic is 0 or relatively prime to the order of the group. Here, the permutation module is completely reducible and can be written as a direct sum of its irreducible submodules. When the characteristic p of the field divides the order of the group i.e.,$p||G|$,we apply Krull-Schmidt's Theorem which shows that any module with finite length can be written as a direct sum of indecomposable submodules, and this decomposition is

unique up to isomorphism and the order of the summands [35]. In addition to Krull-Schmidt theorem, we have the composition series of the module which provides a way of breaking the module into simple components [35]. These concepts have been used to develop different methods to construct submodules hence codes invariant under a group.

Lemma 3.1.1. *The $G-$ invariant submodules of $\mathbb{F}_2G$ are the linear codes in $\mathbb{F}_2G$.*

Proof. Proceeds from [35, *Lemma* 6.19]

Let G be a finite permutation group acting on a finite set Ω in the usual way.

Let $V = \mathbb{F}\Omega$ be the $\mathbb{F}$ vector space with basis the elements of Ω.

Let $\rho : G \to GL(V)$ be a representation of G given by:

$$\rho(g)(x) = g(x) \ \forall g \in G \text{ and } x \in V$$

We can consider V as the $\mathbb{F}_2G-$ module obtained from ρ. Let S be as $\mathbb{F}_2G-$ submodule of the permutation module V.

By definition of $G-$ invariant code,we have:

$$(\textstyle\sum_{g\in G} \alpha_g g) \ .S \in \mathbf{S} \ \forall \ \sum_{g\in G} \alpha_g g \in F_2G \text{ and } S \in \mathbf{S}.$$

In particular,

$$g.S \in \mathbf{S} \ \forall g \in G \text{ and } S \in \mathbf{S}$$

Thus $\forall \ g \in G \ S \in \mathbf{S}$, we obtain

$$\rho(g)(S) \in \mathbf{S} \text{ or } g(S) \in \mathbf{S} \text{ and so } \mathbf{S} \text{ is } G-\text{invariant.}$$

Conversely, if $\mathbf{S}$ is $G-$invariant; then $\forall g \in G$ and $S \in \mathbf{S}$ we have $\rho(g)(S) \in \mathbf{S}$.

Therefore for scalars $\alpha_g \in \mathbb{F}_2$ we have:

$$\sum_{g \in G} \alpha_g \rho(g)\ (S) \in \mathbf{S} \text{ by linearity.}$$

This implies that

$$(\sum_{g \in G} \alpha_g g)\ .S \in \mathbf{S}.$$

□

3.2 Construction of Codes from Maximal submodules

Our point of interest is finding all $G-$invariant codes from the primitive permutation representations. We thus consider the permutation module obtained from the action of the group on the cosets of its maximal subgroups and thus explore the corresponding maximal submodules. Given a permutation group G on a finite set Ω and a finite field $\mathbb{F}$ it is often of considerable interest to know the structure of the permutation module $\mathbb{F}\Omega$ (that is, the vector space over $\mathbb{F}$ with basis Ω considered as an $\mathbb{F}G$ module). In $\mathbb{F}\Omega$, the $G-$invariant submodules equals to the linear codes[35].

For each primitive representation of a given permutation group G, we use atlas of finite groups and Magma [9] to generate permutation module over $\mathbb{F}2$ and subsequently submodules directly. Each submodule constitutes in turn the binary code that is invariant under G.

Let G be a finite group and $H = G\alpha$ where $\alpha \in \Omega$ its maximal subgroup and consider the action of G on the set of cosets $\Omega = (G, G/G\alpha)$ where $G/G\alpha = \{gG\alpha | g \in G\}$. We know

that G acts transitively and primitively in a natural way by left multiplication on Ω and the image of this action is a primitive permutation representation. The $\mathbb{F}\Omega-$ permutation module over $\mathbb{F}_q$ corresponds to this representation [35].

The Group G acts on given primitive permutation representations (from the atlas)over a finite field to base 2 to obtain permutation modules. We break down the permutation modules into submodules which are themselves the dimensions of the G-invariant codes. The $G-$invariant subspaces (i.e., submodules) of the permutation module give all the $p-$ary codes invariant under G. The codes constructed using those methods are in general subcodes[35].

3.3 Construction of symmetric 1-designs from primitive permutation groups

In this section, we describe how to construct symmetric 1-designs from primitive groups.

Theorem 3.3.1. *Let G be a finite primitive permutation group acting on the set Ω of size n . Let $\alpha \in \Omega$, and let $\triangle \neq \{\alpha\}$ be an orbit of the stabilizer G_α of α.*

If $\beta = \{\Delta^g : g \in G\}$

and, given $\delta \in \Delta$,

$\varepsilon = \{\{\alpha, \delta\}^g : g \in G\}$,

then β forms a symmetric $1-(n, |\Delta|, |\Delta|)$ design with n blocks, and ε 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 vertices of the graph, and on points and blocks of the design.

Proof. Proceeds from [21]. We have $|G| = |\Delta^G||G_\Delta|$, and clearly $G_\Delta \supseteq G_\alpha$. Since G is primitive on Ω, G_α is maximal in G, and thus $G_\Delta = G_\alpha$ and $|\Delta^G| = |\beta| = n$. This proves

that we have a $1-(n,|\Delta|,|\Delta|)$ design.

For the graph, we notice that the vertices adjacent to α are the vertices in Δ. Now as we orbit these pairs under G, we get the nk ordered pairs, and thus $nk/2$ edges, where $k=\Delta$. Since the graph has G acting, it is clearly regular, and thus the valency is k as required, i.e. the only vertices adjacent to α are those in the orbit Δ. The graph must be connected, as a maximal connected component will form a block of imprimitivity, contradicting the group's primitive action. Now notice that an adjacency matrix for the graph is simply an incidence matrix for the 1-design, so that the 1-design is necessarily symmetric. This proves all our assertions. □

Remark 3.3.2. *Notice that by forming any union L, where $\{\alpha\} \neq L \neq \Omega$, of orbits of the stabilizer of a point, including the orbit consisting of the single point, and orbit this under the full group, we obtain a symmetric 1-design.*

Lemma 3.3.3. *A design can be obtained by orbiting a union of orbits of a point-stabilizer, as described in Theorem 3.3.1 if the group G acts primitively on the points and the blocks of a symmetric 1-design D.*

Proof. See [21] □

Theorem 3.3.4. *The automorphism group of D contains G if D is a self-dual 1-design obtained by taking all the images under G of a non-trivial orbit Δ of the point stabilizer in $G's$ primitive representations, and on which G acts primitively on points and blocks.*

Proof. See [28]. □

Theorem 3.3.5. *The automorphism group of D is contained in the automorphism group of C if C is a linear code of length n of a symmetric $1-(v,k,k)$ design D over a finite field $\mathbb{F}_q$.*

Proof. See [28]. □

3.4 Construction of codes from combinatorial designs

This section describes how to construct codes from combinatorial designs. Coding theory has made many contributions to the theory of combinatorial designs. A code generated by the incidence matrix of designs has been useful in either constructing new designs or showing that certain designs do not exist, as it is for example the case of the projective plane of order 10 [28]. Coding theory has also been used to extend designs [28].

Using the knowledge about codes and the existence of designs in codes can be useful for decoding purposes. For example a binary vector x of weight w is said to determine the block of w points corresponding to the positions where x has non-zero coordinates [28]. In such case we say that vectors of a fixed weight w in a binary code of length n hold a t-design if the blocks determined by these vectors are the blocks of a t-design on n points. This means that there must exist t and A so that every set of t coordinate positions occurs as non-zero positions for exactly A vectors of weight w [28]. 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 could form a design [28].

For $D = (P, B, I)$ and any field $\mathbb{F}$, we denote the vector space of functions from P to $\mathbb{F}$ by $\mathbb{F}^p$. For $w \in \mathbb{F}^p$, the value of W at the points p is $w(p)$ in $\mathbb{F}$. The definitions below are key to the construction of the codes.

Definition 3.4.1. *The support set of a function $w \in \mathbb{F}^p$ is defined to be the subset of points in P whose images under w are non-zero , that is, $Supp(w) = p \in P|w(p) \neq 0$. The character function for a block B is denoted by V^B and defined to be:*

$$v^b(p) = \{1 if p \in B$$

$$v^b(p) = \{0 if p not \in B$$

The basis for this vector space is $v^p | p \in P$

Definition 3.4.2. *A code of a* $D = (P, B, I)$ *design is contained in the space* $\mathbb{F}_q^p$ *obtained by the characteristic functions of the blocks of* D *and is denoted by* $C_q(D)$.

The incidence vector of Q is v^Q if the point set of D is denoted by P and the block set by B, and if Q is any subset of P. Thus $C_{\mathbb{F}}(D) = \langle v^B | B \in B \rangle$ and is a subspace of $\mathbb{F}_p$. The dimension of the code $C_p(D)$ of the design D over a prime field $\mathbb{F}_p$ is the rank of the generating matrix of the code and is referred to as the p-rank of D [35].

NOTE: The minimum weight is less than the block size of D, but for the p-ary codes of geometry designs, where p is the characteristic of the underlying field of the geometry, we have equality by the work of Delsarte et al.

We are concerned with self-dual symmetric 1- (v, k, k) designs. In Theorem 3.3.1 we give a method to construct such designs. These designs will result from the primitive permutation representations of groups.

Chapter 4

Internal structures of $U_3(4)$

This chapter covers the internal structure of $U_3(4)$. The simple linear group $U_3(4)$ falls in the unitary group of degree n, denoted by $U(n)$ and is a sub group of the general linear group $GL(n, C)$. The unitary group $U(n)$ is a real Lie group of dimension n^2 [12]. The general unitary group consists of all matrices A such that $A^\star A$ is non-zero multiple of the identity matrix, and is just the product of the unitary group with the group of all positive multiples of the identity matrix. Since the determinant of a unitary matrix is a complex number with norm 1, the determinant gives a group homomorphism

$$\det: U(n) \to U(1)$$

The Unitary group $U(n)$ is non abelian for $n > 1$ [12]. There are twenty unitary groups in the atlas of finite groups. For the background on the unitary groups see [16, 17, 20, 26].

This group has order $62,400 = 2^6.3.5^2.13$. From [11], $U_3(4) \cong 2A_2(4)$. There are two ways in which G can be constructed :

1) $GU_3(4) \cong 5 \times G$: all 3×3 matrices over $\mathbb{F}_{16}$ preserving a non singular Hermitian form;

2) $PGU_3(4) \cong SU_3(4) \cong PSU_3(4) \cong G$.

We discuss the three primitive representation of degrees 208, 416 and 1600. The primitive representations are shown in table 4.1. The group $U_3(4)$ has four primitive groups of degrees 65, 208, 416 and 1600 respectively (see [11]). They are summarized in the Table below: The first, second, third and fourth columns outline the degree of the primitive

group, the structure of the maximal subgroups, the the number of orbits of the point-stabilizer and the orbit length respectively.

Table 4.1: Maximal subgroups and representation of $U_3(4)$

Degree	Maximal Subgroup	No.of orbits	Length of orbits
65	$2^{2+4} : 15$	2	1, 64
208	$5 \times A_5$	5	1,12,60(2),75
416	$5^2 : S_3$	9	1,15,25(4),75(2),150
1600	$13 : 3$	48	1,13(9),39(38)

These primitive representations may also be described in terms of the action of G on geometrical objects called isotropic point, non-isotropic point, base and $U_1(64)$. When a group G acts on given primitive permutation representation (from the atlas)over a finite field with 2 elements a permutation module is obtained.

In this chapter, we generate linear codes, designs and graphs from primitive representation of degrees 208, 416 and 1600 and discuss their properties. For a primitive representation of degree 65 , when the group G acts on the the maximal subgroup $2^{2+4} : 15$ over $\mathbb{F}_2$, the permutation module formed generates trivial submodules and designs which are not significant in this thesis.

4.1 Dimension representation of 208

A group $U_3(4)$ acts on a primitive permutation representation of degree 208 over a finite field with 2 elements to obtain a permutation module. We generate the submodules from the permutation module which represents the dimensions of the G-invariant codes.

4.1.1 G-invariant codes

Let G be a primitive representation of $U_3(4)$ of degree 208. The group G acts on non-isotropic point to generate the stabilizer $5\times A_5$. The stabilizer is a maximal subgroup of degree 208 in G. The group G acts on this maximal subgroup over $\mathbb{F}_2$ to produce a permutation module of size 208 contained in G. This permutation module is decomposed into 56 submodules. These submodules represent the dimensions of the linear binary codes of permutation module of size 208 contained in G.

A complete list of $U_3(4)-$ invariant submodules of the permutation module $\mathbb{F}_2\Omega$ of degree 208 consists of 56 submodules whose dimensions are given in Table 4.2. From the table, m represents the submodule dimension and # is the submodule number of each dimension.

Table 4.2: The number of Submodules of length 208 invariant under $U_3(4)$

m	#	m	#	m	#	m	#
0	1	67	1	118	3	144	1
1	1	77	1	119	1	153	1
16	1	78	3	127	1	154	3
17	1	79	1	128	1	155	1
53	1	80	1	129	1	191	1
54	3	81	1	130	3	192	1
55	1	89	1	131	1	207	1
64	1	90	3	141	1	208	1
65	2	91	1	142	3		
66	3	117	1	143	2		

The number of submodules of dimension $208 - m$ is the same as the number of the dimension m. In other words, the dimension of the code equals to the dimension of its dual. Using Magma, we decompose the permutation module into 56 non isomorphic submodules. The following layers form the lattice diagram.

First layer: The 208-dimensional permutation module decomposes into three submodules of dimensions 144,192 and 207.

Second layer: The 144 dimensional submodule decomposes into two submodules of dimension 128 and 143. The 192 dimensional submodule decomposes into two submodules of dimension 128 and 191. The 207 dimensional submodule decomposes into two submodules of dimension 143 and 191.

Third layer: The 128 dimensional submodule decomposes into a submodule of dimension 127. The 191 dimensional submodule decomposes into two submodules of dimension 127 and 155. The 143 dimensional submodule decomposes into a submodule of dimension 127. The 191 dimensional submodule decomposes into two submodules of dimension 127 and 155.

Fourth layer: The 127 dimensional submodule decomposes into a submodule of dimension 91 . The 155 dimensional submodule decomposes into five submodules of dimension 91, 143, 154, 154 and 154.

Fifth Layer: The 91 dimensional submodule decomposes into four submodules of dimension 79, 90, 90 and 90. The 143 dimensional submodule decomposes into five submodules of dimension 79, 131, 142, 142 and 142. The 154 dimensional submodule decomposes into three submodules of dimension 90, 142 and 153 in each case.

Sixth Layer: The 79 dimensional submodule decomposes into four submodules of dimension 67, 78, 78 and 78. The 90 dimensional submodule decomposes into two submodules of dimension 78 and 89. The 131 dimensional submodule decomposes into five submod-

ules of dimension 67, 119, 130, 130 and 130. The 142 dimensional submodule decomposes into three submodules of dimension 67, 119 and 130 in each case. The 153 dimensional submodule decomposes into two submodules of dimension 89 and 141.

Seventh Layer: The 67 dimensional submodule decomposes into four submodules of dimension 55, 66, 66 and 66. The 78 dimensional submodule decomposes into two submodules of dimension 66 and 77. The 89 dimensional submodule decomposes into one submodule of dimension 77. The 119 dimensional submodule decomposes into four submodules of dimension 55, 118, 118 and 118. The 130 dimensional submodule decomposes into three submodules of dimension 66, 118 and 129. The 141 dimensional submodule decomposes into two submodules of dimension 77 and 129.

Eighth Layer: The 55 dimensional submodule decomposes into a submodule of dimension 54. The 66 dimensional submodule decomposes into two submodules of dimension 54 and 65. The 77 dimensional submodule decomposes into submodule of dimension 65. The 118 dimensional submodule decomposes into submodules of dimension 54 and 117. The 129 dimensional submodule decomposes into submodules of dimension 65 and 117.

Ninth Layer: The 54 dimensional submodule decomposes into a submodule of dimension 53. The 65 dimensional submodule decomposes into a submodule of dimension 53. The 117 dimensional submodule decomposes into two submodules of dimension 53 and 81.

Tenth Layer: The 53 dimensional submodule decomposes into a submodule of dimension 17. The 81 dimensional submodule decomposes into three submodules of dimension 17, 65 and 80.

Eleventh Layer: The 17 dimensional submodule decomposes into two submodules of dimension 1 and 16. The 65 dimensional submodule decomposes into two submodules of dimension 1 and 64. The 80 dimensional submodule decomposes into two submodules of dimension 16 and 64.

Twelfth Layer: The 1, 16 and 64 dimensional submodules decompose in each case to a submodule of dimension 0.

Note: We have two non-isomorphic submodules of dimension 65 and two non-isomorphic submodules of dimension 143 that decomposes into different submodules.

Lattice of submodules is shown below:

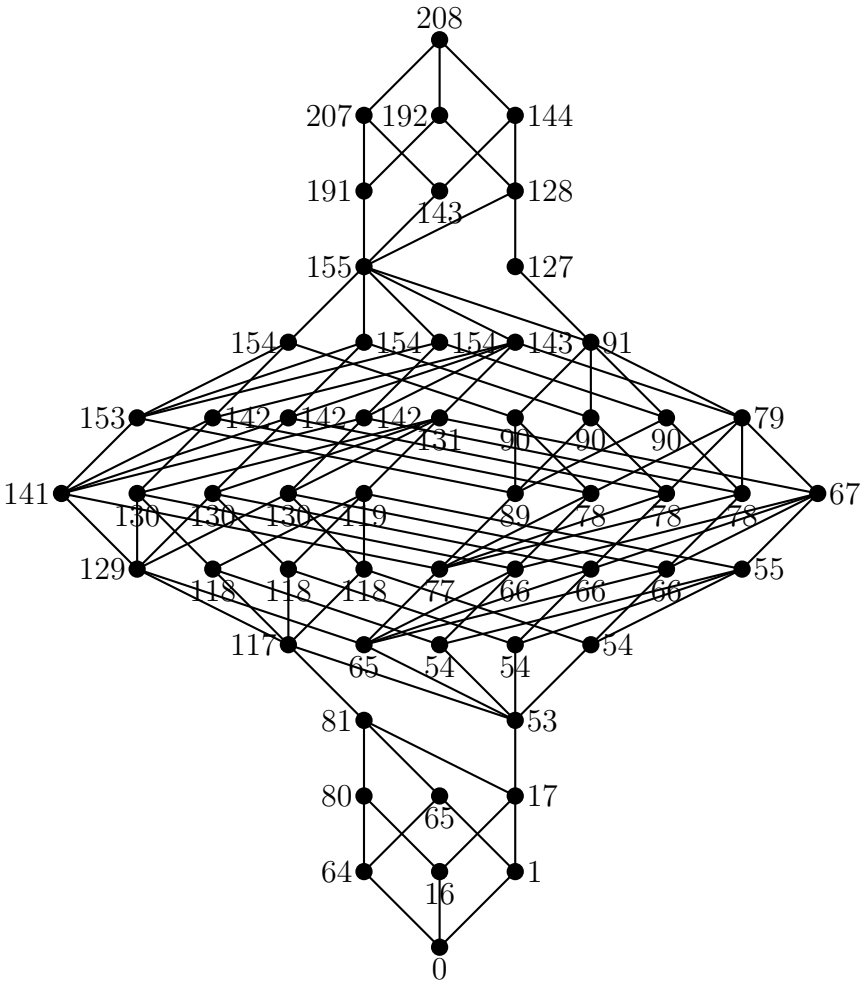

Figure 4.1: Lattice of submodules of length 208 invariant under $U_3(4)$

Remark 4.1.1. *There are 52 G-invariant codes.*

4.1.2 Binary codes

We list non trivial linear binary codes in Table 4.3. We name the linear binary codes as $C_{208,i}$ with their respective duals as $C^{\perp}_{208,i}$. For some codes, we indicate minimum distance where computations are possible.

Table 4.3: Non-trivial codes invariant under $U_3(4)$

Code	(Parameters)	Code	(Parameters)	Code	(Parameters)
$C_{208,1}$	[208,16,72]	$C_{208,19}$	[208,79]	$C^{\perp}_{208,16}$	[208,130]
$C_{208,2}$	[208,17,72]	$C_{208,20}$	[208,80,12]	$C^{\perp}_{208,15}$	[208,131]
$C_{208,3}$	[208,53]	$C_{208,21}$	[208,81,12]	$C^{\perp}_{208,14}$	[208,141]
$C_{208,4}$	[208,54]	$C_{208,22}$	[208,89]	$C^{\perp}_{208,13}$	[208,142]
$C_{208,5}$	[208,54]	$C_{208,23}$	[208,90]	$C^{\perp}_{208,12}$	[208,142]
$C_{208,6}$	[208,54]	$C_{208,24}$	[208,90]	$C^{\perp}_{208,11}$	[208,142]
$C_{208,7}$	[208,55]	$C_{208,25}$	[208,90]	$C^{\perp}_{208,10}$	[208,143]
$C_{208,8}$	[208,64]	$C_{208,26}$	[208,91]	$C^{\perp}_{208,9}$	[208,143]
$C_{208,9}$	[208,65]	$C^{\perp}_{208,26}$	[208,117]	$C^{\perp}_{208,8}$	[208,144,10]
$C_{208,10}$	[208,65]	$C^{\perp}_{208,25}$	[208,118]	$C^{\perp}_{208,7}$	[208,153]
$C_{208,11}$	[208,66]	$C^{\perp}_{208,24}$	[208,118]	$C^{\perp}_{208,6}$	[208,154]
$C_{208,12}$	[208,66]	$C^{\perp}_{208,23}$	[208,118]	$C^{\perp}_{208,5}$	[208,154]
$C_{208,13}$	[208,66]	$C^{\perp}_{208,22}$	[208,119]	$C^{\perp}_{208,4}$	[208,154]
$C_{208,14}$	[208,67]	$C^{\perp}_{208,21}$	[208,127]	$C^{\perp}_{208,3}$	[208,155]
$C_{208,15}$	[208,77]	$C^{\perp}_{208,20}$	[208,128]	$C^{\perp}_{208,2}$	[208,191,4]
$C_{208,16}$	[208,78]	$C^{\perp}_{208,19}$	[208,129]	$C^{\perp}_{208,1}$	[208,192,3]
$C_{208,17}$	[208,78]	$C^{\perp}_{208,18}$	[208,130]		
$C_{208,18}$	[208,78]	$C^{\perp}_{208,17}$	[208,130]		

We discuss the properties of these codes in Table 4.4.

Table 4.4: Properties of codes from degree 208

Code	Self orthogonal	Doubly Even	Aut(C)	Code	Self orthogonal	Doubly Even	Aut(C)
$C_{208,1}$	Yes	Yes	249600	$C_{208,1}^{\perp}$	No	No	249,600
$C_{208,2}$	Yes	Yes	249600	$C_{208,2}^{\perp}$	No	No	249,600
$C_{208,3}$	Yes	Yes	-	$C_{208,3}^{\perp}$	No	No	-
$C_{208,4}$	Yes	No	-	$C_{208,4}^{\perp}$	No	No	-
$C_{208,5}$	Yes	No	-	$C_{208,5}^{\perp}$	No	No	-
$C_{208,6}$	Yes	No	-	$C_{208,6}^{\perp}$	No	No	-
$C_{208,7}$	No	No	-	$C_{208,7}^{\perp}$	No	No	-
$C_{208,8}$	No	No	-	$C_{208,8}^{\perp}$	No	No	-
$C_{208,9}$	No	No	-	$C_{208,9}^{\perp}$	No	No	-
$C_{208,10}$	Yes	Yes	-	$C_{208,10}^{\perp}$	No	No	-
$C_{208,11}$	Yes	No	-	$C_{208,11}^{\perp}$	No	No	-
$C_{208,12}$	Yes	No	-	$C_{208,12}^{\perp}$	No	No	-
$C_{208,13}$	Yes	No	-	$C_{208,13}^{\perp}$	No	No	-
$C_{208,14}$	No	No	-	$C_{208,14}^{\perp}$	No	No	-
$C_{208,15}$	No	No	-	$C_{208,15}^{\perp}$	No	No	-
$C_{208,16}$	No	No	-	$C_{208,16}^{\perp}$	No	No	-
$C_{208,17}$	No	No	-	$C_{208,17}^{\perp}$	No	No	-
$C_{208,18}$	No	No	-	$C_{208,18}^{\perp}$	No	No	-
$C_{208,19}$	No	No	-	$C_{208,19}^{\perp}$	No	No	-
$C_{208,20}$	No	No	-	$C_{208,20}^{\perp}$	No	No	-
$C_{208,21}$	No	No	-	$C_{208,21}^{\perp}$	No	No	-
$C_{208,22}$	No	No	-	$C_{208,22}^{\perp}$	No	No	-
$C_{208,23}$	No	No	-	$C_{208,23}^{\perp}$	No	No	-
$C_{208,24}$	No	No	-	$C_{208,24}^{\perp}$	No	No	-
$C_{208,25}$	No	No	-	$C_{208,25}^{\perp}$	No	No	-
$C_{208,26}$	No	No	-	$C_{208,26}^{\perp}$	No	No	-

Note that the parameters of the above codes are given in table 4.3. From the table, there are 10 $G-$invariant self orthogonal codes of length 208, 4 $G-$invariant doubly even codes of length 208 and no self dual codes of length 208.

We give weight distributions of some codes and their duals where computations are possible and discuss their properties. We discuss codes $C_{208,1}$ and $C_{208,2}$ of parameters $[208, 16, 72]_2$ and $[208, 17, 72]_2$ respectively. See Tables 4.5 and 4.6.

Table 4.5: Weight distribution of $C_{208,1}$ and $C_{208,2}$

Weight	$[208, 16, 72]_2$	$[208, 17, 72]_2$
0	1	1
72	416	416
80	0	195
88	3120	3328
96	12220	31356
104	30240	60480
112	19136	31356
120	208	3328
128	195	195
136	0	416
208	0	1

Table 4.6: Partial weight distribution of $C^{\perp}_{208,1}$ and $C^{\perp}_{208,2}$

Weight	$[208, 192, 3]_2$	$[208, 191, 4]_2$	Weight	$[208, 192, 3]_2$	$[208, 191, 4]_2$
0	1	1	10	511575290720	511575290720
3	416	0	200	1160074110	1160074110
4	4420	4420	201	47261760	0
5	68640	0	202	1820000	1820000
6	1820000	1820000	203	68640	0
7	47261760	0	204	4420	4420
8	1160074110	1160074110	205	416	0
9	25712797760	0	208	1	1

Our results from tables 4.5 and 4.6 are summarized in lemma 4.1.2 and proposition 4.1.3. Using the same tables, we can assert the inclusions depicted in lemma 4.1.2. We note that the two codes are related. We note that $C_{208,1}$ is contained in $C_{208,2}$ and $C_{208,2}$ is contained in $C^{\perp}_{208,1}$. i.e $C_{208,1}$ is subcode of these two codes and $C^{\perp}_{208,1}$ contains $C_{208,1}$ and $C_{208,2}$. Also, $C_{208,2}$ is contained in $C^{\perp}_{208,2}$.

Lemma 4.1.2.

(i) $C_{208,1} \subset C_{208,2} \subset C^{\perp}_{208,1}$

(ii) $C_{208,2} \subset C^{\perp}_{208,2}$

Proposition 4.1.3.

Let $C_{208,1}$ and $C_{208,2}$ be non-trivial linear binary codes generated when the group G acts on 208 primitive permutation representation over a finite field with 2 elements. We have:

(i.) $C_{208,1}$ has the parameters $[208, 16, 72]_2$. It has a minimum weight of 72. Its dual $C_{208,1}^{\perp}$ has the parameters $[208, 192, 3]_2$. It is self orthogonal and projective. $C_{208,1}$ is irreducible. Moreover, the Aut $(C_{208,1}) \cong 2^2 : U_3(4)$.

(ii.) $C_{208,2}$ has parameters $[208, 17, 72]_2$. It has a minimum weight of 72. Its dual $C_{208,2}^{\perp}$ has the parameters $[208, 191, 4]_2$. It is self orthogonal and projective. $C_{208,2}$ is decomposable. Moreover, the Aut $(C_{208,2}) \cong 2^2 : U_3(4)$.

Proof. (i) The proof proceeds using weight distribution that is given in Tables 4.5 and 4.6. From the weight distribution, the codewords weight of $C_{208,1}$ are divisible by 4, it follows that $C_{208,1}$ is a doubly even code. As such it is self orthogonal. The minimum dual distance is 3. From the lattice structure, with reference to the twelfth layer, the submodule of dimension 16 breaks into trivial submodules 0 and 1 thus irreducible. Since $C_{208,1}$ code is generated by 416 words of minimum weight 72 and $U_3(4)$ is a primitive group of degree 416 , the automorphism group of the $C_{208,1}$ of degree 416 is also primitive. From Magma, we observe that $|Aut(C_{208,1})| = 249{,}600 = 62400 \times 2 \times 2$ and the composition factors are $\mathbb{Z}_2, \mathbb{Z}_2, U_3(4)$. Since $2^2 : U_3(4) = Aut(C_{208,1})$

We have $Aut(C_{208,1}) \cong 2^2 : U_3(4)$

(ii) Accordingly, from the weight distribution, the codewords weight of $C_{208,2}$ are divisible by 4, it follows that $C_{208,2}$ is a doubly even code and hence self orthogonal. The minimum dual distance is 4. The submodule of dimension 17 decomposes into submodules of

dimensions 16 and 1 respectively.

Also as in (i), Since $C_{208,2}$ code is generated by 416 words of minimum weight 72 and $U_3(4)$ is a primitive group of degree 416 , the automorphism group of the $C_{208,2}$ of degree 416 is also primitive. From Magma, we observe that $|Aut(C_{208,2})| = 249{,}600 = 62400 \times 2 \times 2$ and the composition factors are $\mathbb{Z}_2, \mathbb{Z}_2, U_3(4)$. Since $2^2 : U_3(4) = Aut(C_{208,2})$
we have $Aut(C_{208,2}) \cong 2^2 : U_3(4)$

□

The codes $C_{208,1}^{\perp}$ and $C_{208,2}^{\perp}$ with parameters $[208, 192, 3]_2$ and $[208, 191, 4]_2$ respectively can correct up to one error.

Proposition 4.1.4. *The code $C_{208,1}^{\perp}$ and $C_{208,2}^{\perp}$ can correct up to one error.*

Proof. By applying lemma 2.2.4, we obtain that $(d-1)/2 = 1$; thus the result. □

4.1.3 Strongly regular graph related to $[208, 144, 10]_2$ code.

In this sub-section, we show that the code $[208, 144, 10]_2$ is related to a strongly regular graph in lemma 4.1.5.

Lemma 4.1.5. *$\Gamma(C_{208,8}^{\perp})$ is a strongly regular (208,75,30,25) graph with spectrum $[75]^1$, $[17.5]^{143}$, $[-12.5]^{64}$.*

Remark 4.1.6. *We observe that the Eigen values of an adjacency matrix A of $\Gamma(C_{208,8}^{\perp})$ are $\theta_0 = 75$,$\theta_1 = 17.5$ and $\theta_2 = -12.5$ and the corresponding multiplicities of θ_0, θ_1 and θ_2 are $f_0 = 1$, $f_1 = 143$ and $f_2 = 64$. The upper bound on 5-rank of $\Gamma(C_{208,8}^{\perp})$ is $rank_5(\Gamma(C_{208,8}^{\perp})) \leqslant min(f_1 + 1; f_2 + 1) = 65$ since $2/\theta_1 - \theta_2$.*

4.1.4 Designs in codewords of $C_{208,i}$

We describe and construct designs from codes (see, e.g.,[15], theorem 4.1.9).

Theorem 4.1.7. *The support of the codewords of a code C of non-zero weight forms a t-design.*

We use codewords of weight m to construct t-designs from $[208, 16, 72]_2$ and $[208, 17, 72]_2$. In Tables 4.7 and 4.8, the first, second, third and fourth columns show the weight m, the parameters of the designs-(D_{w_m}) , the number of blocks of the designs and if a design (D_{w_m}) is primitive or not under the action of $Aut(C)$ respectively.

Table 4.7: T-Designs from codewords of the code $C_{208,1}$

m	(D_{w_m})	No.of blocks	Primitive
72	$1-(208, 72, 144)$	416	yes
88	$1-(208, 88, 1320)$	3120	No
96	$1-(208, 96, 5640)$	12220	No
104	$1-(208, 104, 15120)$	30240	No
112	$1-(208, 112, 10304)$	19136	No
120	$1-(208, 120, 120)$	208	Yes
128	$1-(208, 128, 120)$	195	No

Table 4.8: T-Designs from codewords of the code $C_{208,2}$

m	(D_{w_m})	No. of blocks	Primitive
72	$1-(208, 72, 144)$	416	Yes
80	$1-(208, 80, 75)$	195	No
88	$1-(208, 88, 1408)$	3328	No
96	$1-(208, 96, 14472)$	31356	No
104	$1-(208, 104, 30240)$	60480	No
112	$1-(208, 112, 16884)$	31356	No
120	$1-(208, 120, 1920)$	3328	No
128	$1-(208, 128, 120)$	195	No
136	$1-(208, 136, 272)$	416	Yes
208	$1-(208, 208, 1)$	1	No

.

Remark 4.1.8. *For $m = 72, 120, 136$, the t-designs are primitive.*

4.1.5 Symmetric 1-Designs

The Group G acts on a primitive permutation representation to obtain a maximal subgroup which is a point stabilizer in G. From the orbits of the point stabilizer, we construct symmetric 1- designs and consequently from the designs, we construct the desired codes.(See theorem 3.3.1, lemma 3.3.3 and theorem 3.3.4).

We construct and examine all symmetric 1-designs invariant under $U_3(4)$ from orbits of rank-5 permutation representation of degree 208. The primitive G-set of degree 208 is denoted by Ω and Ω_1, Ω_2, Ω_3, Ω_4, Ω_5 are the sub orbits of G on Ω with respect to the stabilizer $5 \times A_5$ group with lengths 1, 12, 60, 60 and 75 respectively. .

In Table 4.9, the first, second and third columns show the symmetric 1-design, automorphism of the design and the code derived from the design respectively. The same parameters are repeated for columns four, five and six.

Table 4.9: Symmetric 1-designs from primitive representation of degree 208

Design	$Aut(D_{w_m})$	Code	Design	$Aut(D_{w_m})$	Code
1-(208,12,12)	$2^2 : U_3(4)$	$[208, 80, 12]_2$	1-(208,136,136)	$2 : U_3(4)$	$[208, 17, 72]_2$
1-(208,13,13)	$2^2 : U_3(4)$	$[208, 144, 10]_2$	1-(208,196,196)	$2^2 : U_3(4)$	$[208, 81, 12]_2$
1-(208,60,60)	$2 : U_3(4)$	$[208, 80, 12]_2$	1-(208,88,88)	$2^2 : U_3(4)$	$[208, 17, 72]_2$
1-(208,61,61)	$2 : U_3(4)$	$[208, 144, 10]_2$	1-(208,121,121)	$2^2 : U_3(4)$	$[208, 79]_3$
1-(208,73,73)	$2 : U_3(4)$	$[208, 144]_5$	1-(208,148,148)	$2 : U_3(4)$	$[208, 81, 12]_2$
1-(208,75,75)	$2^2 : U_3(4)$	$[208, 144, 10]_2$	1-(208,207,207)	$2 : A_{208}$	$[208, 208, 1]_2$
1-(208,72,72)	$2 : U_3(4)$	$[208, 16, 72]_2$	1-(208,132,132)	$2^2 : U_3(4)$	$[208, 64]_2$
1-(208,76,76)	$2^2 : U_3(4)$	$[208, 65]_2$	1-(208,147,147)	$2 : U_3(4)$	$[208, 144, 10]_2$
1-(208,135,135)	$2 : U_3(4)$	$[208, 143]_5$	1-(208,195,195)	$2^2 : U_3(4)$	$[208, 144, 10]_2$
1-(208,87,87)	$2^2 : U_3(4)$	$[208, 78]_3$	1-(208,133,133)	$2^2 : U_3(4)$	$[208, 144, 10]_2$
1-(208,120,120)	$2^2 : U_3(4)$	$[208, 16, 72]_2$			

We summarize results of Table 4.9 as follows:

Lemma 4.1.9. *Let D_k be symmetric 1-design, then:*

(i) there are precisely 21 non isomorphic symmetric 1-designs.

(ii) For $k = 12, 13, 75, 76, 87, 88, 120, 121, 132, 195, 196, 133$, $Aut(D_k) \cong 2^2 : U_3(4)$.

(iii) For $k = 60, 61, 72, 73, 135, 136, 147, 148$, $Aut(D_k) \cong 2 : U_3(4)$.

(iv) For $k = 207$, $Aut(D_k) \cong S_{208}$.

4.2 Dimension representation of 416

A group $U_3(4)$ acts on a primitive permutation representation of degree 416 over a finite field with 2 elements to obtain a permutation module. We generate the submodules from the permutation module which represents the dimensions of the G-invariant codes.

4.2.1 G-invariant codes

Let G be a primitive representation of $U_3(4)$ of degree 416. The group G acts on base to generate the stabilizer $5^2 : S_3$. The stabilizer is a maximal subgroup of degree 416 in G. The group G acts on this maximal subgroup over $\mathbb{F}_2$ to produce a permutation module of size 416 contained in G. This permutation module is decomposed into 920 submodules. These submodules represent the dimensions of the linear binary codes of permutation module of size 416 contained in G.

Remark 4.2.1. *The complete list of $U_3(4)-$ invariant submodules of the permutation module $\mathbb{F}_2\Omega$ of degree 416 consists of 920 submodules whose dimensions are given in Table 4.10. From the table, m represents the submodule dimension and # is the submodule number of each dimension.*

Table 4.10: The number of submodules of length 416

m	#	m	#	m	#	m	#
0	1	75	7	125	1	167	1
1	1	76	1	126	7	169	1
37	1	77	1	127	18	170	7
38	7	78	7	128	36	171	7
39	7	79	7	129	12	172	1
40	1	80	1	130	7	175	1
49	1	89	1	131	7	176	3
50	7	90	7	132	1	177	1
51	7	91	7	137	1	180	2
52	1	92	1	138	7	181	7
53	1	101	1	139	7	182	7
54	7	102	7	140	1	183	1
55	7	103	7	141	1	185	1
56	1	104	1	142	7	186	7
61	1	111	1	143	8	187	7
62	7	112	3	144	4	188	1
63	7	113	2	145	1	191	11
64	2	114	7	153	1	192	35
65	2	115	7	154	7	193	11
66	7	116	2	155	7	207	2
67	7	117	1	156	1	208	6
68	1	118	7	164	1		
73	1	119	7	165	7		
74	7	120	1	166	7		

We classified these submodules using the partial submodule lattice as shown in figure 4.2. The diagram shows the upper and lower sections of the lattice diagram. We were not able to produce the whole lattice diagram due to many number of submodules.

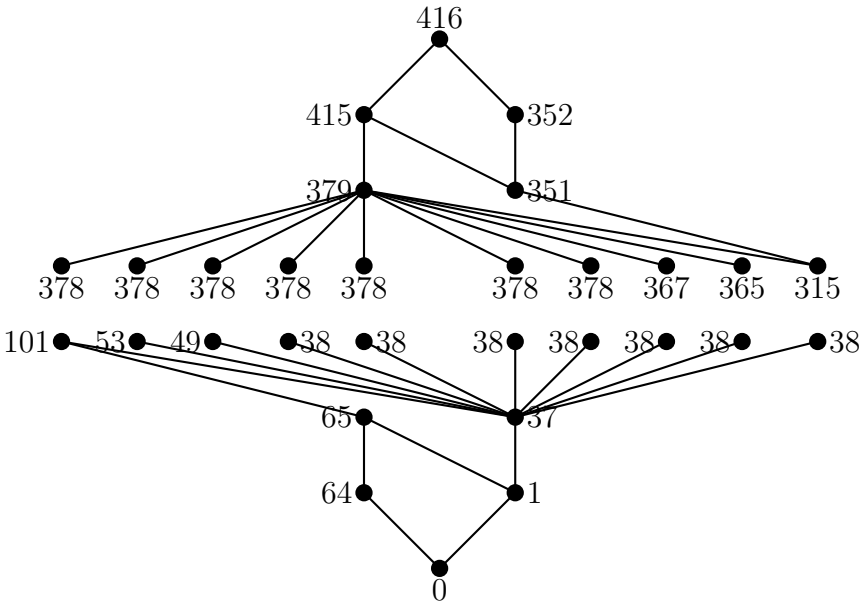

Figure 4.2: Partial Submodule lattice of degree 416

The submodules of dimension 416, 415, 1 and 0 are the dimensions of trivial codes.

Lemma 4.2.2. *There are 916 $G-$invariant codes.*

4.2.2 Symmetric 1-Designs

The Group G acts on a primitive permutation representation to obtain a maximal subgroup which is a point stabilizer in G. From the orbits of the point stabilizer, we construct symmetric 1- designs.(See theorem 3.3.1, lemma 3.3.3 and theorem 3.3.4).

We constructed and examined symmetric 1-designs invariant under $U_3(4)$ from orbits of rank-9 permutation representation of degree 416. The primitive G-set of degree 416 is denoted by Ω and Ω_1, Ω_2, Ω_3, Ω_4 , Ω_5,Ω_6, Ω_7 , Ω_8 , Ω_9 are the sub orbits of G on Ω with respect to the stabilizer $5^2 : S_3$ group with lengths 1, 15, 25(4), 75(2) and 150 respectively.

Table 4.11: Symmetric 1-designs from primitive representation of degree 416

Design	orbit length	parameters	Automorphism Group
D_{15}	15	1-(416, 15, 15)	$2^2 : U_3(4)$.
D_{16}	16	1-(416, 16, 16)	$2^2 : U_3(4)$
D_{25}	25	1-(416, 25, 25)	$U_3(4)$
D_{26}	26	1-(416,26,26)	$U_3(4)$
D_{75}	75	1-(416,75,75)	$2 : U_3(4)$
D_{150}	150	1-(416,150,150)	$2^2 : U_3(4)$
D_{76}	76	1-(416,76,76)	$2 : U_3(4)$
D_{151}	151	1-(416,151,151)	$2^2 : U_3(4)$
D_{40}	40	1-(416,40,40)	$U_3(4)$
D_{90}	90	1-(416,90,90)	$2 : U_3(4)$
D_{165}	165	1-(416,165,165)	$2^2 : U_3(4)$
D_{100}	100	1-(416,100,100)	$U_3(4)$
D_{175}	175	1-(416,175,175)	$U_3(4)$
D_{225}	225	1-(416,225,225)	$2 : U_3(4)$
D_{41}	41	1-(416,41,41)	$U_3(4)$
D_{91}	91	1-(416,91,91)	$2 \cdot U_3(4)$
D_{166}	166	1-(416,166,166)	$2^2 : U_3(4)$
D_{101}	101	1-(416,101,101)	$U_3(4)$
D_{176}	176	1-(416,176,176)	$U_3(4)$
D_{226}	226	1-(416,226,226)	$2 : U_3(4)$
D_{115}	115	1-(416,115,115)	$U_3(4)$
D_{190}	190	1-(416,190,190)	$U_3(4)$
D_{250}	250	1-(416,250,250)	$U_3(4)$
D_{240}	240	1-(416,240,240)	$2 : U_3(4)$
D_{116}	116	1-(416,116,116)	$U_3(4)$
D_{191}	191	1-(416,191,191)	$U_3(4)$
D_{265}	265	1-(416,265,265)	$U_3(4)$
D_{251}	251	1-(416,251,251)	$U_3(4)$
D_{241}	241	1-(416,241,241)	$2 : U_3(4)$

In Table 4.11 above, the first, second, third and fourth columns give the symmetric 1-design, the orbit length, the the parameters of the designs the automorphism of the design respectively. From the table, we come up with proposition 4.2.3.

Proposition 4.2.3. *Let L, M and N be the sets L =[15, 16, 150, 151, 165, 166], M =[75, 76, 90, 225, 91, 226, 240, 241] and N = [25, 26, 40, 100, 175, 41, 101, 176, 115, 190, 250, 116, 191, 265, 251]. Let* $\beta = \{\triangle^g : g \in G\}$ *and* $D_k = (\Omega, \beta)$*. Then it follows that:*

i D_k *is a primitive symmetric* $1 - (416, |\triangle|, |\triangle|)$ *design.*

ii If $k \in L$*, then* $|Aut(D_k)| \cong 2^2 : U_3(4)$

iii if $k \in M$*, then* $|Aut(D_k)| \cong 2 : U_3(4)$

iv if $k \in N$*, then* $|Aut(D_k)| \cong U_3(4)$

Proof

i The definition of Ω and β is inferred from theorem 3.3.1, and from this it is clear that $G \subseteq \mathrm{Aut}(D_k)$.

ii First, we consider the case when k = 15. The composition factors of $\mathrm{Aut}(D_{15})$ are $\mathbb{Z}_2, \mathbb{Z}_2$ *and* $U_3(4)$. Therefore it follows that the $\mathrm{Aut}(D_{15}) = 2^2 : U_3(4)$.

An argument similar to that used in ii above could be used to prove iii and iv. □

4.3 Dimension representation of 1600

The group G acts on $U_1(64)$ to generate the stabilizer $13 : 3$. The stabilizer is a primitive group of degree 1600 in G.

4.3.1 Symmetric 1-Designs

The Group G acts on a primitive permutation representation to obtain a maximal subgroup which is a point stabilizer in G. From the orbits of the point stabilizer, we construct

some symmetric 1- designs.(See theorem 3.3.1, lemma 3.3.3 and theorem 3.3.4).

We constructed and examined some symmetric 1-designs invariant under $U_3(4)$ from orbits of rank-48 permutation representation of degree 1600. The primitive G-set of degree 1600 is denoted by Ω and $\Omega_1, \Omega_2, ..., \Omega_{48}$, are the sub orbits of G on Ω with respect to the stabilizer 13:3 group with lengths 1, 13(9) and 39(38) respectively. In Table 4.12, the first, second, third and fourth columns give the symmetric 1-design, orbit length, parameters of the designs and the automorphism of the design respectively.

Table 4.12: Symmetric 1-designs from primitive representation of degree 1600

Design	orbit length	parameters	Automorphism Group
D_{13}	13	1-(1600, 13, 13)	$U_3(4)$
D_{39}	39	1-(1600, 39, 39)	$2 : U_3(4)$
D_{14}	14	1-(1600, 14, 14)	$U_3(4)$
D_{40}	40	1-(1600,40,40)	$2 : U_3(4)$
D_{52}	52	1-(1600,52,52)	$U_3(4)$
D_{53}	53	1-(1600,53,53)	$U_3(4)$

Proposition 4.3.1. *Let L and M be the sets L=[13,14,52,53] and M = [39,40]. Let* $\beta = \{\triangle^g : g \in G\}$ *and* $D_k = (\Omega, \beta)$. *It follows that:*

i D_k *is a primitive symmetric* $1 - (1600, |\triangle|, |\triangle|)$ *design.*

ii If $k \in L$, *then* $|Aut(D_k)| \cong U_3(4)$

iii if $k \in M$, *then* $|Aut(D_k)| \cong 2 : U_3(4)$

Proof

i The definition of Ω and β is inferred from theorem 3.3.1, and from this it is clear that $G \subseteq Aut(D_k)$.

ii First, we consider the case when k = 13. The composition factors of Aut(D_{13}) are 1 *and* $U_3(4)$. Therefore it follows that the Aut(D_{13})= $U_3(4)$.

iii Here, we consider the case when k = 39. The composition factors of Aut(D_{39}) are $\mathbb{Z}_2$ *and* $U_3(4)$. Therefore it follows that the Aut(D_{39})= $2 : U_3(4)$. □

4.4 Conclusion

We constructed and enumerated all G-invariant codes from primitive permutation representation of degrees 208 and 416 . We constructed some linear binary codes with minimum distance where computations were possible. Properties of the codes where computations were possible were studied. We found 10 self orthogonal codes of length 208, 4 doubly even codes of length 208, two irreducible codes [208, 64] and [208 ,16, 72]. We also found 17 decomposable codes of dimensions 91, 90, 90, 90, 81, 80, 79, 78, 78, 78, 67, 66, 66, 66, 65, 55 and 17. There were 7 reducible codes of dimension 89, 77, 65, 54, 54 , 54 and 53 . There were also 6 non-isomorphic self dual [416, 208] codes of length 416. We determined designs using weights of codewords of some linear binary codes of length 208. The designs 1-(208, 72, 144), 1-(208, 120, 120), 1-(208, 72, 144 and 1-(208, 136, 272) were primitive. Others were not primitive. Symmetric 1- designs were determined from the primitive permutation representation of degrees 208, 416 and 1600. It was found that the automorphism group was either $2^2 : U_3 4$, $U_3 4$, $2 : U_3 4$ or $2 : A_{208}$.

References

[1] Assmus, E.F and Key, J.D, *Designs and their Codes,* Cambridge University Press, (1992).

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

[3] Briggs, N.L and White, A.T , *Permutation Groups and Combinatorial Structures,* Cambridge University press, London Mathematical Society Lecture Notes series 33, (1979).

[4] Brooke, P.L.H, *On matrix representations and codes associated with the simple group of order 25920,* Journal of Algebra , 91(2)(1984), 536-566.

[5] Brooke, P.L.H , *On the Steiner system S(2,4,28) and codes associated with the simple group of order 6048*, Journal of Algebra, 97 (2)(1985), 376-406.

[6] Calderbank, A.R and Wales, D.B , *A global code invariant under the Higman Sims group* , Journal of Algebra 75(1982), 233-260.

[7] Cameron, P.J, *Permutation Groups*, Cambridge University Press, Cambridge, London Math(1999).

[8] Cannon,J, Steel,A and White.G , *Linear Codes over Finite Fields. Handbook of Magma Functions (J. Cannon and W. Bosma, eds.)*, Computational Algebra Group. Department of Mathematics, University of Sydney, http://magma.maths.usyd.edu.au/magma, pp. 3951- 4023(2008).

[9] Chikamai, L , Moori, J and Rodrigues, B. G, *2-modular representations of the alternating group A8 as binary codes*, Glasnik Matematicki, 47(67)(2012), 225-252.

[10] Colbourn, C.J and Dinitz, J.H , *A handbook of Combinatorial Designs*, CRC Press, Second Edition (2007).

[11] Conway, J.H and Sloane, N. J, *Sphere Packings Lattices and Groups* , Springer Verlag (1988).

[12] Conway, J.H, Curtis, R.T, Norton, S.P, Parker, R.A and Wilson, R.A , *Atlas of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups*, Oxford University (1985).

[13] Dind , P , *Linear codes from some 2-designs*, IEEE Transactions on information theory , 61 (6) (2015).

[14] Ding, C , *Linear codes from Designs.* [CS.IT], 14(5).1503.1651 (2005).

[15] Georges, F.R.R , *Designs and Codes from certain finite Simple Groups*, Mafikeng(2013).

[16] Grove, L.C, *Classical groups and geometric algebra* , Graduate Studies in Mathematics, 39, Providence (2002).

[17] Huber, M , *Coding theory and algebraic combinatorics*, Berlin: Institute for Mathematics, Technical University (2008).

[18] Hamming, R.W , *Error detecting and error correcting Codes* , The Bell System technical Journal 29(2)(1950) 147-160.

[19] Katz, D and Kahn, R , *The Social Psychology of Organizations*, John Wiley and Sons (1978).

[20] Key, J.D and Moori, J ,Rodrigues, B.G , *On some designs and codes from Primitive representations of some finite simple groups*, J.Comb in Math and Comput.(2003)

[21] Key, J.D and Moori, J , *Designs, codes and graphs from the Jacko Groups J_1 and J_2* , J.Comb in Math and Comput.(2002).

[22] Key, J.D and Moori, J , *Correction to " Codes , Designs and graphs from the Jacko Groups J_1 and J_2"* , [J.Comb in Math and Comput. 40(2002),143-159] J.Comb in Math and Comput. 40(2008),153.

[23] Krone et al, *Communication Theory and Organizational Communication: Multiple Perspective* , [In F. Jablin, L. Putnam, K. Roberts and PL, Handbooks of Organizational Communication(pp 18 -40)]. SAGE Publications , Inc (1987).

[24] Louck, J.D , *Unitary Symmetry and combinatorics* , World Scientific publishing co.(2008).

[25] Mackey, G. W , *The theory of unitary group representation* , The university of Chicago press (1976).

[26] MacWilliams F. J. MacWilliams , *A theorem on the distribution of weights in a systematic code* , Bell System Tech. J. 42(6)(1963) 79-94.

[27] Randriafanomezantsoa, G. F , *Designs and codes from certain finite simple groups*, North West University, Mafikeng (2013).

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

[29] Schwarzbach, Y.K , *Groups and symmetries: From finite groups to lie groups*, Springer science and business media (2010).

[30] Shannon, C.E, *A mathematical theory of communication* , Bell System Tech.J 27(1948), 379-423, 623-656.

[31] Shier, D.R and Wallenius, K.T , *Applied Mathematical Modeling: A disciplinary Approach* , Chapman and Hall / CRC press(1999).

[32] Svob, A, Crnkovic, D and Mikulic, V , *Designs on which Unitary Group $U_3(3)$ acts transitively*, Croatia, Department of Mathematics, University of Rijeka(2015).

[33] Steinberg , R , *Automorphism of finite linear groups*, Canada, J.Math,12(1996),605-606.

[34] Stellmacher, H.B , *The theory of Finite groups: An Introduction* , Springer (2004).

[35] Walingo, L.C, *Linear Codes obtained from 2-modular representations of some finite simple groups* , University of Kwazulu-Natal, School of Mathematics , Statistics and Computer Science (2012).

[36] Wientraub, S. H , *Representation theory of finite groups, algebra and arithimetic* , American mathematical society (2003).

[37] Yehuda, L , *Introduction to Coding Theory Lecture notes*, Israel, Barlian University, Department of Computer Sciences(2010).