Linear codes obtained from 2-modular representations of some finite simple groups

by

Walingo Lucy Chikamai

A Thesis submitted in fulfillment of the requirements for the degree of

Doctor of Philosophy

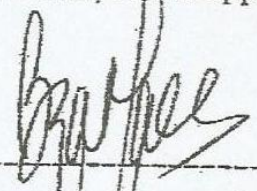
in the

School of Mathematics, Statistics and Computer Science

University of KwaZulu-Natal

November 2012

As the candidate's supervisor, I have approved this dissertation for submission.



Professor B.G. Rodrigues (Supervisor)

As the candidate's co-supervisor, I have approved this dissertation for submission.

Professor J. Moori (Co-supervisor)

Abstract

Let $\mathbb{F}$ be a finite field of q elements and G be a primitive group on a finite set Ω. Then there is a G-action on Ω, namely a map $G \times \Omega \longrightarrow \Omega, (g, \omega) \mapsto \omega^g = g\omega$, satisfying $\omega^{gg'} = (gg')\omega = g(g'\omega)$ for all $g, g' \in G$ and all $\omega \in \Omega$, and that $\omega^1 = 1\omega = \omega$ for all $\omega \in \Omega$. Let $\mathbb{F}\Omega = \{f \mid f : \Omega \longrightarrow \mathbb{F}\}$, be the vector space over $\mathbb{F}$ with basis Ω. Extending the G-action on Ω linearly, $\mathbb{F}\Omega$ becomes an $\mathbb{F}G$-module called an $\mathbb{F}G$-permutation module. We are interested in finding all G-invariant $\mathbb{F}G$-submodules, i.e., codes in $\mathbb{F}\Omega$. The elements $f \in \mathbb{F}\Omega$ are written in the form $f = \sum_{\omega\in\Omega} a_\omega\lambda_\omega$ where λ_ω is a characteristic function. The natural action of an element $g \in G$ is given by $g\left(\sum_{\omega\in\Omega} a_\omega\lambda_\omega\right) = \sum_{\omega\in\Omega} a_\omega\lambda_{g(\omega)}$. This action of G preserves the natural bilinear form defined by

$$\left\langle \sum a_\omega\lambda_\omega, \sum b_\omega\lambda_\omega \right\rangle = \sum a_\omega b_\omega.$$

In this thesis a program is proposed on how to determine codes with given primitive permutation group. The approach is modular representation theoretic and based on a study of maximal submodules of permutation modules $\mathbb{F}\Omega$ defined by the action of a finite group G on G-sets $\Omega = G/G_x$. This approach provides the advantage of an explicit basis for the code. There appear slightly different concepts of (linear) codes in the literature. Following Knapp and Schmid [83] a code over some finite field $\mathbb{F}$ will be a triple $(V, \Omega, \mathbb{F})$, where $V = \mathbb{F}\Omega$ is a free $\mathbb{F}G$-module of finite rank with basis Ω and a submodule C. By convention we call C a code having ambient space V and ambient basis Ω. $\mathbb{F}$ is the alphabet of the code C, the degree n of V its length, and C is an $[n, k]$-code if C is a free module of dimension k.

In this thesis we have surveyed some known methods of constructing codes from

primitive permutation representations of finite groups. Generally, our program is more inclusive than these methods as the codes obtained using our approach include the codes obtained using these other methods. The designs obtained by other authors (see for example [40]) are found using our method, and these are in general defined by the support of the codewords of given weight in the codes. Moreover, this method allows for a geometric interpretation of many classes of codewords, and helps establish links with other combinatorial structures, such as designs and graphs.

To illustrate the program we determine all 2-modular codes that admit the two known non-isomorphic simple linear groups of order 20160, namely $L_3(4)$ and $L_4(2) \cong A_8$. In the process we enumerate and classify all codes preserved by such groups, and provide the lattice of submodules for the corresponding permutation modules. It turns out that there are no self-orthogonal or self-dual codes invariant under these groups, and also that the automorphism groups of their respective codes are in most cases not the prescribed groups. We make use of the Assmus Matson Theorem and the Mac Williams identities in the study of the dual codes. We observe that in all cases the sets of several classes of non-trivial codewords are stabilized by maximal subgroups of the automorphism groups of the codes. The study of the codes invariant under the simple linear group $L_4(2)$ leads as a by-product to a unique flag-transitive, point primitive symmetric 2-$(64, 28, 12)$ design preserved by the affine group of type $2^6{:}S_6(2)$. This has consequently prompted the study of binary codes from the row span of the adjacency matrices of a class of 46 non-isomorphic symmetric 2-$(64, 28, 12)$ designs invariant under the Frobenius group of order 21. Codes obtained from the orbit matrices of these designs have also been studied. The thesis concludes with a discussion of codes that are left invariant by the simple symplectic group $S_6(2)$ in all its 2-modular primitive permutation representations.

Preface

The research reported in this dissertation was done under the supervision of Professor B.G. Rodrigues, School of Mathematical Sciences, University of KwaZulu-Natal and and Professor J. Moori, School of Mathematical Sciences, North-West University (Mafikeng) and it is the author's original work except where otherwise, due reference has been made. It has not been submitted before for any other degree or to any other institution.

Signed:

Lucy Walingo Chikamai (Student)

Professor B.G. Rodrigues (Supervisor)

Professor J. Moori (Co-supervisor)

Dedication

To two lovely ladies to whom it was not permitted to witness this vain human enterprise. God is sovereign: His agenda supreme; He alone has the full picture!

Mama Julia Khayanga Khautu Nandi (1928–16th Aug 2009)

and

Daughter Fehmida Khayanga Khautu Julia (28th Feb 1989–26th Feb 2012)

" For we know that if our earthly house of this tabernacle were dissolved, we have a building of God, an house not made with hands, eternal in the heavens. 2: For in this we groan, earnestly desiring to be clothed upon with our house which is from heaven. " ***2Co 5:1-2***

" And I heard a voice from Heaven saying to me, Write, Blessed are the dead who die in the Lord from now on. Yes, says the Spirit, they shall rest from their labors, and their works follow them." ***Re 14:13***

"I will ransom them from the power of the grave; I will redeem them from death" **Hos 13:14**

"Jesus said to her, I am the Resurrection and the Life! He who believes in Me, though he die, yet he shall live." **Jo 11:25**

" On Christ the solid rock I stand all other ground is sinking sand." So this is for you and to all them who believe in the second coming of Jesus Christ. To Him be praise glory and honor forever. Amen.

Acknowledgments

... he determined the times set for them and the exact places where they should live. Ac 17:26 For the vision is yet for an appointed time; ...though it tarries, wait for it; because it will surely come, it will not tarry. Hab 2:3 And it came to pass ... the LORD said ... Arise, ...for I have delivered it into thine hand. Jg 7:9

A work like this can only be accomplished with the contribution of many people in various ways. To them all, I owe a debt of love and appreciation. I am most grateful to my supervisors Prof B. G. Rodrigues and Prof J. Moori, for their guidance and unending patience without which this work would not have been accomplished and which, I am sure, contributed to some grey hairs.

I acknowledge financial support from; NRF via the Grant holders scholarship, UKZN graduate scholarship and the Mathematics department under Prof Govinder; This enabled me attend various conferences that made me meet some leading Mathematicians and enlightened me with the current trends in Mathematical research. I thank my employer at MMUST for giving me leave to study; The entire Mathematics fraternity provided a friendly and cohesive environment that lightened my stay and more so the Discrete Mathematics research group for the stimulating presentations, particularly Patrick for sharing many learning experiences including the pizza;

My family in Christ: the Friday fellowship at Dr Hayanga's, the "watchmen", Pastors Drew of Citizen Church and Dean of Joshua Covenant Ministries, Durban, the precious "go ye" church, USOMI; Blow the trumpet faithfully and courageously!

And now the last wine! Tom omwana wefu ehe! Walola elijina omusi! Wachila ndakhulondakho endi siesi endolekho omusi okwo! My husband Ben and kids: what a sacrifice! I can only repeat the words of Ac 17:26. Keith my scribe and turned companion; always quietly listening or pretending to. My family and all them who held fort back home; what a blessing you are! If there is anything inspiring in this work that can lift you up, be blessed with it and may God surely reward you.

God! We don't list you among men for you are the all in all, the Alpha and the Omega. Take your rightful position in this work. Glory, honor, power, dominion be unto you forever.

Notation and terminology

$\mathbb{N}$	natural numbers
$\mathbb{Z}$	integer numbers
$\mathbb{R}$	real numbers
$\mathbb{C}$	complex numbers
Ω	a set
$\varnothing$	empty set
$\|\Omega\|$	the cardinality of the set
V	vector space
$\mathbb{F}$	a Field
$\mathbb{F}_q$	the Galois field of q elements
$\mathbb{F}^*$	Field $\mathbb{F} - \{0\}$
$char(\mathbb{F})$	characteristic of the field $\mathbb{F}$
$G{:}H$	a split extension of G by H
$G.H$	general extension
$G{\cdot}H$	a non-split extension respectively of G by H
G, H, K	groups
$\mathrm{Aut}(G)$	Automorphism group of a group G
$\mathrm{Inn}(G)$	Inner automorphism group of a group G
$\mathrm{Out}(G)$	Outer automorphisms of a group G

1_G	the identity element of G
$K \leqslant G$	K is a subgroup of G
$K \leqslant_{max} G$	K is a maximal subgroup of G
$K \trianglelefteq G$	K is normal subgroup of G
$H \cong G$	H is isomorphic to G
$N_G(K)$	the normalizer of the subgroup K in G
$\mathrm{C}_G(K)$	the centralizer of the subgroup K in G
gkg^{-1}	conjugation of k by g
$ccl_G K$	The conjugacy class of a subgroup K of G
$\mathrm{End}(V)$	set of endomorphisms of a vector space V
$\mathrm{Hom}_{\mathbb{F}}(V, W)$	homomorphisms of a vector space from V to W over a field $\mathbb{F}$
$[n, k, d]q$	a $q-$ary code of length n, dimension k and minimum distance d
C	a linear code
G	a generator matrix for C
H	a parity check matrix for C
$\mathcal{D}$	an incidence structure
$(\mathcal{D}, \mathcal{P}, \mathcal{I})$	an incidence structure with $\mathcal{P}$ points and $\mathcal{B}$ blocks
$C_p(D)$	$p-$ary code of an incidence structure D
Γ	a graph
$T(n)$	the triangular graph
$\mathrm{PG}(V)$	the projective geometry
$P\Gamma L(V)$	the projective semi- linear group
$\mathbb{F}\Omega$	$\mathbb{F}G-$module
$\mathbb{F}G$	Group algebra
$x.y$	the dot product of x and y
$\langle x, y \rangle$	the inner product of x and y
$GL_n(q)$	general linear group of dimension n over F_q
$GL(V)$	general linear group over V
$Sc(V)$	the center of $GL(V)$

$dim(V)$	the dimension of a vector space V
pdim(U)	the projective dimension of U
S_n	the symmetric group on n symbols
A_n	the alternating group on n symbols
PSL(n,q), $L_n(q)$	Projective special linear group
PGL(n,q)	Projective general linear group
$V_n(q)$	a vector space of dimension n over F_q
$PSp_n(q), S_n(q)$	Projective symplectic group of dimension n over F_q
$\langle x_1, x_2, ..., x_n \rangle$	the subspace spanned over F by the subset $\{x_1, x_2, ..., x_n\}$
Aut(C)	the automorphism group of a code C
$H \leq_{max} G$	H is a maximal subgroup of G
STS	Steiner triple system
C_A	the code of the incidence matrix A of an incidence structure
$d_q(n,k)$	the maximum distance d such that an $[n,k,d]_q$ code exists
$n_q(k,d)$	the smallest integer n for which an $[n,k,d]_q$ code exists
J	the all-ones matrix
$\mathbf{1}$	the all-ones vector or codeword
I	the identity matrix
I_n	the $n \times n$ identity matrix

Contents

Chapter 1

Introduction

Algebraic coding theory originated in communications as a result of an effort to control errors caused by distortion and interference in transmitted data and has since then expanded and established itself as a field of study. Though coding theory has its roots in communications, it is richly related to many areas of mathematics. Linear codes have been constructed from row spaces of incident matrices of combinatorial objects such as graphs, designs and finite geometries, to name but a few, and their properties derive from the underlying structures. As such codes are closely linked with many mathematical objects and this lends a study of the interplay between the codes and the mathematical objects as important as the study of the codes themselves.

This thesis is a study of binary linear codes obtained from 2-modular primitive permutation representations of some finite simple groups. Given a primitive representation of a group G on a finite set Ω, defining a multiplication on the group ring $V = \mathbb{F}_2 G$ by elements of the group makes V an $\mathbb{F}G$-module. The invariant submodules (i.e., the subspaces of $\mathbb{F}_2 G$ taken into themselves by every group element) are all the p-ary codes for which G is a subgroup of the automorphism group of the code. We attempt to determine and examine all the binary invariant codes under the prescribed group. This is an enumeration and classification problem which not only has a merit of its own but also lends itself naturally to revealing an interplay between coding theory, modular representation theory and combinatorial structures.

Enumeration and classification problems, though revealing the structure of an object, are generally laborious and are fundamentally connected with algorithms and computations. Proofs therefore require significant computations and effort to produce and verify and involve lengthy, time consuming searches but very often, they have saved the day by providing a proof where the traditional methods of simple arguments have failed. It is our view that the enumeration and classification of codes invariant under a prescribed finite group is an intricate problem and that a definite or complete answer to it is not easily attainable, due to there being many perspectives and approaches, and also due to current computational limitations, particularly when the degree of the primitive representations is significantly large.

Codes from primitive permutation groups have received a lot of attention before. Some earlier attempts in this direction was carried out in [83] with a view of studying codes via monomial actions and projective representations of transitive permutation groups. Later in [13, 14] all binary codes obtainable from the primitive permutation representations of the simple groups $U_3(3)$ and $U_4(2)$ were found using irreducible modules. See also [28] for related results. More recently in [80], the authors looked at those codes from the irreducible modules invariant under the Janko groups and in particular those of small dimension.

In this thesis we have proposed a program to determine codes with given primitive permutation group. The approach is modular representation theoretic and, based on a study of maximal submodules of permutation modules over a field $\mathbb{F}$ defined by the action of a finite group on sets $\Omega = G/G_\alpha$. This approach provides the advantage of an explicit basis for the code. By way of illustration of this program we selected three simple groups, namely; $L_3(4), L_4(2)$ and $S_6(2)$ and examined all 2-modular codes which admit these groups as automorphisms. As a by product we reveal the lattice of submodules for the corresponding permutation modules. This contributes to enumerating the codes, and in most cases classifying by giving a geometric characterization of some classes of codewords.

One of the central aims of our investigation is to explore further the interplay between 2-modular representation theory of finite groups and coding theory. We

have gathered together, in the first three chapters in readily usable form a collection of most of the basic terms from the theory of finite groups, group representations and $\mathbb{F}G$-modules. In addition, we give a brief but complete overview of the combinatorial structures that are to be used, namely combinatorial designs, graphs, codes and finite geometries and their links. As this study encompasses several different topics, this has the effect of making the introduction unusually, but yet necessarily long. These concepts, though fairly known and found in any standard textbook, are collected here in a self contained format for easy access and coherency. In Chapter 2 we describe the three classes of groups that we use in the thesis, namely: linear, symplectic and alternating groups. An important tool for studying the structure of groups is the concept of group homomorphism or representation. Representations can be studied via $\mathbb{F}G$-modules due to a one-to-one correspondence between them. This is discussed in Chapter 3, where we also give some results on modular representation theory briefly highlighting the differences between ordinary and modular representations and in Chapter 4 we focus on combinatorial structures: codes, designs, graphs and finite geometries.

Chapter 5 explores how codes are constructed from combinatorial structures, namely graphs, designs or finite geometries. In Chapter 6, after surveying some known methods of construction of codes from primitive groups, we propose a novel program to construct codes from primitive permutation representations of a group. This is done by using a chain of maximal submodules of the corresponding permutation modules. In the subsequent chapters, using the methods described in Chapter 6 we determine all binary linear codes invariant under the simple groups $L_3(4), A_8$ and $S_6(2)$ respectively. The computations have been carried recursively in Magma with a built-in component of Meat-Axe. The theoretical generalizations of these computations give us our results.

In Chapter 7, we construct and enumerate all non-trivial binary linear codes from the 2-modular primitive representations of the simple group $L_3(4)$, using a chain of maximal submodules of a permutation module induced by the action of $L_3(4)$ on objects such as the lines, hyperovals, Baer subplanes and unitals of $PG_2(4)$.

Several codes with interesting properties are obtained, among these optimal and self-orthogonal codes invariant under $L_3(4)$. We establish results on non-existence of $L_3(4)$-invariant self-dual codes of lengths 56, 120 and 280 respectively, and moreover that $L_3(4)$ is not realizable as the automorphism group of a binary linear code. A fundamental problem in coding theory is to optimize one of the parameters n, k, d given the other two (over a given field $\mathbb{F}_q$). Two versions of the problem are known, namely to find the smallest n for which an $[n, k, d]_q$ code exists; and to find the maximum distance d for which an $[n, k, d]_q$ code exists. In this thesis we deal with the second problem, for some linear codes over $\mathbb{F}_2$. Recall that a linear $[n, k]$ code C is called optimal if $n = n_q(k, d)$ or $d = d_q(n, k)$.

In Chapter 7, using a chain of maximal submodules of a permutation module induced by the action of the simple linear group $L_3(4)$ we obtained almost all non-trivial binary codes invariant under the group. However, it is well known that there are two non-isomorphic simple groups of order 20160, respectively $L_3(4)$ and the alternating group A_8. It thus seems natural to ask for the codes invariant under A_8 and their weight distribution. Moreover, the isomorphism $A_8 \cong L_4(2) \cong \Omega^+(6, 2)$ adds a rich geometrical structure that can be used to explore the connections with objects such as combinatorial designs, graphs, groups and irreducible modules. In Chapter 8 in a manner similar to that in Chapter 7 we consider the primitive representations of A_8 and determine the irreducible constituents of the primitive 2-modular permutation representations and from these we determine the dimensions and constituents of all submodules of each of the subspaces. The incidences between the constituents are determined and used to describe the nature of the codewords of several weights. In addition, we used the Atlas of Brauer characters to determine the irreducibility of the codes and the MacWilliams identities relating the weight enumerators of the dual codes.

It was proved by Jungnickel and Tonchev that there exist four non-isomorphic symmetric 2-$(64, 28, 12)$ designs characterized by symmetric difference property and minimality of their 2-rank. Moreover, these designs have large full automorphism groups with large 2-subgroups. In particular, the orders of the full automorphism

groups are divisible by 2^6, and their derived 2-$(28, 12, 11)$ quasi-symmetric designs give rise to four inequivalent $[28, 7, 12]_2$ codes. More recently Crnković and Pavčević constructed 46 non-isomorphic 2-$(64, 28, 12)$ designs for which 2^6 is not a divisor of the order of their full automorphism groups and have in addition shown that none of the derived designs is quasi-symmetric, thus proving that the said designs are non-isomorphic to those with the same parameters. Further, according to [[91], Table 11.1, p.38] there are at least 8784 designs with parameters 2-$(64, 28, 12)$ whose derived 2-$(28, 12, 11)$ designs are not quasi-symmetric. Using modular representation theoretical methods in Chapter 8 we examine the structure of a $[28, 7, 12]_2$ code invariant under the symplectic group $S_6(2)$ and show that the supports of the codewords of minimum weight 12 in that code give rise to a 2-$(28, 12, 11)$ quasi-symmetric design which is a derived design of the unique point-primitive and flag-transitive 2-$(64, 28, 12)$ design with automorphism group isomorphic to $2^6{:}S_6(2)$. This study led us to investigate the binary codes of the class of 46 non-isomorphic 2-$(64, 28, 12)$ designs described above. Hence in Chapter 9 we examine the binary codes defined by the row span of the incidence matrices of the 46 non-isomorphic designs whose defining properties are given above.

In Chapter 10 we examine further some of the links encountered implicitly in Chapters 8 and 9 and explore the 2-modular codes invariant under the simple symplectic group $S_6(2)$. Due to computer time limitations we restrict our studies up to the representation of degree 135. For the other representations we simply outline the irreducible codes. We prove that there are no self dual codes of length 28, 36 and 120 invariant under the symplectic group $S_6(2)$.

Chapter 2

Groups

The aim of this chapter is to bring together in an accessible form a selection of mostly standard results from the theory of groups, which will be required in the subsequent chapters. We will not give proofs of every result. Most of the results could be found in standard texts such as [8, 24] and [106]. We have however, mostly used reference [102] for a number of stated results.

2.1 Permutation groups

The symmetric group on a set Ω (Ω is non-empty throughout) is the group S_Ω of all permutations of Ω. If Ω is 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, and G is said to be **transitive** on Ω if, for all $\alpha, \beta \in \Omega$, there exists an element $g \in G$ such that the image α^g of α under g is equal to β. More generally, the **orbit** of G containing the point $\alpha \in \Omega$ is the set $\alpha^G = \{\alpha^g \mid g \in G\}$.

The permutation group G on Ω can also be regarded as a permutation group on $\Omega \times \Omega$ by defining

$$(\alpha, \beta)^g = (\alpha^g, \beta^g),$$

where $\alpha, \beta \in \Omega$ and $g \in G$. The number of orbits of G on $\Omega \times \Omega$ is called the **rank** of G on Ω, which is denoted by $rank(G)$. If α, β are distinct points of Ω, then the

pairs (α, α) and (α, β) lie in different orbits of G on $\Omega \times \Omega$. Thus, for $|\Omega| > 1$, the rank of G is at least 2. A permutation group is said to be 2-**transitive** (or **doubly transitive**) on Ω if it is transitive on the ordered pairs of distinct points of Ω. Thus, for $|\Omega| > 1$ the 2-transitive groups are precisely the permutation groups of rank 2.

The orbits of G on $\Omega \times \Omega$ are called **orbitals,** and to each orbital E we associate the directed graph with vertex set Ω and edge set E, the so-called **orbital digraph** for E. It is easy to show that the orbitals of G are in one-to-one correspondence with the orbits on Ω of the **stabilizer** $G_\alpha = \{g \in G \mid \alpha^g = \alpha\}$ of a point $\alpha \in \Omega$. This correspondence maps an orbital E to the set of points $\{\beta \mid (\alpha, \beta) \in E\}$. The orbits of G_α on Ω are called **suborbits** of G, and their lengths are called **subdegrees** of G. If G has rank r on $\Omega \times \Omega$ then a point stabilizer will have exactly r orbits on Ω and we say that such a stabilizer is a **rank-r** subgroup of G.

2.2 Permutation representations

Definition 2.1. *Let G be a group and Ω be a set. An* **action** *of 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 $g, h \in G$, $\alpha^1 = \alpha$ and $(\alpha^g)^h = \alpha^{gh}$.*

In a natural way, an action defines a permutation representation of G on Ω, which is a homomorphism ψ from G into S_Ω. Simply define $\psi(g) \in S_\Omega$ by $\psi(g)(\alpha) = \alpha^g$. Conversely a permutation representation naturally defines an action of G on Ω, leading to a natural bijection between the action of G on Ω and the permutation representation of G on Ω.

Most of the definitions of Section 2.1 apply to permutation representations by applying them to the permutation group which is the image of that representation. Thus a permutation representation is said to be transitive if its image is transitive. Similarly the orbits of a representation are those of its image and, if the representation is transitive, then its rank, orbitals, suborbits and subdegrees are those of its image. However the point stabilizer $G_\alpha = \{g \in G \mid \alpha^g = \alpha\}$ for the representation may be a proper preimage of the point stabilizer for the permutation representation group

image.

A permutation representation is said to be **faithful** if its kernel is the identity group, in which case G is isomorphic to its permutation group image and we are back to the case of permutation groups.

Theorem 2.2. *Let G act on a set Ω. Then $|\alpha^G| = [G : G_\alpha]$, that is the number of elements in the orbit of α is equal to $[G : G_\alpha]$.*

Proof: See [106]. ■

Corollary 2.3 (,)**.** *If G is a finite group acting on a finite set Ω then for all $\alpha \in \Omega$ we have $|\alpha^G| \mid |G|$.*

Proof: By Theorem 2.2 we have $|\alpha^G| = [G : G_\alpha] = \frac{|G|}{|G_\alpha|}$. Hence $|G| = |\alpha^G|.|G_\alpha|$. Thus $|\alpha^G|$ divides $|G|$.■

Theorem 2.4. (a) *If G is a finite group, then for all $g \in G$ the number of conjugates of g in G is equal to $[G : C_G(g)]$.*

(b) *If G is a finite group and H is a subgroup of G, then the number of conjugates of H in G is equal to $[G : N_G(H)]$.*

Proof: (a) Since G acts on itself by conjugation, using Theorem 2.2 we have $|g^G| = [G : G_g]$. But since $g^G = \{g^h \mid h \in G\} = \{hgh^{-1} \mid h \in G\} = [g]$ and $G_g = \{h \in G \mid g^h = g\} = \{h \in G \mid hgh^{-1} = g\} = \{h \in G \mid hg = gh\} = C_G(g)$, we have $|g^G| = |[g]| = [G : C_G(g)] = \frac{|G|}{|C_G(g)|}$.

(b) Let G act on the set of all its subgroups by conjugation. Then by the Theorem 2.2 we have $|H^G| = [G : G_H]$.
Since $H^G = \{H^g \mid g \in G\} = \{gHg^{-1} \mid g \in G\} = [H]$ and $G_H = \{g \in G \mid H^g = H\} = \{g \in G \mid gHg^{-1} = H\} = N_G(H)$ we have $|[H]| = |H^G| = [G : G_H] = [G : N_G(H)] = \frac{|G|}{|N_G(H)|}$. ■

Note 2.5. If G is a finite transitive group acting on a finite set Ω, then Theorem 2.2 (ii) implies that

$$|\alpha^G| = |\Omega| = \frac{|G|}{|G_\alpha|}.$$

Hence $|G| = |\Omega|.|G_\alpha|$.

Given a finite group G, it is of interest to know for what $n = |\Omega|$ the action of G on Ω is transitive. Knowing this allows us to decide for what n we can view G as a subgroup of S_n with a transitive action. For this we consider H a subgroup of G and allow G to act on G/H by $g \cdot xH = gxH$. If $xH \neq yH$ we have that $xH = xy^{-1}yH$, and thus we deduce immediately that this is a transitive action. From Definition 2.1 it follows that there is a permutation representation of G on $[G : H]$ with a transitive action of G. We are now in a position to prove

Theorem 2.6 ([106])**.** *Any transitive action of a group G on a subgroup H is equivalent to the action of G by left multiplication on a coset space G/H.*

Proof: Suppose that G has a permutation representation on $|\Omega|$ points with G acting transitively on Ω. Fix $\alpha \in \Omega$ and let $H = \{x \in G \,|\, \alpha^x = \alpha\}$ be the stabilizer of the point α. Define a map $\phi : G \longrightarrow \Omega$ by $\phi(x) = \alpha^x$. Notice that for $y \in H$ we have $\phi(xy) = \alpha^{xy} = \alpha^x = \phi(x)$ and so $\psi : G/H \longrightarrow \Omega$ given by $\psi(xH) = \phi(x)$ is well defined. We need to establish a bijective correspondence between $G/H = \{xH \,|\, x \in G\}$ and the points of Ω. We do this by defining the map $\psi : G/H \longrightarrow \Omega$ given by $\psi(xH) = \alpha^x$. This map is well defined: if $x, y \in G$ we have $yH = xH \Leftrightarrow x^{-1}y \in H \Leftrightarrow \alpha^{x^{-1}y} = \alpha \Leftrightarrow \alpha^y = \alpha^x \Leftrightarrow \psi(yH) = \psi(xH)$. It is also one-to-one: if $\psi(xH) = \psi(yH)$ then $\alpha^x = \alpha^y \Leftrightarrow \alpha^{x^{-1}y} = \alpha \Leftrightarrow x^{-1}y \in H \Leftrightarrow yH = xH$. In addition, we have that ϕ is onto since G acts transitively. Hence ψ is a bijection. Finally, $\psi(xyH) = \phi(xy) = \alpha^{xy} = x\psi(y)$ implies that ψ preserves the action of G. ■

We have thus shown that every transitive action can be realized by means of an action of a group G on the set of all left cosets of its subgroup H and therefore the study of transitive groups is equivalent to the study of the action on the set of the left cosets of a subgroup.

Definition 2.7. *Let G act on a set Ω. Let $|\Omega| = n$ and $1 \leq k \leq n$ be a positive integer. We say that G is k-**transitive** on Ω if for every two ordered k-tuples*

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

Lemma 2.8. *Let G be a transitive group on a set Ω, $|\Omega| = n \geq 2$. If G_α is $(k-1)$-transitive on $\Omega \setminus \{\alpha\}$ for every $\alpha \in \Omega$, then G is k-transitive on Ω.*

Proof: See [8, Lemma 1.3.6]. ■

Theorem 2.9 ([106])**.** *If G is a k-transitive group on a set Ω with $|\Omega| = n$, then*

$$|G| = n(n-1)(n-2)\cdots(n-k+1) \mid G_{[\alpha_1, \alpha_2, \ldots, \alpha_k]}$$

for every choice of k-distinct $\alpha_1, \alpha_2, \ldots, \alpha_k \in \Omega$, where $G_{[\alpha_1, \alpha_2, \ldots, \alpha_k]}$ denotes the set of all elements g in G such that ${\alpha_i}^g = \alpha_i$, $1 \leq i \leq k$.

2.3 Automorphism groups

Definition 2.10. *The* **automorphism group** *of a group G, denoted by* $\mathrm{Aut}(G)$*, is the set of all automorphisms of G, under the operation of composition.*

Definition 2.11. *Let g be any element of G. Define a map $\phi_g : G \longrightarrow G$ by $\phi_g(x) = gxg^{-1}$ for all $x \in G$. Then ϕ_g is an automorphism of G, known as an* **inner automorphism** *of G.*

For a given $x \in G$ we have that $x = \phi_g(g^{-1}xg)$ and if $\phi_g(x) = \phi_g(y)$ then $gxg^{-1} = gyg^{-1}$ and so $x = y$. We also have that $\phi_{gh}(x) = ghx(gh)^{-1} = ghxh^{-1}g^{-1} = g\phi_h(x)g^{-1} = \phi_g\phi_h(x)$. So that $\phi_{gh} = \phi_g\phi_h$ for $g, h \in G$.

Theorem 2.12. *(a) If H is a subgroup of G, then $C_G(H) \trianglelefteq N_G(H)$ and $N_G(H)/C_G(H)$ can be embedded in* $\mathrm{Aut}(H)$*, that is $N_G(H)/C_G(H)$ is isomorphic to a subgroup of* $\mathrm{Aut}(H)$*.*
(b) The set of all inner automorphisms of G, denoted by $Inn(G)$, is a normal subgroup of $\mathrm{Aut}(G)$ *and $G/Z(G) \cong Inn(G)$.*

Proof: (a) For each $x \in N_G(H)$, define a map ϕ_x on H by $\phi_x(h) = xhx^{-1}$.

(i) If $\phi_x(h) = \phi_x(g)$ then $xhx^{-1} = xgx^{-1}$, so $h = g$ and hence ϕ_x is injective.

(ii) For any $h \in H$ we have that $x^{-1}hx \in H$ because x^{-1} normalizes H. Now since $\phi_x(x^{-1}hx) = x(x^{-1}hx)x^{-1} = h$, ϕ_x is surjective.

Now it only remains to show that ϕ_x is a homomorphism. But for all g and h in H we have $\phi_x(gh) = xghx^{-1} = xgx^{-1}xhx^{-1} = \phi_x(g)\phi_x(h)$, which implies that ϕ_x is a homomorphism.

The map $\phi : N_G(H) \longrightarrow \mathrm{Aut}(H)$ given by $\phi(x) = \phi_x$ is a homomorphism. Because $\forall h \in H$, and $\forall x, y \in N_G(H)$ we have

$$\begin{aligned}(\phi(x)\phi(y))(h) &= \phi(x)(\phi(y)(h)) = \phi(x)(yhy^{-1}) \\ &= x(yhy^{-1})x^{-1} = (xy)h(xy)^{-1} = \phi(xy)(h),\end{aligned}$$

. This implies $\phi(x)\phi(y) = \phi(xy)$.

$$\begin{aligned}\mathrm{Ker}(\phi) &= \{x \in N_G(H) \mid \phi(x) = I_H\} \\ &= \{x \in N_G(H) \mid \phi(x)(h) = h, \text{ for all } h \in H\} \\ &= \{x \in N_G(H) \mid xhx^{-1} = h, \text{ for all } h \in H\} \\ &= \{x \in N_G(H) \mid xh = hx, \text{ for all } h \in H\} \\ &= C_G(H).\end{aligned}$$

Therefore $C_G(H) \trianglelefteq N_G(H)$ and by the first isomorphism theorem we have that $N_G(H)/C_G(H) \cong \mathrm{Im}(\phi)$. Hence $N_G(H)/C_G(H) \cong \mathrm{Im}(\phi) \leq \mathrm{Aut(H)}$.

(b) If $H = G$, then $N_G(H) = G$ and so $C_G(H) = Z(G)$ and the map ϕ given in part (1) has Inn(G) as its image. Therefore the isomorphism established in (1) is now $G/Z(G) \cong \mathrm{Inn(G)}$. To show that $\mathrm{Inn(G)} \trianglelefteq \mathrm{Aut(G)}$ we must show that if $\rho \in \mathrm{Aut(G)}$ and $\phi_g \in \mathrm{Inn(G)}$ then $\rho\phi_g\rho^{-1} \in \mathrm{Inn(G)}$. We can see that $(\rho\phi_g\rho^{-1})(x) = \rho(\phi_g(\rho^{-1}(x))) = \rho(g\rho^{-1}(x)g^{-1}) = \rho(g)\rho(\rho^{-1}(x))\rho(g^{-1}) = \rho(g)x\rho(g^{-1}) = \phi_{\rho(g)}(x)$ for all $x \in G$. Hence $\rho\phi_g\rho^{-1} = \phi_{\rho(g)}$ and $\mathrm{Inn(G)} \trianglelefteq \mathrm{Aut(G)}$. ■

2.4 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, i.e., for $B \in P$ and $g \in G$, the set B^g is also a block of P. 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 P have the same cardinality and G acts transitively on P. Moreover, every permutation group G on Ω preserves two partitions namely Ω and $\{\{\alpha\} \mid \alpha \in \Omega\}$; these are called **trivial partitions** of Ω, and their blocks Ω and $\{\alpha\}$ for $\alpha \in \Omega$ are called **trivial blocks of imprimitivity.** All other blocks of Ω are said to be **non-trivial**.

Definition 2.13. *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 2.14. (a) *For every n, the symmetric group S_n acts n-transitively on $\Omega = \{1, 2, \cdots, n\}$,*
(b) *for $n \geq 3$ the alternating group A_n acts $(n-2)$-transitively, but not $(n-1)$-transitively on Ω.*

Proof: (a) Since S_n contains all permutations of the set Ω, it is clearly n-transitive on Ω.
(b) We use induction on n, beginning with the fact that A_3 is transitive, but not 2-transitive, on $\{1, 2, 3\}$. For $n > 3$ we have that $(A_n)_n = A_{n-1}$, and A_{n-1} is $(n-3)$-transitive on $\{1, 2, \cdots, n-1\}$ by the induction hypothesis. So A_n is $(n-2)$-transitive, by Lemma 2.8. Now suppose that A_n is $(n-1)$-transitive, then there is $g \in A_n$ fixing each $1, 2, \cdots, n-2$ and taking $n-1$ to n. But the only $g \in A_n$ which does this is the transposition $(n-1\ n) \notin A_n$. ■

Theorem 2.15. *Every k-transitive group G (with $k \geq 2$) acting on a set Ω, is primitive.*

Proof: See [8, Lemma 1.6.3]. ■

Theorem 2.16 (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 [8, Theorem 1.6.5]. ■

By Theorem 2.16 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 from Theorem 2.6 that a transitive action is equivalent to an action on the coset space G/H. In view of this and Theorem 2.16 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 groups in the later chapters.

2.5 Rank-3 primitive permutation groups

In this section we consider finite primitive permutation groups of rank-3. Given a transitive permutation group G on Ω, the number of orbits of the point stabilizer G_α is independent of the particular $\alpha \in \Omega$ and it is equal to the rank of G. From Section 2.1 we know that for $|\Omega| \geq 2$ we have rank$(G) \geq 2$.

If G is a transitive permutation group on Ω of rank-3 then we say that G is a rank-3 permutation group. In this case G_α has exactly three orbits $\{\alpha\}$, $\Delta(\alpha)$ and $\Gamma(\alpha)$.

The above notation is used in such a way that $\Delta(\alpha)^g = \Delta(\alpha^g)$ and $\Gamma(\alpha)^g = \Gamma(\alpha^g)$ for all $\alpha \in \Omega$ and $g \in G$ so that by setting $|\Delta(\alpha)| = k$ and $|\Gamma(\alpha)| = l$ we get that $|\Omega| = n = 1 + k + l$.

The study of finite primitive permutation groups has lead to the discovery of interesting new groups (for instance, some sporadic simple groups) and to application of new techniques in the theory of permutation groups. For more information on rank-3 permutation groups the reader should consult [52, 68, 26, 75, 86, 87] and [65,

Section 2].

In light of the matter we dealt with we will give a brief account of linear, symplectic and alternating groups. For these latter groups, we present them as examples of finite primitive permutation groups of rank-3. In the next section we deal with linear groups followed by a discussion on the symplectic groups in Section 2.7 and the alternating groups in Section 2.8.

2.6 Linear groups

We describe the linear groups and discuss the action of the projective groups on the points of the projective space. We start by defining a linear transformation on a vector space. For the classical background on symplectic forms and symplectic groups, the reader should consult [3, 68, 26, 1, 106, 118].

Let V and W be two vector spaces over a field $\mathbb{F}$. A vector space homomorphism $T : V \longrightarrow W$ such that $T(v_1 + v_2) = T(v_1) + T(v_2)$ and $T(cv) = cT(v)$ for all $c \in \mathbb{F}$ and $v, v_1, v_2 \in V$, is called a **linear transformation**. The set of all linear transformations $T : V \longrightarrow W$ is denoted $\mathrm{Hom}_{\mathbb{F}}(\mathrm{V}, \mathrm{W})$, and if $V = W$, the homomorphism $T : V \longrightarrow V$ is called an endomorphism and $\mathrm{Hom}_{\mathbb{F}}(\mathrm{V}, \mathrm{V})$ is denoted by $\mathrm{End}_{\mathbb{F}}(\mathrm{V})$. A linear transformation T which is one-to-one and onto is called **invertible**.

2.6.1 The general linear group

Definition 2.17. *The* **general linear group** *denoted $GL(V)$, is the group of all invertible endomorphisms on a vector space V over a field $\mathbb{F}$ under addition and composition of maps.*

If V is a vector space of dimension n over a finite field $\mathbb{F} = GF(q)$ by choosing a basis, we can identify the vector space V with the space $\mathbb{F}_q^n$ of the n-tuples of elements of $\mathbb{F}$. In this case any linear transformation of V can be represented by an invertible $n \times n$ matrix acting on $\mathbb{F}$ by right multiplication. It can be seen that the general

linear group is in fact the group of all invertible $n \times n$ matrices over $\mathbb{F}$ with matrix multiplication and is denoted by $GL(n, q)$. For $n = 1$ we have $GL(1, \mathbb{F}) \cong \mathbb{F}^*$ where $\mathbb{F}^*$ is the multiplicative group of the field. The general linear group is generally not a simple group apart from some exceptional cases.

Let V be a n-dimensional space over $\mathbb{F}$. Suppose we denote by $[v] = \{av : a \in \mathbb{F}\}$ the line through the origin spanned by a vector $v \in V$. Then $[v]$ is called a projective point. The set of all projective points in V has dimension $q - 1$ and is called a **projective space** based on V. We denote this space by $P(V)$ or $PG(n - 1, q)$.

The elements of $GL(n, q)$ map a subspace to another subspace of same dimension. Therefore $GL(n, q)$ acts naturally on the points of the projective space $PG(n - 1, q)$ where the action is given by $T[v] = [Tv]$ for all $T \in GL(n, q)$. This action is faithful and the kernel of the action is $Z(GL(n, q))$. It has been shown (see [26, Proposition 2.1] that

$$Z(GL(n, q)) = \{cI_n : c \neq 0, c \in \mathbb{F}\}$$

where I_n is the $n \times n$ identity matrix, is a normal subgroup of $GL(n, q)$ consisting of all scalar matrices of $GL(n, q)$. This is a cyclic group whose order is $q - 1$. If we factor out $GL(n, q)$ by the kernel we get the projective group. So we define:

Definition 2.18. *The quotient group of $GL(n, q)$ by its center is called the* **projective general linear group** *and is denoted $PGL(n, q)$.*

Therefore

$$PGL(n, q) = GL(n, q)/Z(GL(n, q)) = GL(n, q)/\mathbb{F}^*.$$

Theorem 2.19.

$$|GL(n, q)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$$
$$|PGL(n, q)| = \frac{|GL(n, q)|}{(q - 1)}$$

Proof: The rows of an invertible matrix are linearly independent and will be determined by the image of its ordered basis. The $(k - 1)$-th vector spans a vector

space of dimension $k-1$. This vector space has q^{k-1} vectors. The k-th vector must be independent of the previous ones and therefore will have $q^n - q^{k-1}$ choices. Multiplying these for $1 \leq k \leq n$ we get the result.
The second part follows since there are $q-1$ non-zero scalars in $\mathbb{F}$. ■

2.6.2 Projective special linear group

Among the important groups constructed from the general linear group are the special linear group and projective special linear group. The **special linear group** is the subgroup of $GL(V)$ consisting of all unimodular linear transformations or in terms of matrices the group of all $n \times n$ matrices with determinant 1. It is denoted $SL(V)$ or $SL(n,q)$. Equivalently if we define the determinant map $\phi : GL(n,q) \longrightarrow \mathbb{F}$ by $\phi(v) = \det(v)$ then since

$$\phi(uv) = \det(uv) = \det(u)\det(v) = \phi(u)\phi(v)$$

we have that ϕ is an onto homomorphism. The Ker $\phi = \{v \in GL(n,q) : \det(v) = 1_{\mathbb{F}}\}$ is a normal subgroup of $GL(n,q)$ consisting of the matrices whose determinant is 1. This subgroup is in fact the special linear group. We thus have $SL(n,q) \trianglelefteq GL(n,q)$ and so $GL(n,q)$ is generally not a simple group.

$SL(n,q)$ induces an action on the projective space $PG(n-1,q)$ whose kernel is the subgroup

$$Z(SL(n,q)) = \{cI_n : 0 \neq c \in \mathbb{F} \text{ and } c^n = 1\}$$

normal in $SL(n,q)$ consisting of all scalar matrices with determinant 1. The order of $Z(SL(n,q))$ is found by taking $\gcd(q-1,n)$.

The **projective special linear** group $PSL(n,q)$ is defined as the quotient group of $SL(n,q)$ by its center i.e.,

$$PSL(n,q) = \frac{SL(n,q)}{Z(SL(n,q))} = \frac{SL(n,q)}{\{cI_n : 0 \neq c \in \mathbb{F} \text{ and } c^n = 1\}}$$

Theorem 2.20. *The groups $SL(n,q)$ and $PSL(n,q)$ have order:*

$$|SL(n,q)| = |GL(n,q)|/(q-1)$$

$$|PSL(n,q)| = |SL(n,q)|/(n,q-1),$$

repectively, where $(n, q-1)$ *is the* gcd *of* n *and* $q-1$.

Proof: The proof is clear from the definition and Theorem 2.19. ■

In this thesis we shall use the notation of the $\mathbb{ATLAS}$ of finite groups [34], and thus write $L_n(q)$ for $PSL(n, q)$.

Theorem 2.21. *The projective special linear groups* $PSL(n, q)$ *is a simple group except for* $PSL_2(2)$ *and* $PSL_2(3)$.

Proof: The groups $PSL(2, 2) \cong S_3$ of order 6 which has A_3 as a normal subgroup and $PSL(2, 3) \cong A_4$ which has a normal subgroup of order 4. See [111, Theorem 4.5] for the proof of simplicity for the remaining groups. ■

Theorem 2.22. *The group* $SL(n, q)$ *and therefore* $PSL(n, q)$ *acts double transitively on the points of the projective geometry* $PG(n-1, q)$.

Proof: Let $[x] \neq [y]$ and $[x'] \neq [y']$ be two ordered pairs of points in $PG(n-1, q)$. (Recall that projective points are simply lines in the underlying vector space $V(n, q)$). Then $\{x, y\}$ and $\{x', y'\}$ are both linearly independent pairs in $V(n, q)$ so we may choose them as the first two elements of the basis of $V(n, q)$. Then we choose $g \in GL(n, q)$ such that $g(x) = x'$ and $g(y) = y'$. If this $g \in GL(n, q)$ we have chosen has $\det(g) = \lambda \neq 1$ then we may replace y by λy and repeat the argument to obtain $\bar{g} \in GL(n, q)$ with $\det(\bar{g}) = 1$. Since $[\lambda y] = [y]$, it follows that $\bar{g} \in PSL(n, q)$ has the same property as g. This shows that the group $SL(n, q)$ and therefore $PSL(n, q)$ act doubly transitively on the points of the projective geometry $PG(n-1, q)$. ■

2.7 Symplectic groups

For the classical background on the symplectic forms and symplectic groups see [2, 49, 68, 111]. Most parts of the discussion in this section can also be found readily available in [102, 101]. We give a brief but sufficient overview of the symplectic groups necessary for the purposes of the thesis.

Definition 2.23. *Let V be a finite dimensional vector space over a field $\mathbb{F}$. A function $\langle , \rangle$ from the set $V \times V$ of ordered pairs in V to $\mathbb{F}$ is called a* **bilinear form** *on V if for each $v \in V$, the functions $\langle v, \ \rangle$ and $\langle \ , v\rangle$ are linear functionals on V. In this case we say that $(V, \langle , \rangle)$ is an* **inner product space.**

If $\langle , \rangle$ is a bilinear form on V such that for each non-zero $x \in V$, there exists $y \in V$ for which $\langle x, y\rangle \neq 0$, then $\langle , \rangle$ is said to be **non-degenerate.**

Remark 2.24. A bilinear form $\langle , \rangle$ is called **alternating** (**symplectic**) on V if $\langle x, x\rangle = 0$ for all $x \in V$.

Let V be a vector space over a field $\mathbb{F}$ and $\langle , \rangle$ be a symplectic form on V. If $char(\mathbb{F}) \neq 2$ then we obtain that for all $x, y \in V$,

$$0 = \langle x + y, x + y\rangle = \langle x + y, x\rangle + \langle x + y, y\rangle = \langle x, x\rangle + \langle y, x\rangle + \langle x, y\rangle + \langle y, y\rangle.$$

However, since $\langle x + y, x + y\rangle = \langle x, x\rangle = \langle y, y\rangle = 0$ we have that $\langle x, y\rangle = -\langle y, x\rangle$. Conversely if $\langle , \rangle$ is a bilinear form for which $\langle x, y\rangle = -\langle y, x\rangle$ for all $x, y \in V$, then in particular for $x \in V$ we have $\langle x, x\rangle = -\langle x, x\rangle$. This implies that $2\langle x, x\rangle = 0$ and so $\langle x, x\rangle = 0$, for all $x \in V$.

Definition 2.25. *Let V be a vector space over a field $\mathbb{F}$. Let $\langle , \rangle : V \times V \longrightarrow \mathbb{F}$ be a bilinear form on V such that*
(i) $\langle x, x\rangle = 0, \quad$ for all $x \in V$
(ii) $\langle x, y\rangle = -\langle y, x\rangle, \quad$ for all $x, y \in V$.
Then we say that $(V, \langle , \rangle)$ is a **symplectic space** *over the field $\mathbb{F}$.*

Remark 2.26. If $char(\mathbb{F}) \neq 2$, then the properties (i) and (ii) in the above definition are equivalent.

Let $(V, \langle , \rangle)$ and $(U, \langle , \rangle)$ be symplectic spaces over $\mathbb{F}$, then we say that $V \cong U$ if there exists an isomorphism $T \in Hom_{\mathbb{F}}(V, U)$ such that for all $x, y \in V$ we have $\langle x, y\rangle = \langle T(x), T(y)\rangle$.

Definition 2.27. *Let $(V, \langle , \rangle)$ be a symplectic space. If $x, y \in V$, then x and y are* **orthogonal** *if $\langle x, y\rangle = 0$. If W is a subspace of V then the* **orthogonal**

complement *of W is defined by*

$$W^{\perp} = \{y \in V \mid \langle x, y\rangle = 0, \ for\ all\ \ x \in W\}.$$

Note 2.28. Note that for all $x \in W$ we have $\langle 0, x\rangle = \langle x - x, x\rangle = \langle x, x\rangle - \langle x, x\rangle = 0 - 0 = 0,$ so that $0 \in W^{\perp}$. Now if $x, y \in W^{\perp}$, then for any $\alpha, \beta \in F$ and $z \in W$ we have

$$\langle \alpha x + \beta y, z\rangle = \langle \alpha x, z\rangle + \langle \beta y, z\rangle = \alpha\langle x, z\rangle + \beta\langle y, z\rangle = \alpha 0 + \beta 0 = 0,$$

therefore $\alpha x + \beta y \in W^{\perp}$, and hence $W^{\perp}$ is a subspace of V.

Let $(V, \langle , \rangle)$ be a symplectic space and define $R(V)$ by $R(V) = V^{\perp}$. Then $R(V)$ is called the **radical** of V. We can easily see that $(V, \langle , \rangle)$ is non-degenerate if and only if $R(V) = \{0_V\}$.

Definition 2.29. *In an inner product space $(V, \langle\, , \rangle)$, a vector v is called* **isotropic** *if $\langle v\, , v\rangle = 0$. A subspace U of V is called isotropic if there exists in U a non-zero vector z such that it is orthogonal to V.*

It is clear that in a symplectic space every vector is isotropic.

Note 2.30. Definition 2.29 suggests that U being isotropic is equivalent to $\langle , \rangle$ being degenerate when restricted to U. This in turn equivalent is to $U \cap U^{\perp} \neq V$. A subspace U is called totally isotropic if all its vectors are isotropic. Having U being totally isotropic is equivalent to having any two vectors in U orthogonal. This then implies that $U \subseteq U^{\perp}$.

Definition 2.31. *Consider $(V, \langle , \rangle)$ with $\langle , \rangle$ bilinear . If $\{v_1, v_2, \ldots, v_m\}$ is an ordered basis of V, then the* **inner product matrix** *of $\langle , \rangle$ relative to this basis is given by an $m \times m$ matrix $A = [\langle v_i, v_j\rangle]_{m\times m}$.*

If $(V, \langle , \rangle)$ is a symplectic space of dimension $2m$ then the form is given by

$$\langle u, v\rangle = uMv^T \tag{2.1}$$

where a basis $\{e_1, e_2, \ldots, e_{2m}\}$ for V can be chosen such that $M = [m_{i,j}]$ is the $2m \times 2m$ matrix given as follows: if B is the $m \times m$ matrix $[b_{i,j}]$ where $b_{i,j} = 1$ if $i + j = m + 1$, and $b_{i,j} = 0$ otherwise, that is

$$B = \begin{bmatrix} & & & & 1 \\ & & & 1 & \\ & & \cdot & & \\ & \cdot & & & \\ & 1 & & & \\ 1 & & & & \end{bmatrix},$$

then

$$M = \begin{bmatrix} 0 & -B \\ B & 0 \end{bmatrix}.$$

Thus

$$\langle e_i, e_j \rangle = e_i M e_j^T = 0$$

if $i + j \neq 2m + 1$, and

$$\langle e_i, e_{2m+1-i} \rangle = e_i M e_{2m+1-i}^T = -1$$

for $1 \leq i \leq m$, and

$$\langle e_i, e_{2m+1-i} \rangle = e_i M e_{2m+1-i}^T = 1$$

for $m + 1 \leq i \leq 2m$.

The **symplectic group** $Sp_{2m}(q)$ is the subgroup of $GL_{2m}(q)$ of transformations g for which $\langle u^g, v^g \rangle = \langle u, v \rangle$, for all $u, v \in V$. That is, it is matrix Q for which $QMQ^T = M$. The **projective symplectic group** $PSp_{2m}(q)$ is the factor group $Sp_{2m}(q)/Z(Sp_{2m}(q))$ and we have

$$\begin{aligned} Z(Sp_{2m}(q)) &= \{I\} \quad if \quad char(\mathbb{F}_q) = 2 \ \ and \\ Z(Sp_{2m}(q)) &= \{I, -I\} \quad if \ \ char(\mathbb{F}_q) \neq 2. \end{aligned}$$

The projective symplectic groups are simple except for $PSp_2(2) = PSL_2(2)$,

$PSp_2(3) = PSL_2(3)$ and $PSp_4(2)$. The order of $PSp_{2m}(q)$ is given by

$$\begin{aligned} |PSp_{2m}(q)| &= \frac{1}{(2, q-1)} \times |Sp_{2m}(q)| \\ &= \frac{q^{n^2}}{(2, q-1)} \prod_{i=1}^{n} (q^{2i} - 1). \end{aligned}$$

Now if we let $\mathcal{P}(V)$ denote the projective space defined by V, that is $\mathcal{P}(V) = PG_{2m-1}(q)$ (see Section 4.4 for more details on projective geometry) then the symplectic form on V defines a **polarity** on $\mathcal{P}(V)$, a correspondence between the elements of $\mathcal{P}(V)$ that reverses inclusion and has order 2. If we denote this polarity by σ, then for any $U \in \mathcal{P}(V)$ we have $\sigma : U \mapsto U^\sigma$ where

$$U^\sigma = \{v \mid v \in V,\ uMv^T = 0,\ \ for\ all,\ \ u \in U\}. \tag{2.2}$$

It can be shown that $PSp_{2m}(q)$ is the group of all the collineations of $\mathcal{P}(V)$ that commute with the polarity σ.

In the context of projective space, the subspace $U \in \mathcal{P}(V)$ is called **totally isotropic** if $U \cap U^\sigma = U$, **isotropic** if $U \cap U^\sigma \neq \varnothing$ and **non-isotropic** if $U \cap U^\sigma = \varnothing$. We can see that for symplectic polarity, points are always totally isotropic. Any totally isotropic space has dimension at most m, and those subspaces of dimension m are called **maximal isotropic** subspaces. A point P of $\mathcal{P}(V)$ is said to be **absolute** if P lies on P^σ.

If P is a point of the projective $(2m-1)$-space $PG_{2m-1}(q)$ then the affine subgroup of $G = PSp_{2m}(q)$ is the stabilizer G_P of the form $N : PSp_{2m-2}(q)$, a split extension, where N is a p-group of order q^{2m-1} (see [57]).

If $q = p^r$ where p is an odd prime, N will be a non-abelian special p-group of order q^{2m-1}. If $p = 2$, then N is an elementary abelian 2-group. For further information on the affine subgroups of the symplectic group, see ([101, Chapter 10]).

The simple symplectic group $PSp_{2m}(q)$, where m is at least 2 and q is any prime power, acts as a primitive rank-3 group of degree $\frac{q^{2m}-1}{q-1}$ on the points of the projective $(2m-1)$-space $PG_{2m-1}(\mathbb{F}_q)$, (see Theorem 2.32). The orbits of the stabilizer of a point P consist of $\{P\}$ and one of length $\frac{q^{2m-1}-1}{q-1} - 1$ and the other of length q^{2m-1}.

Theorem 2.32. *If $m \geq 2$, then $PSp_{2m}(q)$ acts as a primitive permutation group of rank-3 on the points of $\mathcal{P}(V)$.*

Proof: See [111, Theorem 8.2 and Theorem 8.3]. ■

2.8 Alternating groups

For a set Ω of size n the notation $\Omega^{\{k\}}$ is used to denote the set of all k-subsets (a set of k unordered elements) of Ω for $1 \leq k \leq n$. If $k = 2$ we call $\Omega^{\{2\}}$ the set of all **duads** of Ω following the $\mathbb{ATLAS}$ notation (see [34]). Since $|\Omega| = n$ we have $|\Omega^{\{k\}}| = \binom{n}{k}$. A group G acting on Ω is called k-homogeneous if it is transitive on the set $\Omega^{\{k\}}$. Clearly k-transitivity implies k-homogeneity. If $\Upsilon = \{\sigma_1, \sigma_2, \cdots, \sigma_k\}$ is a k-subset of Ω, then the stabilizer of the "point" Υ in the action of G on $\Omega^{\{k\}}$ is the setwise stabilizer G_Υ in the action of G in Ω. The pointwise stabilizer of Υ in the action of G on Ω is denoted by $G_{[\Upsilon]}$. Obviously $G_{[\Upsilon]} \leq G_\Upsilon$. The permutation representation of G_Υ associated with its action on Υ defines a homomorphism of G_Υ into the symmetric group $S_\Upsilon \cong S_k$ with kernel $G_{[\Upsilon]}$ and so the factor group $G_\Upsilon/G_{[\Upsilon]}$ is isomorphic to a subgroup of S_k.

Lemma 2.33. *If $n \geq 3$ then the alternating group A_n acts transitively on $\Omega^{\{2\}}$ the set of duads of $\Omega = \{1, 2, \cdots, n\}$.*

Proof: For if we let $\{\sigma_1, \sigma_2\}$ and $\{\sigma_3, \sigma_4\}$ be duads in $\Omega^{\{2\}}$, then the permutation $(\sigma_1\ \sigma_3)(\sigma_2\ \sigma_4) \in A_n$ moves them accordingly.■

We now look at the structure of the stabilizer $(A_n)_\Upsilon$ of $\Upsilon = \{\sigma_1, \sigma_2\} \in \Omega^{\{2\}}$ and show that $(A_n)_\Upsilon \cong S_{n-2} = (S_n)_{\{\sigma_1, \sigma_2\}}$.

Theorem 2.34. *The alternating group A_n where $n \geq 5$ acts primitively as a rank-3 permutation group of degree $\frac{n(n-1)}{2}$ on $\Omega^{\{2\}}$ where $\Omega = \{1, 2, \cdots, n\}$.*

Proof: That the action is transitive follows from Lemma 2.33. Since A_n acts on $\Omega^{\{2\}}$ and $|\Omega^{\{2\}}| = \binom{n}{2}$ we have that

$$|(A_n)_{\{\sigma_1,\, \sigma_2\}}| = \frac{n!}{2} \times \frac{2}{n(n-1)} = (n-2)!. \tag{2.3}$$

Now

$$\begin{aligned}(A_n)_{\{\sigma_1,\,\sigma_2\}} &= \{g \in A_n \mid \{\sigma_1,\sigma_2\}^g = \{\sigma_1,\sigma_2\}\} \\ &= \{g \in A_n \mid {\sigma_1}^g = \sigma_1, {\sigma_2}^g = \sigma_2 \ \text{ or } \ {\sigma_1}^g = \sigma_2, {\sigma_2}^g = \sigma_1\}.\end{aligned}$$

Clearly

$$(A_n)_{[\sigma_1,\sigma_2]} = A_{n-2} \leq (A_n)_{\{\sigma_1,\,\sigma_2\}}$$

and

$$K = \{(\sigma_1\ \sigma_2)\cdot\alpha \mid \alpha \in (S_n)_{[\sigma_1,\sigma_2]},\ \ \alpha \text{ is odd}\} \subseteq (A_n)_{\{\sigma_1,\,\sigma_2\}}.$$

Thus $A_{n-2} \cup K \leq (A_n)_{\{\sigma_1,\,\sigma_2\}}$ and

$$|A_{n-2}\cup K| = |A_{n-2}|+|K| = 2|A_{n-2}| = \frac{2(n-2)!}{2} = (n-2)! = |(A_n)_{\{\sigma_1,\,\sigma_2\}}|, \quad \text{by 2.3 .}$$

Hence $(A_n)_{\{\sigma_1,\,\sigma_2\}} = A_{n-2} \cup K$. Since

$$(A_n)_{\{\sigma_1,\sigma_2\}} \leq A_n, \quad |(A_n)_{\{\sigma_1,\,\sigma_2\}}| = 2|A_{n-2}| = |S_{n-2}|$$

and $A_{n-2} = (A_n)_{[\sigma_1,\sigma_2]} \leq (A_n)_{\{\sigma_1,\sigma_2\}}$, we can deduce that $(A_n)_{\{\sigma_1,\,\sigma_2\}} \cong S_{n-2}$.

The group $(A_n)_{\{\sigma_1,\,\sigma_2\}}$ has three orbits $\{\{\sigma_1,\ \sigma_2\}\}$, $\{\sigma_i,\gamma \mid i \in \{1,2\},\gamma \in \Omega \setminus \{\sigma_1,\ \sigma_2\}\}$ and $\{\gamma,\mu \mid \gamma,\mu \in \Omega \setminus \{\sigma_1,\ \sigma_2\},\gamma \neq \mu\}$. These orbits have lengths 1, $2(n-2)$ and $\frac{(n-2)(n-3)}{2}$, respectively. Now any non-trivial block for the action of A_n on $\Omega^{\{2\}}$ which contains the point $\{\sigma_1,\sigma_2\}$ must also contain one of the other orbits of $(A_n)_{\{\sigma_1,\,\sigma_2\}}$. However, a simple argument shows that for $n \neq 4$ such a block must also contain the other orbit, and so the action of A_n on $\Omega^{\{2\}}$ is primitive. Now since $(A_n)_{\{\sigma_1,\,\sigma_2\}}$ is the stabilizer of a point in the action of A_n on $\Omega^{\{2\}}$ and A_n is primitive we have that $(A_n)_{\{\sigma_1,\,\sigma_2\}}$ is maximal. ■

Remark 2.35. If $n = 4$, then Theorem 2.34 is not true since $(A_4)_{\{\sigma_1,\,\sigma_2\}} \cong S_2 = \{1_{S_2},(\sigma_1\ \sigma_2)(\sigma_3\ \sigma_4)\}$ and A_4 is clearly not a rank-3 group on $\Omega^{\{2\}}$ where $\Omega = \{1,2,3,4\}$.

Groups that act two-transitively yield two designs as we shall see in Section 5.4. A group G acts sharply transitively on a set Ω if its action is regular, that is, it is transitive and the stabilizer of a point is the identity.

Chapter 3

Representations and modules

In this section we give some preliminary results on representations and characters of groups which will be needed in later chapters. We note that in this section $\mathbb{F}$ is a field and V is a finite-dimensional vector space over $\mathbb{F}$. References for this section include [9, 90, 94, 72, 100].

3.1 Representations

Definition 3.1. Let G be a finite group and let V be a vector space of dimension n over the field $\mathbb{F}$. Then a homomorphism $\rho : G \longrightarrow GL(n, \mathbb{F})$ is said to be a **matrix representation** of G of **degree** n over the field $\mathbb{F}$. The column space, $\mathbb{F}^{n\times 1}$ of ρ is called the **representation module** of ρ. If the characteristic of $\mathbb{F}$ is zero then ρ is called an **ordinary representation** while a representation over a field of non-zero characteristic is called a **modular representation**.

Remark 3.2. (i) A representation $\rho : G \longrightarrow GL(n, \mathbb{F})$ is said to be **injective** if the kernel $\mathrm{Ker}(\rho) = \{1_G\}$. An injective representation is called a **faithful representation** in which case $G \cong \mathrm{Im}(\rho)$ so that G is isomorphic to a subgroup of $GL(n, \mathbb{F})$.

(ii) Every group has a degree 1 matrix representation $\rho : G \longrightarrow GL(1, \mathbb{F}) = \mathbb{F}^*$ defined by $\rho(g) = 1_{\mathbb{F}}$ for all, $g \in G$. This representation is called the **trivial**

representation.

Definition 3.3. Let $\rho : G \longrightarrow GL(n, \mathbb{F})$ be a representation of G over the field $\mathbb{F}$. The function $\chi : G \longrightarrow \mathbb{F}$ defined by $\chi(g) = \text{trace}(\rho(g))$ is called the **character** of ρ. If $\phi : G \to F$ is a function that is constant on conjugacy classes of G i.e., $\phi(g) = \phi(\alpha g \alpha^{-1})$ 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.

Recall from linear algebra that, if V is a finite dimensional $\mathbb{F}$-vector space then $GL(V) \cong GL(n, \mathbb{F})$. Hence given any $g \in G$ and a representation $\varrho : G \longrightarrow GL(V)$, $\varrho(g) \in GL(V)$ and if we let $\mathfrak{B} = \{v_1, \ldots, v_n\}$ be a basis for V then we obtain that the corresponding matrix representation $\rho(g) \in GL(n, \mathbb{F})$ with respect to the basis $\mathfrak{B}$ is given by $\rho(g) = [a_{ij}]$ where

$$\rho(g)(v_j) = \sum_{i=1}^{n} a_{ij} v_i.$$

Similarly, if we are given an invertible matrix representation $\rho : G \longrightarrow GL(n, \mathbb{F})$ then for $\rho(g) \in GL(n, \mathbb{F})$ it follows that we can define a representation $\varrho : G \longrightarrow GL(V)$ by $\varrho(g)(v) = \rho(g)v$ where $v \in \mathbb{F}^{n \times 1}$ is a column vector in the column space of $\rho(g)$ with respect to the standard basis. Seeing that we can describe a representation in terms of a matrix with respect to some basis, it is clear that we should be able to define what it means for two representations to be equivalent.

Definition 3.4. *Two matrix representations ρ_1 and ρ_2 of G are said to be* **equivalent representations** *if there exists $P \in GL(n, \mathbb{F})$ such that $\rho_2(g) = P\rho_1(g)P^{-1}$ for all, $g \in G$.*

Thus, whenever we consider a representation, it is only considered up to equivalence. We next discus the concepts of reducibility and decomposability of representations.

Definition 3.5. *Let $\rho : G \longrightarrow GL(n, \mathbb{F})$ 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 $g \longmapsto \rho(g)|_W$ is a representation of G*

called a **subrepresentation** *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 3.6. *A representation $\rho : G \longrightarrow GL(n, \mathbb{F})$ 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.*

Suppose $\rho : G \longrightarrow GL(n, \mathbb{F})$ is a **reducible matrix representation** with $U \subseteq \mathbb{F}^{n\times 1}$ and $\dim_{\mathbb{F}} U = m$ then we can choose a basis $\mathfrak{C}$ for U that can be extended to a basis $\mathfrak{B}$ of $V = \mathbb{F}^{n\times 1}$ so that ρ has the form

$$\rho(g) = \begin{pmatrix} \beta(g) & \gamma(g) \\ 0 & \delta(g) \end{pmatrix}$$

for all $g \in G$, where $\beta(g) = \rho_1(g)$, and $\delta(g) = \rho_2(g)$ are matrix representations $\rho_1 : G \longrightarrow GL(m, \mathbb{F})$ and $\rho_2 : G \longrightarrow GL(n-m, \mathbb{F})$ of G respectively. That is the first m columns of ρ are formed by the basis $\mathfrak{C}$ of the subspace U.

The representation module V of an irreducible representation is called **simple** and the ρ-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 3.7. *Let $\rho_1 : G \to GL(n, \mathbb{F})$ and $\rho_2 : G \to GL(n', \mathbb{F})$ be two representations, their direct sum $\rho_1 \oplus \rho_2 : G \to GL(n+n', \mathbb{F})$ is defined by*

$$g \mapsto \begin{bmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{bmatrix}.$$

Definition 3.8. *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**.

Suppose that $\rho : G \longrightarrow GL(n, \mathbb{F})$ is decomposable with G-invariant subspaces U and W i.e., $V = U \oplus W$. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be the basis of the G-subspaces U and W

respectively, then with respect to the basis $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ the matrix representation will be of form:

$$[\rho_g]_{\mathcal{B}} = \begin{bmatrix} [\rho_U(g)]_{\mathcal{B}_1} & 0 \\ 0 & [\rho_W(g)]_{\mathcal{B}_1} \end{bmatrix}.$$

Definition 3.9. *A representation ρ is said to be* **completely reducible or semi-simple** *if it is the direct sum of irreducible representations.*

From the definition we deduce that a completely reducible representation is reducible, however the converse is not necessarily true.

3.2 $\mathbb{F}G$-modules

The main result of this section will describe the correspondence 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. In the sequel we will expound on the correspondence between $\mathbb{F}G$-modules and G-invariant subspaces (it will become apparent later that these are in fact linear codes).

It is worth noting that it is possible to formulate representation theory in the more general context of algebras instead of groups, see for example [88]. In this situation a ring homomorphism $\rho : \mathbb{F}G \longrightarrow \mathrm{End}_{\mathbb{F}}(V)$, where $\mathbb{F}G$ is the group ring of G over $\mathbb{F}$, restricts to a representation of G. In such context V can be viewed as both a vector space over $\mathbb{F}$ and a $\mathbb{F}G$-module through the ring homomorphism ρ.

Definition 3.10. *Let G be a finite group and $\mathbb{F}$ be a field. The* **group ring** *of G over $\mathbb{F}$ is the set of all formal sums of the form*

$$\sum_{g \in G} \lambda_g g, \quad \lambda_g \in \mathbb{F}$$

with componentwise addition and multiplication $(\lambda_g)(\mu_h) = (\lambda\mu)(gh)$ (where λ and μ are multiplied in $\mathbb{F}$ and gh is the product in G) extended to sums by means of the distributive law.

It is a straightforward to verify that the group ring $\mathbb{F}G$ is a vector space over $\mathbb{F}$; and thus we can form $\mathbb{F}G$-modules. In this section we will depict the interplay between representations of G and $\mathbb{F}G$-modules. In particular, our interest will be in the correspondence between $\mathbb{F}G$-modules and G-invariant subspaces (later we will note that these are indeed the codes).

In what follows we give a brief but somewhat complete overview which depicts the correspondence between representations of G and $\mathbb{F}G$-modules. For this we write $G = \{g_1, g_2, \ldots, g_n\}$ and let $\rho : G \longrightarrow GL(V)$ be a representation of G on a vector space V over $\mathbb{F}$. Then $\rho(g_i)$ is a linear map from V into itself for $i \in \{1, 2, \ldots, n\}$. In this way V is made into an $\mathbb{F}G$ by defining

$$\left(\sum_{i=1}^{n} \lambda_i g_i\right) \cdot u = \sum_{i=1}^{n} \lambda_i \rho(g_i)(u) \quad \text{for all } \sum_{i=1}^{n} \lambda_i g_i \in \mathbb{F}G \text{ and } u \in V.$$

We now verify the axioms of a module. It is evident that V is an abelian group under addition. Now, for $\sum_{i=1}^{n} \lambda_i g_i$, $\sum_{i=1}^{n} \mu_i g_i \in \mathbb{F}G$ and $u, v \in V$ we verify:

$$\begin{aligned}
\left(\sum_{i=1}^{n} \lambda_i g_i + \sum_{i=1}^{n} \mu_i g_i\right) \cdot u &= \left(\sum_{i=1}^{n} (\lambda_i + \mu_i) g_i\right) \cdot u \\
&= \sum_{i=1}^{n} (\lambda_i + \mu_i) \rho(g_i)(u) = \sum_{i=1}^{n} \lambda_i \rho(g_i)(u) + \sum_{i=1}^{n} \mu_i \rho(g_i)(u) \\
&= \left(\sum_{i=1}^{n} \lambda_i g_i\right) \cdot u + \left(\sum_{i=1}^{n} \mu_i g_i\right) \cdot u,
\end{aligned}$$

and

$$\begin{aligned}
\left(\sum_{i=1}^{n} \lambda_i g_i\right) \cdot (u + v) &= \sum_{i=1}^{n} \lambda_i \rho(g_i)(u + v) = \sum_{i=1}^{n} \lambda_i \rho(g_i)(u) + \sum_{i=1}^{n} \lambda_i \rho(g_i)(v) \\
&= \left(\sum_{i=1}^{n} \lambda_i g_i\right) \cdot (u) + \left(\sum_{i=1}^{n} \lambda_i g_i\right) \cdot (v).
\end{aligned}$$

For associativity we have that

$$\begin{aligned}
(g_i g_j) \cdot u &= \rho(g_i g_j)(u) \\
&= (\rho(g_i) \circ \rho(g_j))(u) = \rho(g_i)(\rho(g_j)(u)) = g_i \cdot (g_j \cdot (u)).
\end{aligned}$$

Now we extend this linearly to arbitrary elements of $\mathbb{F}G$.

Conversely, suppose that V is an $\mathbb{F}G$-module. Then V is also an $\mathbb{F}$-module, i.e., a vector space over $\mathbb{F}$. For each $g \in G$ we obtain a map $\rho(g) : V \longrightarrow V$ defined by

$$\rho(g)(u) = g \cdot u \text{ for all } u \in V$$

where $\cdot$ is the action of $\mathbb{F}G$ on V. We intend showing that for each $g \in G$, $\rho(g)$ is a linear map. However if we show in addition that ρ is a homomorphism we would have proven that $\rho : G \longrightarrow GL(V)$ is a representation of G. Again we appeal to the properties of modules to see that

$$\begin{aligned} \rho(g)(\lambda u + \mu v) &= g \cdot (\lambda u + \mu v) \\ &= g \cdot \lambda u + g \cdot \mu v \\ &= \lambda(g \cdot u) + \mu(g \cdot v) \\ &= \lambda\rho(g)(u) + \mu\rho(g)(v). \end{aligned}$$

Thus $\rho(g)$ is a linear map. To show that ρ is linear we have

$$\begin{aligned} \rho(g_i g_j)(u) &= (g_i g_j) \cdot u \\ &= g_i \cdot (g_j \cdot u) \\ &= (\rho(g_i) \circ \rho(g_i))(u). \end{aligned}$$

The above discussion shows that having a representation $\rho : G \longrightarrow GL(V)$ of G on a vector space V over $\mathbb{F}$ is equivalent to having an $\mathbb{F}G$-module, thus we have

Theorem 3.11. *[1] If $\mathbb{F}$ is a field and G a finite group, then there is a bijective correspondence between finitely generated FG-modules and representations of G on finite-dimensional $\mathbb{F}$-vector spaces.*

We therefore digress from representations to $\mathbb{F}G$-modules to discuss some basic concepts used in module theory. The definitions stated here have their equivalent stated in representation theory.

Definition 3.12. *Let V be an $\mathbb{F}G$-module, a subspace W of V which itself is an $\mathbb{F}G$-module is called an $\mathbb{F}G$-***submodule** *of V i.e., $gw \in W$, for all$w \in W$.*

An $\mathbb{F}G$-submodule is therefore a subspace of V which is invariant under the action of G. Clearly the submodules 0 and V are $\mathbb{F}G$-submodules of any module V. They are called **trivial submodules**.

Definition 3.13. *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**.

Remark 3.14. In a vector space any set of linearly independent vectors span a subspace therefore a vector space is never irreducible unless it has dimension 1. However with $\mathbb{F}G$-module a subspace need not be a submodule unless it is also invariant under the action of G. Hence it is less easy to find non-trivial submodules and it is possible that there could be none hence irreducible $\mathbb{F}G$-module.

Definition 3.15. *Let $\mathbb{F}$ and L be finite fields. L is an* **extension field** *of $\mathbb{F}$ if and only if $\mathbb{F} \subseteq L$. We denote the field extension by $L/\mathbb{F}$. An irreducible $\mathbb{F}G$-module over a field $\mathbb{F}$ is said to be* **absolutely irreducible** *if it is irreducible for any extension field $L/\mathbb{F}$.*

Definition 3.16. *Let V be an $\mathbb{F}G$-module. We say V is* **decomposable** *if it can be written as a direct sum of two $\mathbb{F}G$-submodules. i.e., there exist submodules U and W of V such that $V = U \oplus V$. If no such submodules for V exist, then V is* **indecomposable**. *If V can be written as a direct sum of irreducible submodules then it is called* **completely reducible** *or* **semisimple**.

Clearly, a completely reducible module implies a decomposable module which in turn implies an reducible one, but the converse relation is not necessarily true.

Lemma 3.17. *Let V be an $\mathbb{F}G$-module, U a submodule of V and $\langle \cdot, \cdot \rangle$ an inner product on V which is invariant under the action of G i.e., $\langle g(u), g(v) \rangle = \langle u, v \rangle$ for all $u, v \in V, g \in G$. Then $U^{\perp}$ is also an $\mathbb{F}G$-submodule of V and therefore $V = U \oplus U^{\perp}$ as $\mathbb{F}G$-modules.*

Proof: Let $u \in U, w \in U^{\perp}$ and $g \in G$. Then since U is G-invariant we have

$$\langle g(w), u \rangle = \langle g^{-1}g(w), g^{-1}(u) \rangle = \langle w, g^{-1}(u) \rangle = 0.$$

Hence $g(w) \in U^{\perp}$. ■

Definition 3.18. *Let V, W be $\mathbb{F}G$-modules. A function $\tau : V \longrightarrow W$ is said to be an $\mathbb{F}G$-homomorphism if τ is a linear transformation and for all $v \in V, g \in G, \tau(gv) = g\tau(v)$ i.e., if τ sends v to w then it sends gv to gw. Then a bijective homomorphism is called an isomorphism.*

Theorem 3.19. *Two $\mathbb{F}G$-modules are isomorphic if and only if they afford equivalent representations.*

Proof: We make use of equivalent matrix representation to prove the first part. Assume that V and W are isomorphic modules i.e., the map $\sigma : V \to W$ is an isomorphism and so they have same dimension say n. We choose bases $B_v = \{v_1, v_2, \cdots, v_n\}$ and $B_w = \{w_1, w_2, \cdots, w_n\}$ for V and W respectively. Let $\rho_v : G \longrightarrow GL(n, \mathbb{F})$ and $\rho_w : G \longrightarrow GL(n, \mathbb{F})$ be the matrix representations afforded by V and W respectively in their given bases. Since V and W are isomorphic then there exists a matrix P such that $B_v = PB_wP^{-1}$ for all $g \in G$ and since σ_v and σ_w are endomorphisms we have that $\sigma_v(g) = P\sigma_wP^{-1}$ for all $g \in G$. Hence σ_v and σ_w are equivalent matrix representations. Conversely, suppose π and π' are equivalent matrix representations of G. Then they have same degree and by definition there exists an invertible matrix P such that $\pi(g) = P\pi'P^{-1}$ $g \in G$. Let V be the $\mathbb{F}G$-module afforded by π and W that afforded by π'. Then we can choose a basis B_w of W such that P is the change of basis matrix from B_v to B_w and if so it follows that V and W are isomorphic. ■

3.2.1 Ordinary representation theory

In ordinary representation theory the study of representations takes on the form of classifying representations by describing the irreducible $\mathbb{F}G$-module of a given group G so as to gain useful information about the group. However not every finite dimensional $\mathbb{F}G$-module is completely irreducible.

Maschke's theorem gives the conditions under which an $\mathbb{F}G$-module is semisimple.

Theorem 3.20 (Maschke's theorem)**.** *Let G be a finite group and $\mathbb{F}$ a field whose characteristic is 0 or a prime p that does not divide the order of G. Then every $\mathbb{F}G$-module V is completely reducible i.e., if V is an $\mathbb{F}G$-module and U any submodule of V, then there exists a submodule W of V such that $V = U \oplus W$. In particular, the group algebra $\mathbb{F}G$ is semisimple.*

Proof: See [54] or [69, Theorem 1.9]. ■

3.2.2 Modular representation theory

Let G be a finite group and $\mathbb{F}$ a splitting field of characteristic a prime $p > 0$. The representation $\varrho : G \longrightarrow GL(V)$ over $\mathbb{F}$ is called modular if p divides the order of G and the study of such representations is called modular representation theory. Modular representation theory was developed by Brauer. The difference between ordinary and modular representation is highlighted by the following proposition.

Proposition 3.21. *Every finitely generated $\mathbb{F}G$-module over the group algebra $\mathbb{F}G$ is semisimple if and only if the characteristic of the field p does not divide the order of the group.*

Proof: See [1, Proposition 3.1]. ■

It therefore follows that if p divides $|G|$ then the $\mathbb{F}G$-module cannot be decomposed into a direct sum of irreducible submodules. In this case we generally consider the decomposition of the finitely generated module into indecomposable summands. Then an equivalent of the Maschke's theorem for the modular case which comes close to it is the Krull-Schmidt's theorem which states that any representation of G has a unique decomposition into indecomposable direct summands. This narrows the study of modular representation theory to the study of indecomposable modules.

Theorem 3.22. *(Krull-Schmidt Theorem) Every module M can be written as $M = M_1 \oplus M_2 \oplus \ldots \oplus M_n$ where the M_i are indecomposable. Furthermore, if $M = M_1 \oplus M_2 \oplus \cdots \oplus M_n$ and also $M = N_1 \oplus N_2 \oplus \ldots \oplus N_p$ where the N_i are*

also indecomposable, then $n = p$ and the M_i are isomorphic to the N_j, in some order.

Proof: See [100]. ■

Modular representations are linked to ordinary representations via some integral values. We give a brief summary of some basic facts which have been established about modular representations linking them to ordinary representations.

Definition 3.23. *Let G be a group and p any prime. An element $g \in G$ can be written as $g = st$ so that p does not divide the order of s and the order of t is a power of p. Then s is called a p-regular and t is called a p-singular element respectively.*

(a) The number of irreducible $\mathbb{F}$-representations of G is equal to the number of elements of the p-regular conjugacy classes of G.

(b) The composition factors together with their multiplicities of the $\mathbb{F}$-representation of G is uniquely determined by the Brauer characters.

Further, Brauer has shown in [12, Theorem 1] that an ordinary irreducible representation is still irreducible in the modular case. We further have that the cancelation law for modules apply in the modular case.

Theorem 3.24 (Brauer and Nesbitt)**.** *Let G be a group of order $g = p^{ag'}$, p a prime and $(g', p) = 1$. An irreducible representation Z_i of degree $z_i \equiv 0 \pmod{p^a}$ remains irreducible as a modular representation.*

Proof: See [12, Theorem 1] ■

Corollary 3.25 (Cancelation law)**.** *If M, U and V are modules, and*

$$M \oplus U = M \oplus V \text{ then } U = V.$$

Another important way of studying a module is by looking at its composition series. This proves to be quite helpful since most modules occurring naturally are not semi-simple and hence can not be written as a direct sum of irreducible modules.

Definition 3.26. *A* **composition series** *for an $\mathbb{F}G$-module V is a series of submodules of the form*

$$V = V_0 \supseteq V_1 \supseteq \ldots \supseteq V_t = 0$$

such that for each $i \geq 1$ the factor V_{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.*

The restrictions $\pi_i = \pi|_{V_{i-1}/V_i}$, $0 < i < n$ of π to the composition series of a finite dimensional $\mathbb{F}G$-representation π are called **irreducible constituents** of π and an irreducible constituent π has multiplicity j if the factor $V_r \cong V_{i-1}/V_i$ for exactly j values of i.

Not every module has a composition series for example the ring $\mathbb{Z}$ when considered as a module over itself does not have a composition series. However when one does exist, Jordan-Hölder theorem states:

Theorem 3.27 (Jordan-Hölder theorem for $\mathbb{F}G$-modules)**.** *If V is a finite dimensional $\mathbb{F}G$-module, then V possesses a composition series and the composition factors (up to order and equivalence) are independent of the choice of the composition series.*

Proof: See [3]. ■

As a consequence of the Jordan-Hölder theorem we observe that given any two composition series the composition factors M_i/M_{i+1} of one of the series is simply a permutation of the composition factors of the other. This suggests that a module can have many composition series. Again all the simple modules appear in a composition series for an $\mathbb{F}G$-module, since every simple module is a quotient of an $\mathbb{F}G$-module, hence there can only be finitely many of them.

Any proper submodule of a finitely generated module is contained in a maximal submodule (see [100]). From this it is apparent that any finitely generated module will have a composition series. The following special submodules require mentioning as we shall meet them in our computations.

Definition 3.28. *Let M be an $\mathbb{F}G$-module over a finite field $\mathbb{F}$. We call the intersection of all maximal submodules of M the* **radical** *of M and denote it* $\mathrm{rad}(M)$ *i.e.,*

$$\mathrm{rad}(M) = \bigcap \{U \leq_{\max} M | M/U \text{ is simple } \}.$$

The **socle** of M is the sum of all irreducible submodules of M and is denoted by $\mathrm{soc}(M)$. Moreover,

$$\mathrm{soc}(M) = \sum \{U \leq M | U \text{ is simple } \}.$$

A socle series is a composition series of socles.

Chapter 4

Links of codes and other combinatorial structures

In this chapter we focus on codes, designs and finite geometries. For a more detailed account and additional information the reader is advised to consult [4, 7, 24] and [89, 102].

4.1 Linear codes

A finite field of order q where q is a power of a prime, will be denoted by $\mathbb{F}_q$ and $\mathbb{F}_q^*$ will denote the non-zero elements of $\mathbb{F}_q$. Denote the vector space of n-tuples of elements of $\mathbb{F}_q$ by $V = {\mathbb{F}_q}^n$. Then the standard dot product of x and y in V is defined by $x \cdot y = xy^t$ where y^t is the transpose of y. The subspace spanned over $\mathbb{F}_q$ by the subset $\{x_1, x_2, \ldots, x_n\}$ of V will be denoted by $\langle x_1, x_2, \ldots, x_n \rangle$.

Definition 4.1. *Let F be a set of q elements. A* **q-ary code** *C is a set of finite sequences of the elements of F, called codewords (words) . If all the codewords are sequences of the same length n, then C is called a* **block code** *of length n.*

Definition 4.2. *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. The* **minimum distance** *d of C is the smallest Hamming*

distance between any two distinct words in C, that is $d = min\{d(x, y) \mid x, y \in C, x \neq y\}$.

The codes from designs that we will study are block codes. The construction of these codes over finite fields will give them additional structure. Specifically we consider codes over finite fields which are finite dimensional vector spaces.

Definition 4.3. *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 4.4. *If* C *is a linear code of length* n *over the field* $\mathbb{F}_q$ *then the* **weight** *of a word* x *in* C *is defined to be* $\mathrm{wt}(x) = d(0, x)$.

It then follows 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** $d \leq n - k + 1$ (see [4]).

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. Obviously $A_0(c) = 1$, $A_i(c) \geq 0$, and $\sum_i A_i(c) = q^k$. For linear codes (and some non-linear codes) $A_i(c)$ is independent of c and will be denoted by A_i.

Definition 4.5. *Let* C *be a linear code. Then the* **weight enumerator** *of* C *is the polynomial* $W_C(x, y) = \sum_{c \in C} x^{n - \mathrm{wt(c)}} y^{\mathrm{wt(c)}} = \sum_{i=0}^{n} A_i x^{n-i} y^i$.

Remark 4.6. The weight distribution classifies codewords according to the number of non-zero coordinates. More detailed information is supplied by the complete weight enumerator, which gives the number of codewords of each composition.

Definition 4.7. *Let C be a $[n,k]_q$ code. A* **generator matrix** *for C denoted by $\mathcal{G}$ is a $k \times n$ matrix obtained from any k linearly independent vectors of C.*

Definition 4.8. *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 $C^{\perp} = \{v \in {F_q}^n | \ (v,c) = 0 \text{ for all } c \in C\}$.*

From elementary linear algebra we have that $\dim(\mathrm{C}) + \dim(\mathrm{C}^{\perp}) = \mathrm{n}$, since $C^{\perp}$ is simply the null space of a generator matrix for C. Taking $\mathcal{G}$ 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 satisfies $\mathcal{G}H^T = 0$, that is $c \in C$ if and only if $cH^T = 0 \in {\mathbb{F}_q}^{n-k}$. For any vector y in ${\mathbb{F}_q}^n$ the vector yH^T is called the **syndrome** of y , denoted $\mathrm{Syn}(y)$. If x and y are in ${\mathbb{F}_q}^n$, then $\mathrm{Syn}(x) = \mathrm{Syn}(y)$ if and only if x and y are in the same coset of C. We will see in Section 4.6 that syndromes can be used to decode a received message more efficiently.

Definition 4.9. *Any generator matrix H for $C^{\perp}$ is called a* **parity-check** *or* **check** *matrix for C. If $\mathcal{G}$ 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 $\mathcal{G}$.*

The first k coordinates are called the **information symbols** and the last $n-k$ coordinates are the **check symbols**.

We can use the generator matrix for a linear code to encode a message. Suppose that we have a set of data consisting of q^k messages that are to be transmitted. We encode the message using a code C with a generator matrix $\mathcal{G}$. To do this we identify the data with the vectors in ${\mathbb{F}_q}^k$. Then for $u \in {\mathbb{F}_q}^k$, we encode u by forming the vector $u\mathcal{G}$. If $u = (u_1, u_2, \ldots, u_k)$ and $\mathcal{G}$ has rows $R_1, R_2, \ldots, R_k$, where each R_i is in ${F_q}^n$, then u is encoded as:

$$u\mathcal{G} = \sum_i u_i R_i = (u_1, u_2, \ldots, u_k, x_{k+1}, \ldots, x_n).$$

But when $\mathcal{G}$ is in standard form, the encoding takes the simpler form $u \mapsto (u_1, u_2, \ldots, u_k, x_{k+1}, \ldots, x_n)$, and here the $u_1, u_2, \ldots, u_k$ are the message or

information symbols, and the last $n-k$ entries are the check symbols, and represent the redundancy .

In general it is not easy to say anything about the minimum weight of $C^{\perp}$ knowing only the minimum weight of C but, of course either a generator matrix or a check matrix gives a complete information about both C and $C^{\perp}$. In particular, a check matrix for C can be used to determine the minimum weight of C as is shown in theorem4.10:

Theorem 4.10. *Let H be a check matrix for a $[n, k, d]$ 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 [4, Theorem 2.3.1]. ■

A **constant vector** is one for which all the coordinate entries are either 0 or 1. If $C^{\perp}$ contains the **all-one** vector $\mathbf{1} \in {\mathbb{F}_q}^n$, whose entries are all $1 \in \mathbb{F}_q$, then every vector in the q-ary code C of weight congruent to 0 modulo q is also in $C^{\perp}$. A code C is **self-complementary** if it contains the all-ones vector, **self-orthogonal** if $C \subseteq C^{\perp}$ and **self-dual** if $C = C^{\perp}$. The **hull** of a design's code over some field is the intersection $C \cap C^{\perp}$. A binary code is **doubly-even** if all its codewords have weight divisible by 4.

4.1.1 Automorphism group of a code

Two linear codes of length n over the field $\mathbb{F}_q$ are **equivalent** if each can be obtained from the other by permuting the coordinate positions of ${\mathbb{F}_q}^n$ and multiplying each coordinate by a non-zero element of the field. They are **isomorphic** if each can be obtained from the other by a permutation of the coordinate positions in which case we say there is an isomorphism between the two codes. In the case of linear binary codes, the notions of equivalence and isomorphism coincide. Any code is isomorphic to a code with generator matrix in standard form.

Definition 4.11. *If C is a linear code of length n over $\mathbb{F}_q$, then any isomorphism of C onto itself is called an* **automorphism** *of C. The set of all automorphisms of C is called* **automorphism group** *of C, denoted by* $\mathrm{Aut}(C)$.

From the definition we can immediately deduce that any automorphism of the code preserves each weight class of C.

The automorphism group of C is thus a subgroup of S_n, or of S_Ω if $C \subseteq {\mathbb{F}_q}^\Omega$. The existence of automorphism for C can provide a richer structure for the code and allow the use of deeper results from group theory.

4.2 Designs

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. We assume that $\mathcal{P} \cap \mathcal{B} = \varnothing$. The points will be written in lower Roman letters and the blocks by capital Roman letters. In the case where the blocks are subsets of the points and the relationship is set containment, the incidence structure is denoted by $(\mathcal{P}, \mathcal{B})$. If (p, B) is in $\mathcal{I}$ for p in $\mathcal{P}$ and $B \in \mathcal{B}$, then we say p is on B or p is incident with B.

Let $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ and $\mathcal{T} = (\mathcal{Q}, \mathcal{C}, \mathcal{J})$ be incidence structures, and let φ be a bijection from $\mathcal{P} \cup \mathcal{B}$ to $\mathcal{Q} \cup \mathcal{C}$. Suppose $\varphi(\mathcal{P}) = \mathcal{Q}$ with $p \in \mathcal{P}$ incident with $B \in \mathcal{B}$ if and only if $\varphi(p) \in \mathcal{Q}$ is incident with $\varphi(B) \in \mathcal{C}$, then φ is an **isomorphism** from $\mathcal{S}$ to $\mathcal{T}$. If $\mathcal{S} = \mathcal{T}$, then φ is an automorphism.

Definition 4.12. *An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is a t-(v, k, λ)* **design** *if*

(1) $|\mathcal{P}| = v$;

(2) every block $B \in \mathcal{B}$ is incident with precisely k points;

(3) and every t distinct points are together incident with precisely λ blocks.

Remark 4.13. A t-(v, k, λ) design is also referred to as a t-design. We shall assume that all the parameters are positive integers, and that $v > k \geq t$ (to avoid trivial cases). Also the members of $\mathcal{B}$ must be distinct, thus repeated blocks are not allowed.

Theorem 4.14. *A t-design $\mathcal{D}$ is also an s-design, for $1 \leq s \leq t$. If the given design has parameters t-(v, k, λ) then its parameters as an s-design are s-(v, k, λ_s) where*

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

Proof: See [8, Theorem 3.2.2]. ■

Definition 4.15. *Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with $|\mathcal{P}| = v$ and $|\mathcal{B}| = b$. Let the points be labelled $\{p_1, p_2, \dots, p_v\}$ and the blocks be labelled $\{B_1, B_2, \dots, B_b\}$. An* **incidence matrix** *for $\mathcal{D}$ is a $b \times v$ matrix $A = (a_{ij})$ of 0's and 1's such that*

$$a_{ij} = \begin{cases} 1 & \text{if } (p_j, B_i) \in \mathcal{I} \\ 0 & \text{if } (p_j, B_i) \notin \mathcal{I} \ . \end{cases}$$

The incidence matrix depends on the ordering of points and blocks. If we impose the labelling on the points of a design $\mathcal{D}$, $\{p_1, p_2, \cdots, p_v\}$, a block B of the design can be represented as an **incidence vector** v^B of length v where the i^{th} entry of v^B is 1 if p_i is incident with B and 0 otherwise. If an ordering is also imposed on the blocks, an incidence matrix A may be defined for $\mathcal{D}$ where the i^{th} row of A is the incidence vector of the i^{th} block.

A design is **trivial** if every k-set of points is incident with a block of the design. A design is called **simple** if distinct blocks are not incident with the same set of k points. In this thesis all designs will be simple and non-trivial. We define λ_i to be the number of blocks incident with i points, $0 \leq i \leq t$. It follows that $\lambda_t = \lambda, \lambda_0 = b$ and λ_1 is the number of blocks through any point in the design, referred to as the **replication number** for the design, and denoted by r. A counting argument proves the well known relationship between the parameters

$$\lambda_i = \lambda_{i+1} \frac{(v-i)}{(k-i)}.$$

In particular,

$$vr = bk.$$

Definition 4.16. *The* **dual** *structure of* $\mathcal{D}$ *is* $\mathcal{D}^t = (\mathcal{B}^t, \mathcal{P}^t, \mathcal{I}^t)$*, where* $\mathcal{P}^t = \mathcal{B}, \mathcal{B}^t = \mathcal{P}$ *and* $\mathcal{I}^t = \{(B, p) \mid (p, B) \in \mathcal{I}\}$.

Given a labelling on the point and block sets of $\mathcal{D}$ the transpose of an incidence matrix for $\mathcal{D}$ is an incidence matrix for $\mathcal{D}^t$. 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.

Definition 4.17. *Let* $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ *be a design. Then the* **complement** *of* $\mathcal{D}$ *is the structure* $\overline{\mathcal{D}} = (\overline{\mathcal{P}}, \overline{\mathcal{B}}, \overline{\mathcal{I}})$*, where* $\overline{\mathcal{P}} = \mathcal{P}$*,* $\overline{\mathcal{B}} = \mathcal{B}$ *and* $\overline{\mathcal{I}} = \mathcal{P} \times \mathcal{B} - \mathcal{I}$.

Theorem 4.18. *If* $\mathcal{D}$ *is a* $t-(v, k, \lambda)$ *design with* $v-k \geq t$*, then* $\overline{\mathcal{D}}$ *is a* $t-(v, v-k, \overline{\lambda})$ *design, where*

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

Proof: See [4, Theorem 1.3.1]. ■

Definition 4.19. *An* **automorphism** *of a design* $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ *is a permutation* π *of* $\mathcal{P}$ *such that* $B \in \mathcal{B}$ *implies* $\pi(B) \in \mathcal{B}$.

Clearly, the automorphisms of $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ form a group under composition which acts on $\mathcal{P}$. Since an automorphism takes blocks to blocks, the group also has a permutation representation on the set $\mathcal{B}$.

Lemma 4.20. *[8] Let* $\mathcal{D}$ *be a* t*-design with* $t \geq 2$*. Then the group of automorphisms of the design acts faithfully on* $\mathcal{B}$.

The existence of multiply transitive groups may be used in order to construct designs, as in the following theorem.

Theorem 4.21. *Let* G *be a* t*-transitive permutation group on a finite set* Ω*, with* $t \geq 2$*, and suppose that* Δ *is a subset of* Ω*, with* $|\Delta| = k$*,* $|\Omega| = v$*, and* $1 < k < v-1$*. Then the set* $\mathcal{B} = \{\Delta^g \mid g \in G\}$ *is the set of blocks of a* t*-design* $\mathcal{D}$*, and* G *is a group of automorphisms acting transitively on* $\mathcal{B}$.

Proof: See [8, Theorem 3.4.3]. ■

Only a few symmetric designs are known to enjoy the property that a primitive nonsolvable group of automorphisms acts on points and blocks. In [74], Kantor classified all designs with 2-transitive group of automorphisms. In [50, Section 1], Dempwolff determined the symmetric designs $\mathcal{D}$ which admit $G \leq \mathrm{Aut}(\mathcal{D})$ such that G has a non-abelian socle and is a primitive rank-3 group on points and on blocks.

In this thesis we shall be concerned mostly with self-dual symmetric 1-(v, k, k) designs. In Theorem 6.1 we give a method to construct such designs. These designs will result from the primitive permutation representations of groups. In particular we are concerned with the primitive permutation representations of finite simple groups.

4.3 Graphs

In this section we shall be concerned with the relationship between permutation groups, graphs and designs. The theory of designs concerns itself with questions about subsets of a set (or relations between two sets) possessing a high degree of regularity. By contrast graph theory is mainly concerned with questions about general relations on a set. The generality usually means that either the questions asked are too particular, or the results obtained are not powerful enough, to have useful consequences for design theory. There are instances where the two theories have interacted fruitfully. The unifying theme is provided by a class of graphs called strongly regular graphs, whose definition reflects the symmetry inherent in t-designs.

Definition 4.22. *A* **graph** $\Gamma = (V, E)$*, consists of a finite set of vertices* V *together with a set of edges* E*, where an edge is a subset of the vertex set of cardinality 2.*

Our graphs are undirected (edges are not allowed to be ordered pairs), and without loops (two vertices comprising an edge are not equal) or multiple edges (a given pair of vertices can comprise at most one edge).

The **complement** of a graph Γ is the graph $\bar{\Gamma}$ whose edge set is the complement of the edge set of Γ (relative to the set of all 2-element subsets of the vertex set).

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

Definition 4.23. *A* **strongly regular graph** *with parameters* (n, k, λ, μ) *is a graph* Γ *with* n *vertices, not complete or null, in which the number of common neighbours of* x *and* y *is* k, λ *or* μ *according as* x *and* y *are equal, adjacent or non-adjacent respectively.*

Remark 4.24. *Notice that the complement of a strongly regular graph with parameters* (v, k, λ, μ) *is again strongly regular, with parameters* $(v, v-k-1, v-2k+\mu-2, v-2k+\lambda)$.

Definition 4.25. *Let* Γ *be a graph with vertex set* $\{x_1, x_2, \cdots, x_n\}$. *The* **adjacency matrix** $A(\Gamma) = (a_{ij})$ *of* Γ *is the* $n \times n$ *matrix given by*

$$(a_{ij}) = \begin{cases} 1 & \text{if } x_i \text{ and } x_j \text{ are adjacent,} \\ 0 & \text{otherwise .} \end{cases}$$

Let $\Gamma = (V, E)$ be a graph, and G be a permutation group on V. We say that G acts on Γ if, for all $(\alpha, \beta) \in E$ and $g \in G$, we have $(\alpha^g, \beta^g) \in E$; that is, G is a group of **automorphisms** of Γ. The automorphism group $\mathrm{Aut}(\Gamma)$ of the graph Γ is the subgroup of S_V consisting of all automorphisms of Γ. We say that Γ is **vertex-transitive** if $\mathrm{Aut}(\Gamma)$ is transitive on the vertex-set V, and we say that Γ is a **rank-r graph** if $\mathrm{Aut}(\Gamma)$ is a transitive group of rank r on V.

The **line graph** of a graph $\Gamma = (V, E)$ is the graph $L(\Gamma) = (E, V)$ where e and f are adjacent in $L(\Gamma)$ if e and f share a vertex in Γ. The **complete graph** K_n on n vertices has for E the set of all 2-subsets of V and the **null** graph is a graph that has no edges at all. The automorphism group of the complete graph K_n is the symmetric group S_n, since in this case any permutation of the vertices preserves adjacency.

The line graph of K_n is the **triangular graph** $T(n)$, and it is strongly regular with parameters $(\frac{n(n-1)}{2}, 2(n-2), n-2, 4)$. The automorphism group of the triangular

graph $T(n)$ for $n > 4$ is the symmetric group S_n. This follows a theorem of Whitney [117], which states that if Γ is a connected graph with more than 4 vertices, then $\mathrm{Aut}(L(\Gamma)) = \mathrm{Aut}(\Gamma)$. Now $T(n) = L(K_n)$ implies $\mathrm{Aut}(T(n)) = S_n$ for all $n > 4$.

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

Thus a relation is established between groups, designs, modules and codes. The interplay between these structures will become evident in Chapter 6, where these relations undergo a considerable development and are explicitly defined. In Chapters 7, 8 and 10 we construct codes from the 2-modular representations of some simple groups defined therein and an interplay between codes and groups is established.

4.4 Finite geometries

We give a brief introduction to projective and affine geometries. The reader should consult any standard text in this area for a more complete discussion, see, for example [4] or [7].

4.4.1 Projective geometries

Let V be a vector space over the field $\mathbb{F}$. The **projective geometry** (space) defined by V is denoted by $PG(V)$. If the vector space V has dimension m over $\mathbb{F}$, then the projective geometry $PG(V)$ has **projective dimension** $m - 1$; $PG(V)$ is also denoted by $\mathcal{P}(V) = PG_{m-1}(\mathbb{F})$. The elements of $PG_{m-1}(\mathbb{F})$ are non-trivial subspaces of V, and the structure of the set is given by set-theoretical containment. The

projective dimension of an element U in $PG_{m-1}(\mathbb{F})$ is denoted by $\text{pdim}(U)$ and is defined to be one less than the dimension of U as a vector space over $\mathbb{F}$. Thus the **points** of $PG(V)$ are the 1-dimensional subspaces of V, the **lines** are the 2-dimensional subspaces of V, and the **hyperplanes** are the $(m-1)$-dimensional subspaces of V.

If $\mathbb{F} = \mathbb{F}_q$, a point of the projective geometry $PG_{m-1}(\mathbb{F}_q)$ is given in homogeneous coordinates by the non-zero vector $(x_1, \ldots, x_m) \in {\mathbb{F}_q}^m$. Each point then has $q-1$ such coordinates representatives since $(x_1, \ldots, x_m)$ and $\lambda(x_1, \ldots, x_m)$ yield the same 1-dimensional subspace of ${\mathbb{F}_q}^m$ for any non-zero vector $\lambda \in \mathbb{F}_q$.

A hyperplane H of the projective geometry $PG_{m-1}(\mathbb{F}_q)$, in homogeneous coordinates is determined by by the non-zero vector $(y_1, \ldots, y_m)^t$ which spans $H^\perp$. A point $\langle(x_1, \ldots, x_m)\rangle$ is on the hyperplane H if and only if $(x_1, \ldots, x_m)\cdot(y_1, \ldots, y_m)^T = 0$.

Grassman's identity for subspaces of V holds for subspaces of a projective space $PG(V)$. Thus if U and W are arbitrary elements of $PG(V)$, then

$$\text{pdim(U)} + \text{pdim(W)} - \text{pdim(U} \cap \text{W)} = \text{pdim(U} + \text{W)}. \tag{4.1}$$

If H is a hyperplane of $PG(V)$ and U is an element of $PG(V)$ with $\text{pdim}(U) = t$, then from the identity (4.1) we get thatpdim$(H \cap U) = t$ or $t-1$, and the former occurs if and only if $U \subseteq H$.

The number of subspaces of V of dimension k, where $0 < k \leq m$, is given by

$$N_{m,k}(q) = \frac{(q^m-1)(q^m-q)\ldots(q^m-q^{k-1})}{(q^k-1)(q^k-q)\ldots(q^k-q^{k-1})}. \tag{4.2}$$

In particular the number of points and the number of hyperplanes of $PG_{m-1}(\mathbb{F}_q)$ is $\frac{q^m-1}{q-1}$.

Similarly, if U is an r-dimensional subspace of an m-dimensional vector space V and k is an integer with $0 \leq r < k \leq m$, then the number of subspaces of V of dimension k that contain U is given by

$$\frac{(q^m-q^r)(q^m-q^{r+1})\ldots(q^m-q^{k-1})}{(q^k-q^r)(q^k-q^{r+1})\ldots(q^k-q^{k-1})}. \tag{4.3}$$

In particular, if $k = m - 1$, this gives the number of hyperplanes that contain U as $\sum_{i=0}^{m-r-1} q^i$.

Given two projective spaces, an **isomorphism** is a bijective map that preserves incidence structure. An isomorphism between two projective spaces is called **collineation**, and an isomorphism from a projective space to itself is called an **automorphism** or collineation. The full automorphism group of $PG(V)$ is given by the well-known fundamental theorem of projective geometry which follows:

Theorem 4.26 (Fundamental theorem of projective geometry)**.** *The full automorphism group of $PG_{m-1}(\mathbb{F}_q)$ is $P\Gamma L_m(q)$ for any $q \geq 2$ and $m \geq 3$.*

Proof: See [6]. ■

The elements of $P\Gamma L_m(q)$ preserve the subspaces of $V = {\mathbb{F}_q}^m$, and thus they form a permutation group on the points of $PG_{m-1}(V)$. We may construct within this group an automorphism α of order $\frac{q^m-1}{q-1}$ that permutes the points of the geometry in a single cycle of this length, called a **Singer cycle**, see [7, Theorem 6.2]. The group generated by a Singer cycle is called a **Singer group.**

4.5 Orbit matrices

Let A be the incidence matrix of a design $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$. A decomposition of A is any partition $B_1, \ldots, B_s$ of the rows of A (blocks of $\mathcal{D}$) and a partition $P_1, \ldots, P_n$ of the columns of A (points of $\mathcal{D}$). We say that a **decomposition is row-tactical** (block-tactical) if the sum of entries of each row in $B_1, \cdots, B_m$ is constant, column-tactical (point-tactical) if the sum of entries of each column in $P_1, \ldots, P_n$ is constant and tactical if it is both row-tactical and column-tactical.

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a symmetric (v, k, λ) design and $G \leq \mathrm{Aut}(\mathcal{D})$ be a subgroup of the automorphism group of the design. The group action of G induces a tactical decomposition of $\mathcal{D}$ and produces same number of orbits on the points as well as on the blocks. Let us denote this number by t, and let the G-orbits on the points be denoted by $\mathcal{P}_1, \ldots, \mathcal{P}_t$ and the G-orbits on the blocks by $\mathcal{B}_1, \ldots, \mathcal{B}_t$. Let $\omega_1, \cdots, \omega_t$

and $\Omega_1, \ldots, \Omega_t$ be the respective orbit lengths i.e., $|\mathcal{P}_r| = \omega_r$ and $|\mathcal{B}_i| = \Omega_i$. We call $\mathcal{P}_1, \ldots, \mathcal{P}_t$ and $\mathcal{B}_1, \ldots, \mathcal{B}_t$ the **orbit distributions**, and $\omega_1, \ldots, \omega_t$ and $\Omega_1, \ldots, \Omega_t$ the orbit size distributions for the design and the group G. The G-orbits on the points and blocks form a **tactical decomposition** of $\mathcal{D}$.

Further denote by γ_{ir} the number of points of $\mathcal{P}_r$ that are incident with a representative of the block orbit $\mathcal{B}_i$ and Γ_{js} the number of blocks of $\mathcal{B}_j$ that are incident with the point $\mathcal{P}_s$. These numbers satisfy the following equalities:

$$\sum_{r=1}^{t} \gamma_{ir} = k, \text{and} \sum_{j=1}^{t} \Gamma_{js} = k, \tag{4.4}$$

$$\sum_{r=1}^{t} \frac{\Omega_j}{\omega_r} \gamma_{ir}\gamma_{jr} = \lambda\Omega_j + \delta_{ij}(k - \lambda) \tag{4.5}$$

Definition 4.27. *A $(t \times t)$ matrix (γ_{ir}) with entries satisfying conditions (4.4) and (4.5) is called an* **orbit matrix** *or* **orbit structure** *for the parameters (v, k, λ) and orbit lengths distributions $(\omega_1, \ldots, \omega_t), (\Omega_1 \ldots, \Omega_t)$.*

Orbit matrices are used to construct designs with a presumed automorphism group. We shall see in Section 5.5 and Chapter 9 how some classes of linear codes can be constructed from orbit matrices.

4.6 Decoding schemes

Codes have been used with great efficiency in some important applications. Perhaps the most immediate application of codes is that which relates them with the encoding and decoding of "messages", and this will be the subject of the this section.

Of primary interest is the capability of a code that is constructed from a design. We will assume that a **symmetric q-ary channel** is used, where each symbol in the alphabet of the code has the same probability of being transmitted erroneously and has the same probability to occur when an error has been made. We will describe the techniques of **syndrome decoding** and **majority logic decoding**. These methods are often used in decoding projective geometry codes.

The following result establishes the exact measurement of the error-detection and error-correction capability of a code assuming the use of a symmetric channel. The proof can be found in any standard text in coding theory: see for example [4, Chapter 2].

Theorem 4.28. *Let C be a code with minimum distance d. Then C can detect $d-1$ errors and correct $\lfloor \frac{d-1}{2} \rfloor$ errors.*

Proof: See [4].■

4.6.1 Nearest neighbour decoding

The decoding scheme in which a received word y is decoded as the closest word in the q-ary code to y, should such a word be uniquely determined, is called **nearest neighbour decoding**. Here "close" is measured in terms of the Hamming distance between two codewords. Thus, the greater the minimum distance of a code, the larger the number of errors can be corrected. Assuming the use of the symmetric q-ary channel, this decoding algorithm maximizes the probability that, after decoding, the correct word is finally received. Note that for large codes this algorithm is costly as it requires a comparison between the received vector y and every codeword in the code. For a linear code, the syndrome of the received vector y, denoted $\mathrm{Syn}(y)$, can be used to reduce the number of comparisons that are needed and to reduce the amount of memory needed to implement nearest neighbour decoding. This method is referred to as **syndrome decoding**.

4.6.2 Majority logic decoding

The majority decoding schemes are useful in decoding several families of codes: see ([107, 47, 45]). We describe the one-step majority logic decoding algorithm. In [33, Section 3.3], Clark shows that this algorithm is an effective decoding scheme for binary codes of the projective planes. Multi-step majority decoding can be implemented with codes of designs from geometries: see [107].

Definition 4.29. *A set of* $1 \times n$ *vectors* $\{v_1, v_2, \ldots, v_r\}$ *is said to be* **orthogonal at position** i *if the vectors form an* $r \times n$ *matrix with all entries in the* i^{th} *column equal to 1, and every column has either all zeros or exactly one 1 and* $r-1$ *zeros.*

Let x be the sent codeword of length n, y the received vector, and suppose that there are at most t errors. Then $x + e = y$ where e has non-zero entries at the coordinate positions where the errors have occurred. Also, $y \cdot v = (x + e) \cdot v = x \cdot v + e \cdot v = e \cdot v$ for every vector $v \in C^{\perp}$. Suppose there are r_i vectors $\{v_1, v_2, \ldots, v_{r_i}\}$ in the dual code $C^{\perp}$ of C that are orthogonal at position i, where $1 \leq i \leq n$.

If an error occurred at the i^{th} position, then there are at least $r_i - (t-1)$ equations (check equations) of the systems $S_i = \{y \cdot v_j \,|\, j \in \{1, 2, \ldots, r_i\}\}$ whose value is e_i. In order to correct the errors that have occurred, we must have a clear majority of the check equations in S_i that equal e_i. Thus we require, $t - 1 < r_i - (t-1)$ so that $r_i > 2(t-1)$.

If no error occurred at the i^{th} position, then there are at most t check equations in S_i that will be non-zero for $1 \leq i \leq n$. This means that at least $r_i - t$ check equations will be 0 for each i. For a clear majority of the checks to be 0 we need $t \leq r_i - t$. Hence $r_i \geq 2t$.

It follows that if there are at most $t \leq \frac{r_i}{2}$ errors introduced and there are r_i vectors in the dual code $C^{\perp}$ of C that are orthogonal at position i, then the majority logic decoding algorithm can detect and correct an error made in the i^{th} position. If such a set of checks exist for every position $i \in \{1, 2, \cdots, n\}$, then we can correct up to t errors, where $2t \leq r$ and $r = \mathrm{Min_i}\{\mathrm{r_i}\}$. If the minimum weight of C is d, then C can correct at most $\lfloor \frac{d-1}{2} \rfloor$ errors. So majority logic will use this capability as long as $r \geq \lfloor \frac{d-1}{2} \rfloor$, that is, $r \geq \frac{d-1}{2}$ if d is odd and $r \geq \frac{d-2}{2}$ if d is even.

Chapter 5

Codes related to combinatorial structures

As a mathematical theory, coding theory is relatively young, with its roots in Shannon's [109] seminal paper in 1948. The practical gains, due to coding, demonstrated there, and elsewhere since, have provided motivation for much of coding theory. It is fascinating how a large mathematical theory was and is continuing to be developed. The mathematical areas needed in classical coding have been mainly algebraic. However through time, subsequent developments have expanded this mathematical theory considerably. A frequent question in coding theory is "how one constructs a code, or structure related to a code, that is optimal in some mathematical or applied sense." In this chapter we consider some ways in which codes have been constructed.

5.1 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. Coding theory has also been

used to extend designs. In [76] Kennedy and Pless extended designs "held" by vectors of a code. The connection between designs and codes leads to the construction of new designs. 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. 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 λ so 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 crucial in determining whether or not the supports of these vectors could form a design. For $q = 2$ the supports are in a one-to-one correspondence with the codewords. The celebrated Assmus-Mattson Theorem ([4, Theorem 2.11.2]) establishes the connection between designs and codes, in that vectors of certain weight in a q-ary code hold a design, and we can determine the number of vectors of such weight. Notice that 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; in fact, precisely $q-1$ vectors if the minimum weight of the code is $|S|$. For $q = 2$ the supports are in a one-to-one correspondence with the codewords. Once again 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 vectors (and other weights also) yield a t-design where t is a positive integer less than the minimum weight.

For a general incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ and any field $\mathbb{F}$, we denote the vector space of functions from $\mathcal{P}$ to $\mathbb{F}$ by $\mathbb{F}^{\mathcal{P}}$. For $w \in \mathbb{F}^{\mathcal{P}}$, the value of w at the point p is $w(p)$ in $\mathbb{F}$.

Definition 5.1. *The* **support set** *of a function w in $\mathbb{F}^{\mathcal{P}}$ is defined to be the subset of points in $\mathcal{P}$ whose images under w are non-zero, that is, Supp(w)=$\{p \in \mathcal{P} \mid w(p) \neq 0\}$. The* **characteristic function** *for a block B is denoted by v^B and defined to be*

$$v^B(p) = \begin{cases} 1, & \text{if } p \in B \\ 0, & \text{if } p \notin B. \end{cases}$$

The standard basis for this vector space is $\{v^{\{p\}} \mid p \in \mathcal{P}\}$.

Definition 5.2. *A q-ary* **code of a design** $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ *is the subspace of the function space* ${\mathbb{F}_q}^{\mathcal{P}}$ *generated by the characteristic functions of the blocks of* $\mathcal{D}$ *and is denoted by* $C_q(\mathcal{D})$.

If the point set of $\mathcal{D}$ is denoted by $\mathcal{P}$ and the block set by $\mathcal{B}$, and if $\mathcal{Q}$ is any subset of $\mathcal{P}$, then we will denote the incidence vector of $\mathcal{Q}$ by $v^{\mathcal{Q}}$. Thus $C_{\mathbb{F}}(\mathcal{D}) = \langle v^B \mid B \in \mathcal{B} \rangle$, and is a subspace of $\mathbb{F}^{\mathcal{P}}$. The dimension of the code $C_p(\mathcal{D})$ of the design $\mathcal{D}$ 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 $\mathcal{D}$.

In general the minimum weight is less than the block size of $\mathcal{D}$, 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 all: see [48] and [33, Section 6.1].

The following Lemma be found in [78], is an important result on the automorphism group of codes obtained from incidence structures.

Lemma 5.3. *[78] Let* C *be the linear code of length* n *of an incidence structure* $\mathcal{I}$ *over a field* $\mathbb{F}$. *Then the automorphism group of* C *is the full symmetric group if and only if* $C = \mathbb{F}^n$ *or* $C = \langle \mathbf{1} \rangle^{\perp}$.

Proof: See [78]. ■

5.2 Codes from strongly regular graphs

Strongly regular graphs were defined in Section 4.3. In general, codes from graphs have not received as much attention as the codes from combinatorial designs. Nevertheless, codes from strongly regular graphs have been extensively studied and some significant results on the $p-$rank of some of the graphs established: (See for example [5, 99]). The code C_A of a graph Γ is the code of its adjacency matrix A. For a general integral $n \times v$ matrix A, it is known (see for example [62], Lemma

2.1) that if A is a symmetric integral matrix with zero diagonal, then 2−rank(A) (i.e., the dimension of C_A) is even and also for a symmetric binary matrix A, the diag$(A) \in C_A$. Following these two results, the following relation between the codes C_A and C_{A+J} is established.

Proposition 5.4 ([62], Proposition 2.3)**.** *Suppose A is the adjacency matrix of a graph then $C_A \leq C_{A+J}$ and the following are equivalent:*

(i) $C_A = C_{A+J}$, (ii) $\mathbf{1} \in C_A$ (iii) dim(C_{A+J}) is even.

Haemers et al in [62] have considered the codes C_A and C_{A+I} of the adjacency matrices of strongly regular graphs over the binary field. Using only the parameters (eigenvalues) of a strongly regular graph Γ, they presented the properties of the binary codes of Γ. They have further determined the binary codes of some known families of strongly regular graphs giving the weight distribution for some of them. See [62] for collected results.

An $[n, k, d]_q$ linear 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 (two weight code) and any two of its coordinates are linearly independent or equivalently minimum distance of the dual code $d \geq 3$ (projective). Projective two weight codes have been widely studied (see for example [4, 23, 20, 60, 62, 46]). Strong connections exist between projective two weight codes and strongly regular graphs which we shall briefly discuss. Every projective two-weight code over a finite field has a strongly regular graph. This was first established by Delsarte ([46], Theorem 2) who then gave the connection between them as in the following theorem.

Theorem 5.1. *([46], Theorem 2). Let w_1 and w_2 (where $w_1 < w_2$) 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 the $v = q^k$ codewords and two vertices corresponding to x and y are adjacent iff $d(x, y) = w_1$. Then $\Gamma(C)$ is a strongly regular.*

A further survey by Calderbank and Kantor in [23] proved the equivalence of the following three concepts: (i) two-weight projective code, (ii) strongly regular graph

defined by a difference set in a vector space, and (iii) subset X of a projective space such that $|X \cap H|$ takes only two values when H runs over all hyperplanes. They gave another construction of the strongly regular graph from projective two weight code and further determined the graph's parameters from the parameters of the code. In this construction, the points of the $k-$dimensional vector space $\mathbb{F}_q^k$ is taken as the vertices. Each such vector defines a linear combination of the ($n-$dimensional) row vectors of a generator matrix G of a projective two-weight code C corresponding to a codeword. Two different points x and y are joined by an edge if and only if $x - y$ is a multiple of a column in G. The graph $\Gamma'(C)$ so obtained is strongly regular ([23], Theorems 3.1 and 3.2) with parameters (N, K, λ, μ) where;

$$
\begin{aligned}
N &= q^k \\
K &= n(q-1) \\
\lambda &= K^2 + 3K - q(w_1 + w_2) - Kq(w_1 + w_2) + q^2 w_1 w_2 \\
\mu &= \frac{q^2 w_1 w_2}{q^k} = K^2 + K - Kq(w_1 + w_2) + q^2 w_1 w_2
\end{aligned}
$$

Proof: See [20] Theorem 5.5 or [23] Corollary 3.7. ■

The two graphs $\Gamma(C)$ and $\Gamma'(C)$ are related such that for a given code C and its projective dual C^*, the graph $\Gamma(C)$ is isomorphic to $\Gamma'(C^*)$ (See [23], Theorem 5.7 and the definition of the projective dual in Section 4). Hence, for projective self-dual codes, the two constructions lead to isomorphic graphs.

5.3 Quasi-symmetric designs and strongly regular graphs

A 2-design is called **quasi-symmetric** if the cardinality of the intersection of any two blocks takes only two distinct values. Every quasi-symmetric design gives rise to a strongly regular graph as follows. Suppose the blocks of a quasi-symmetric design intersect in two values, say x and y. We define a graph Γ on the set of blocks and define any two blocks to be adjacent if the blocks intersect in x points. The resulting

graph is strongly regular. Connections between quasi-symmetric designs and strongly regular graphs have been studied in detail (see for example, [61], [23],[25] for some collected results). A large family of strongly regular graphs is provided by the 2-$(v, k, 1)$ designs. Since any two blocks can intersect in no more than 1 point these designs are quasi symmetric. For example a Steiner triple system 2-$(v, 3, 1)$ denoted $STS(v)$ is a quasi symmetric design with block intersection numbers 0 and 1. The block graph of an $STS(v)$ is strongly regular with parameters; $(\frac{v(v-1)}{6}, \frac{3v-9}{2}, \frac{v+3}{2}, 9)$ [25, Theorem 37.7].

Remark: We can also generate designs from strongly regular graphs as follows. Let $\Gamma = (v, k, \lambda, \mu)$ be a graph. Then

(i) If $\lambda = \mu$ then any two distinct vertices have λ neighbors in common and the design of the graph corresponds to a symmetric 2-(v, k, λ) design. Such graph is called a (v, k, λ) design.

(ii) If $\lambda = \mu - 2$ and A the incidence matrix of this graph. Then $A+I$ is the incidence matrix of a symmetric 2-(v, k, λ) design.

5.4 Codes from geometries

To generate a design from $PG_m(\mathbb{F}_q)$ where $m \geq 2$, we take as the point set of the design the set of points of the geometry. The blocks of the design are all subspaces (or flats) of the same fixed dimension, and the incidence relation is containment. If we take the blocks set to be the set of all r-dimensional subspaces of $PG_m(\mathbb{F}_q)$, then the design is denoted $PG_{m,r}(\mathbb{F}_q)$. The doubly transitivity of the projective groups on points will assure that we are dealing with 2-designs. Thus for example we can consider the designs of points and lines, the design of points and planes, or the design of points and hyperplanes of a geometry and be assured of a 2-design. The parameters will depend on both the dimension of the geometry and the cardinality of the finite field. By fixing one of these and letting the other vary we obtain numerous

infinite families of designs. Each of these designs will have an automorphism group containing $P\Gamma L(V)$ in the projective case.

Proposition 5.5. *[77] $PG_{m,r}(\mathbb{F}_q)$ is a 2-(v, k, λ) design with*

$$v = \frac{q^{m+1}-1}{q-1},\ k = \frac{q^{r+1}-1}{q-1},\ \lambda = \frac{(q^{m-1}-1)\dots(q^{m+1-r}-1)}{(q^{r-1}-1)\dots(q-1)}.$$

The codes over $\mathbb{F}_p$ of any of the designs defined by a projective geometry over a filed of characteristic p are some form of generalized Reed-Muller code, that is possibly a so-called subfield code or a non-primitive sub-field code. This fact follows from the work of Delsarte [44] and Delsarte and MacWilliams [48]. The full results are described in [4, Chapter 5] and [5, Chapter 5]. If x is any number and $x = \sum_i x_i q^i$ where $0 \leq x_i \leq q-1$, then the q-weight of x is defined to be $\mathrm{wt}(q) = \sum_i x_i$. In the following theorems found in [77], these codes are described:

Theorem 5.6. *[77] The code over $\mathbb{F}_p$ of the projective geometry design $PG_{m,r}(\mathbb{F}_q)$, where $q = p^t$ and p is a prime, and $0 < r < m$, is the (non-primitive subfield code) generalized Reed-Muller code $C = \mathcal{R}^{q-1}_{\mathbb{F}_q/\mathbb{F}_p}((m-r)(q-1), m+1)$. It has minimum weight $\frac{q^{r+1}-1}{q-1}$ and the minimum weight vectors are the multiples of the incidence vectors of the blocks.*

The p-rank is given by the cardinality of the set of integers u satisfying $0 \leq u \leq q^{m+1}-1$ where $q-1$ divides u and $\mathrm{wt}(up^j) \leq (m-r)(q-1)$, for $j = 0, 1, \dots, t-1$, where up^j is reduced modulo $q^{m+1}-1$.

The dual code $C^\perp$ satisfies $C^\perp \supseteq \mathcal{R}^{q-1}_{\mathbb{F}_q/\mathbb{F}_p}((m-r)(q-1), m+1) \cap \langle \mathbf{1} \rangle^\perp$ and has minimum weight at least $\frac{q^{m-r+1}-1}{q-1} + 1$, with equality if $q = p$.

In general the dual codes of these codes are not generalized Reed-Muller codes; these are the so-called polynomial codes. Their minimum weight is not known in general and in [77, Section 7] some new results that deduce the minimum weight from the geometrical properties of the designs are described.

5.5 Codes from orbit matrices of symmetric designs

Of great importance in coding theory is the classification of self-orthogonal codes of given length or dimension, see for example [67, 122, 114]. There are several methods in the literature used to classify self-orthogonal codes. Amongst these one popular method is that of orbit matrices. Orbit matrices are also often used to generate and classify designs with a presumed automorphism group. We remind the reader that the notion of orbit matrices was first given in Section 4.5. Our notation is all related to that established in that section. In what follows we give two steps that are commonly used to construct designs from orbit matrices:

For given parameters of orbit length distributions the construction of the designs consists of two steps. The first step is to find all compatible orbit structures (matrices) which means finding all solutions to the Equations (5.1) and (5.2)below.

$$\sum_{r=1}^{t} \gamma_{ir} = k, \tag{5.1}$$

$$\sum_{r=1}^{t} \frac{\Omega_j}{\omega_r} \gamma_{ir}\gamma_{jr} = \lambda\Omega_j + \delta_{ij}(k-\lambda). \tag{5.2}$$

It is worth noting that mutually isomorphic orbit matrices lead to mutually isomorphic designs.

The second step called **indexing** consists of determining precisely which points from the point orbit $\mathcal{P}_r$ are incident with a fixed representative of the block orbit $\mathcal{B}_i$ for each γ_{ir}. The other blocks are obtained as G-images of the constructed representative. The set of all indices of points of the orbit $\mathcal{P}_r$ which are incident with a fixed representative of the block orbit $\mathcal{B}_i$ is called the **index set** for the position (i, r) of the orbit structure and the given representative. This construction then gives all symmetric designs with parameters admitting an automorphism group G acting with presumed orbit length distribution, from which the codes are derived.

Rows and columns of an orbit matrix $\mathcal{M}$ that correspond to non-fixed points and

non-fixed blocks form a sub-matrix called the non-fixed part of the orbit matrix $\mathcal{M}$.

The following theorem proved by Harada and Tonchev [64] gives a construction of self-orthogonal codes from orbit matrices of 2-designs:

Theorem 5.7. *[64, Proposition 1] Let $\mathcal{D}$ be a 2-(v, k, λ) design with a fixed-point-free and fixed-block-free automorphism ϕ of order q, where q is prime. Further, let $\mathcal{M}$ be the orbit matrix induced by the action of the group $G = \langle\phi\rangle$ on the design $\mathcal{D}$. If p is a prime dividing r and λ, then the orbit matrix $\mathcal{M}$ generates a self-orthogonal code of length $b|q$ over $\mathbb{F}_p$.*

In addition to Proposition 5.7 the following result which we quote from [114] helps in the construction of self-orthogonal codes from orbit matrices:

Theorem 5.8. *[114, Theorem 1.113] If G is a cyclic group of a prime order p that does not fix any point or block and $p|(r - \lambda)$, then the rows of the orbit matrix $\mathcal{M}$ generate a self-orthogonal code over $\mathbb{F}_p$.*

The result which follows next is a generalization of Theorem 5.8 and it was proved recently in [39]. This result concerns the construction of self-orthogonal codes from orbit matrices of 2-designs admitting a fixed-point or fixed-block-free action of an automorphism of prime order.

Theorem 5.9. *[39, Theorem 4] Let G be an automorphism group of a symmetric (v, k, λ) design $\mathcal{D}$. If G is a cyclic group of prime order p and $p|(r - \lambda)$, then the rows of the non-fixed part of the orbit matrix generate a self-orthogonal code of length $\frac{v-f}{p}$ over $\mathbb{F}_p$, where f is the number of fixed points.*

The reader is made aware that Theorem 5.9 gives a construction of self-orthogonal codes from the non-fixed parts of orbit matrices of symmetric 2-designs. Based on these results in Chapter 9 we present a classification of self-orthogonal codes obtained from a class of symmetric designs with parameters 2-$(64, 28, 12)$ generated from orbit matrices.

Chapter 6

Links between codes and primitive groups

6.1 Introduction

The study of finite groups prompts many questions about the groups and related structures. The symmetries involved can enable lattices and codes preserved to be examined efficiently. An interplay between groups and codes has been established by the now standard construction given in [78], and later corrected in [79] where codes are obtained from symmetric 1-designs admitting a primitive action of the group, and such that the point and the block stabilizers are conjugate. The designs obtained in this way have the group acting primitively on points and on the blocks. In particular, codes with interesting properties having finite simple groups acting on have been found by a series of subsequent papers. Recently, in [41] a generalization of the construction outlined in [78, 79] was presented. This new construction allows for 1-designs which are not necessarily symmetric, and stabilizers of a point and a block that are not necessarily conjugate, although the group acts primitively on points and on the blocks of the design. The most recent source for reference for codes obtained from the action of primitive groups is perhaps [102]. In what follows we present an account on the known results on codes from primitive groups described as given in

[78] and developed further in [102].

6.2 Codes of designs from primitive permutation representations

6.2.1 Construction method 1

Theorem 6.1. *[78] Let G be a finite primitive permutation group acting on the set Ω of size n. Let $\alpha \in \Omega$, and let $\Delta \neq \{\alpha\}$ be an orbit of the stabilizer G_α of α. If*

$$\mathcal{B} = \{\Delta^g : \ g \in G\}$$

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

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

then $\mathcal{B}$ forms a self-dual 1-$(n, |\Delta|, |\Delta|)$ design with n blocks, 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 vertices of the graph, and on points and blocks of the design.

Proof: See [78].

Remark 6.2. 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, the design obtained is still a self-dual symmetric 1-design with the group operating.

Proof: Let $B_L = \{L^g \mid g \in G\}$. Then we have $G_L = \{g \mid L^g = L\}$ and $G_\alpha \leq G_L \leq G$. Since G_α is maximal $G_L = G_\alpha$ or $G_L = G$. Since $L \neq \Omega$, $G_L \neq G$. We deduce that $G_L = G_\alpha$ and $|B_L| = [G : G_L] = [G : G_\alpha] = |\Omega|$. Hence we get a symmetric $1 - (|\Omega|, |L|, |L|)$ design. ■

Thus the orbits of the stabilizer can be regarded as "building blocks". Since the complementary design (that is, taking the complements of the blocks to be the new blocks) will have exactly the same properties.

This gives all possible designs on which the group act primitively on points and blocks:

Lemma 6.3. *If the group G acts primitively on the points and the blocks of a symmetric 1-design $\mathcal{D}$, then the design can be obtained by orbiting a union of orbits of a point-stabilizer, as described in Theorem 6.1.*

Proof: See [78].

Remark 6.4. If G is simple, then the maximality of the point stabilizer, implies that there is only one orbit of length 1.

Proof: Suppose that G_α fixes also β. Then $G_\alpha = G_\beta$. Since G is transitive, there exists $g \in G$ such that $\alpha^g = \beta$. Then $(G_\alpha)^g = G_{\alpha^g} = G_\beta = G_\alpha$, and thus $g \in N_G(G_\alpha) = N$. Since G_α is maximal in G, we have $N = G$ or $N = G_\alpha$. But G is simple, so we must have $N = G_\alpha$, so that $g \in G_\alpha$ and so $\beta = \alpha$. ■

The following two theorems deal with the automorphism groups of the designs and codes constructed from a finite primitive permutation group in a manner described in Theorem 6.1.

Theorem 6.5. *Let $\mathcal{D}$ be a self-dual 1-design obtained by taking all the images under G of a non-trivial orbit Δ of the point stabilizer in any of G's primitive representations, and on which G acts primitively on points and blocks, then the automorphism group of $\mathcal{D}$ contains G.*

Proof: See [102].

Theorem 6.6. *If C is a linear code of length n of a symmetric $1-(v,k,k)$ design $\mathcal{D}$ over a finite field $\mathbb{F}_q$, then the automorphism group of $\mathcal{D}$ is contained in the automorphism group of C.*

Proof: See [102].

6.2.2 A generalization of construction method 1

In [41], Crnković et al generalized construction method 1 by considering the action of the group on the conjugacy classes of maximal subgroups. In what follows below we outline this construction. In this section we shall use the notation found in [41] and will write $\delta_i G_\alpha$ for $\delta_i^{G_\alpha}$. We refer the reader to [42] for collected results.

Theorem 6.7. *Let G be a finite permutation group acting primitively on the sets Ω_1 and Ω_2 of size m and n, respectively. Let $\alpha \in \Omega_1$ and $\Delta_2 = \bigcup_{i=1}^{s} \delta_i G_\alpha$, where $\delta_1, \ldots, \delta_s \in \Omega_2$ are representatives of distinct G_α-orbits. If $\Delta_2 \neq \Omega_2$ and*

$$\mathcal{B} = \{\Delta_2 g : g \in G\},$$

then $(\Omega_2, \mathcal{B})$ is a $1-(n, |\Delta_2|, \sum_{i=1}^{s} |\alpha G_{\delta_i}|)$ design with m blocks, and G acts as an automorphism group, primitive on points and blocks of the design.

Proof: See [41, Theorem 2]. The proof uses arguments similar to those in the proof of Theorem 6.1. ■

Using construction method 1 gives 1-designs which are not necessarily symmetric, and stabilizers of a point and a block that are not necessarily conjugate. In the above construction of the design $\mathcal{D}(G, \alpha, \delta)$ described in Theorem 6.7, instead of taking a single G_α-orbit, one can take Δ_2 to be any union of G_α-orbits. In fact, this construction gives us all designs on which the group G acts primitively on points and blocks. The following result depicts such cases:

Corollary 6.8. *If the group G acts primitively on the points and the blocks of a 1-design $\mathcal{D}$, then $\mathcal{D}$ can be obtained as described in Theorem 6.7, where Δ_2 is a union of G_α-orbits. The set Δ_1 of blocks incident with the point δ is a union of G_δ-orbits.*

The following interpretation of the construction of a design from Theorem 6.7 is given in [41] (see also [42]):

- the point set is $\Omega_2 = \delta G$, and the block set is $\Omega_1 = \alpha G$,
- the block $\alpha g'$ is incident with the set of points $\{\delta g : g \in G_\alpha g'\}$.

Let a point $\delta g \in \Omega_2$ be incident with a block $\alpha g' \in \Omega_1$. Then for $g \in G_\alpha g'$ there exists $\overline{g} \in G_\alpha$ such that $g = \overline{g}g'$. Hence we have

$$G_{\alpha g'} \cap G_{\delta g} = G_{\alpha g'} \cap G_{\delta \overline{g} g'} = G_\alpha^{g'} \cap G_{\delta\overline{g}}^{g'} = (G_\alpha \cap G_{\delta\overline{g}})^{g'} =$$

$$(G_\alpha \cap G_\delta^{\overline{g}})^{g'} = (G_\alpha^{\overline{g}^{-1}} \cap G_\delta)^{\overline{g}g'} = (G_\alpha \cap G_\delta)^{\overline{g}g'} = (G_\alpha \cap G_\delta)^g.$$

If a point $\delta g \in \Omega_2$ is incident with the block $\alpha \in \Omega_1$, then $G_\alpha \cap G_{\delta g} = (G_\alpha \cap G_\delta)^g$. If the set $\{G_\alpha \cap G_{\delta g} \mid g \in G\}$ contains $Orb(G_\alpha, \Omega_2)$ G_α-conjugacy classes, where $Orb(G_\alpha, \Omega_2)$ is the number of G_α-orbits on Ω_2, then each conjugacy class corresponds to one G_α-orbit, and the incidence relation in the design $\mathcal{D}(G, \alpha, \delta)$ can be defined as follows:

- the block $\alpha g'$ is incident with the point δg if and only if $G_{\alpha g'} \cap G_{\delta g}$ is conjugate to $G_\alpha \cap G_\delta$.

Similarly, if the set $\{G_\alpha \cap G_{\delta g} \mid g \in G\}$ contains $Orb(G_\alpha, \Omega_2)$ isomorphism classes, then the incidence in the design $\mathcal{D}(G, \alpha, \delta)$ can be defined as follows:

- the block $\alpha g'$ is incident with the point δg if and only if $G_{\alpha g'} \cap G_{\delta g} \cong G_\alpha \cap G_\delta$,

6.2.3 Designs from conjugacy classes of maximal subgroups of simple groups

Let G be a simple group and K_1 and K_2 be maximal subgroups of G. The conjugacy class of of K_1 and K_2 is denoted $ccl_G(K_1)$ and $ccl_G(K_2)$ respectively and $|ccl_G(K_i)| = [G : N_G(K_i)]$. Let us denote the elements of $ccl_G(K_1)$ by $K_1^{g_1}, K_1^{g_2}, \ldots, K_1^{g_m}$ and those of $ccl_G(K_2)$ by $K_2^{h_1}, K_2^{h_2}, \ldots, K_2^{h_n}$. The group G acts primitively by conjugation on the conjugacy classes $ccl_G(K_1)$ and $ccl_G(K_2)$ of K_1 and K_2 respectively. In this way a primitive 1-design can be constructed and it is such that:

- the point set of the design is $ccl_G(K_2)$,
- the block set is $ccl_G(K_1)$,

- the block ${K_1}^{g_i}$ is incident with the point ${K_2}^{h_j}$ if and only if ${K_2}^{h_j} \cap {K_1}^{g_i} \cong G_i$, $i = 1, \ldots, k$ where $\{G_1, \ldots, G_k\} \subset \{{K_2}^x \cap {K_1}^y | x, y \in G\}$.

Denote a $1-$design constructed in this way by $\mathcal{D}(G, K_2, K_1; G_1, \ldots, G_k)$.

From the conjugacy class of a maximal subgroup K of a simple group G for example, using the method given earlier the authors postulated in [41] that one can obtain a regular graph, in the following way:

- the vertex set of the graph is $ccl_G(K)$,
- the vertex K^{h_i} is adjacent to the vertex K^{h_j} if and only if $K^{h_i} \cap K^{h_j} \cong G_i$, $i = 1, \ldots, k$, where $\{G_1, \ldots, G_k\} \subset \{K^g \cap K^{g'} \mid g, g' \in G\}$. We denote this graph $\mathcal{G}(G, K; G_1, \ldots, G_k)$.

G acts primitively on the set of vertices of $\mathcal{G}(G, K; G_1, \ldots, G_k)$.

Remark 6.9. Let ψ be an automorphism of a finite group G. Then the design $\mathcal{D}(G, K_2, K_1; G_1, \ldots, G_k)$ is isomorphic to $\mathcal{D}(G, \psi(K_2), \psi(K_1); G_1, \ldots, G_k)$, and the graph $\mathcal{G}(G, K; G_1, \ldots, G_k)$ is isomorphic to $\mathcal{G}(G, \psi(K); G_1, \ldots, G_k)$.

6.3 $\mathbb{F}G$-modules and G-invariant codes

In this section we will present a development of coding theory based on the correspondence between representations of G and $\mathbb{F}G$-modules described in Section 3.2. Moreover, we reformulate some of the concepts given in Section 3 and Chapter 4 adapting some of the definitions of coding theory to work with $\mathbb{F}G$-modules.

Definition 6.10. *Let $\mathbb{F} = \mathbb{F}_q$ be the finite field of q elements where q is a power of a prime p, and G be a finite group acting primitively on a finite set Ω. Let $V = \mathbb{F}\Omega$ be the vector space over $\mathbb{F}$, of all linear combinations of $\sum \lambda_i x$, $\lambda_i \in \mathbb{F}$, $x \in \Omega$ i.e., the vector space with basis the elements of Ω. To define an $\mathbb{F}G-$module on V it suffices to stipulate the action of the elements of G on the basis elements of V. So we consider*

the group action $\rho : G \longrightarrow GL(V)$ *defined by* $\rho(g, x) \mapsto x^g = \rho(g)(x), g \in G, x \in V$. *Extending linearly the induced* G*-action on* V *makes* V *into an* $\mathbb{F}\Omega$*-module called an* $\mathbb{F}\Omega-$ **permutation module** .

In the following we define how a permutation group $G \leq S_n$ acts on $\mathbb{F}\Omega$.

Definition 6.11. *Let* $G \leq S_n$ *and* $g \in G$, *and let* $W \subseteq \mathbb{F}\Omega$ *with* $\mathbf{u} = (u_1, u_2, \ldots, u_j) \in \mathbb{F}\Omega$. *Then we make the following definitions:*

$$\begin{aligned} g(\mathbf{u}) &= g((u_1, u_2, \ldots, u_j)) = (g(u_1), g(u_2), \ldots, g(u_j)); \\ g(W) &= \{g(\mathbf{u}) \mid \mathbf{u} \in W\}, \\ G \cdot W &= \{g(\mathbf{u}) \mid \mathbf{u} \in W,\, g \in G\}. \end{aligned}$$

We now define the notion of G-invariance for codes.

Definition 6.12. *Let* $G \leq S_n$ *and let* $C \subseteq \mathbb{F}\Omega$. *We say that* C *is* **invariant** *under* G *if* $G \cdot C = C$.

Remark 6.13. Notice that since C is a submodule of $\mathbb{F}\Omega$ we can talk about invariant codes. We will show in Lemma 6.16 that a group G that leaves a code C invariant is related to the automorphism group of C. We define and discuss the automorphism group of a code and explore the interplay between G and this automorphism group.

Definition 6.14. *Let* C *be a code of length* n. *We define the automorphism group of* C *as*

$$\mathrm{Aut}(C) = \{g \in S_n \mid g(C) = C\}.$$

The following lemma from [108] will be of use in the chapters which ensue.

Lemma 6.15. *Let* C *be an* $[n, k, d]$ *code and let* $\{b_1, b_2, \ldots, b_k\}$ *be a basis for* C *and* $g \in S_n$. *Then* $g \in \mathrm{Aut}(C)$ *if and only if* $g(b_i) \in C$ *for all* $1 \leq i \leq k$.

Proof: Let $g \in \mathrm{Aut}(C)$. Then by definition $g(c) \in C$ for every $c \in C$ and so the result. Conversely, let $g(b_i) \in C$ for $1 \leq i \leq k$ and let $\mathbf{u} \in C$ so that we can write $\mathbf{u} = \sum_{i=1}^{k} \alpha_i b_i$ for some scalars $\alpha_i \in \mathbb{F}_2$. Then

$$g(\mathbf{u}) = g\left(\sum_{i=1}^{k} \alpha_i b_i\right) = \sum_{i=1}^{k} \alpha_i g(b_i) \in C,$$

and from this expression we deduce that $g(C) \subseteq C$. In fact $g(C) = C$, and hence $g \in \mathrm{Aut}(C)$. ■

Note though that Lemma 6.15 is not practical when finding the automorphism group of a code with large length. More sophisticated tools would be needed in such a case. We discuss next the relationship between $\mathrm{Aut}(C)$ and any group G which leaves C invariant.

Lemma 6.16. *[108] If C is a code, then C is invariant under the group G if and only if $G \leq Aut(C)$.*

Proof: Suppose that $G \leq \mathrm{Aut}(C)$, then $g(C) = C$ for all $g \in G$ which in turn implies that $G \cdot C = C$. Conversely, if $G \cdot C = C$, then

$$\begin{aligned} \{g(\mathbf{u}) \mid \mathbf{u} \in C,\, g \in G\} = C \quad &\Rightarrow \quad g(\mathbf{u}) \in C \text{ for all } \mathbf{u} \in C,\, g \in G \\ &\Rightarrow \quad g(C) = C \text{ for all } g \in G \\ &\Rightarrow \quad G \leq \mathrm{Aut}(C). \blacksquare \end{aligned}$$

Now we define the inner product on $\mathbb{F}\Omega$ that we will be using throughout the thesis. The $\mathbb{F}$-vector space $\mathbb{F}\Omega$ is equipped with a non-degenerate symmetric bilinear form $\langle \cdot, \cdot \rangle$. Let $\mathbf{u}, \mathbf{v} \in \mathbb{F}\Omega$, then $\langle \cdot, \cdot \rangle : \mathbb{F}\Omega \times \mathbb{F}\Omega \longrightarrow \mathbb{F}$ where

$$\langle \mathbf{u}, \mathbf{v} \rangle = \sum_{x \in \Omega} \alpha_x \beta_x \text{ for all } \mathbf{u} = \sum_{x \in \Omega} \alpha_x x,\, \mathbf{v} = \sum_{x \in \Omega} \beta_x x \in \mathbb{F}\Omega$$

is an inner product on $\mathbb{F}\Omega$.

The following is a reformulation of Definition 4.8.

Definition 6.17. *Let W be a submodule of a permutation module $\mathbb{F}\Omega$. The* **dual code** *of W denoted by $W^{\perp}$, is the orthogonal under the given inner product, that is $W^{\perp} = \{\mathbf{u} \in \mathbb{F}\Omega \mid \langle \mathbf{w}, \mathbf{v} \rangle = 0 \text{ for all } \mathbf{w} \in W\}$.*

Lemma 6.18. *Let C be a G-invariant code, then $C^{\perp}$ is also G-invariant.*

Proof: For any $g \in G$ and any $\mathbf{u} = \sum_{x \in \Omega} \alpha_x x$ and any $\mathbf{v} = \sum_{x \in \Omega} \beta_x x \in \mathbb{F}\Omega$, we

have

$$\begin{aligned}\langle g(\mathbf{u}), g(\mathbf{v})\rangle &= \left\langle g(\sum_{x\in\Omega}\alpha_x x), g(\sum_{x\in\Omega}\beta_x x)\right\rangle \\ &= \left\langle \sum_{x\in\Omega}\alpha_x g(x), \sum_{x\in\Omega}\beta_x g(x)\right\rangle \\ &= \sum_{x\in\Omega}\alpha_x\beta_x \\ &= \langle \mathbf{u}, \mathbf{v}\rangle.\end{aligned}$$

That is, the classical inner product on $\mathbb{F}\Omega$ is G-invariant in the following sense:

$$\langle g(\mathbf{u}), g(\mathbf{v})\rangle = \langle \mathbf{u}, \mathbf{v}\rangle.$$

Now, suppose that C is G-invariant and let $w \in C^{\perp}$, $u \in C$, and $g \in G$. Since C is G-invariant it follows that $\langle g(w), u\rangle = \langle g(w), g(w')\rangle$ for some $w' \in C$. As we have seen earlier the inner product is preserved, so $\langle g(w), g(w')\rangle = \langle w, w'\rangle$. By definition of dual code we get $\langle w, w'\rangle = 0$. Therefore, $\langle g(w), u\rangle = 0$ and $g(w) \in C^{\perp}$ for all $g \in G$. Thus $C^{\perp}$ is G-invariant. In addition $C^{\perp}$ is an $\mathbb{F}G$-submodule. ■

6.3.1 Codes from quotient modules

Codes obtained from permutation representations of finite groups have been given particular attention in recent years. Given a representation of group elements of a group G by permutations one can work modulo p and obtain a representation of G on a vector space V over $\mathbb{F}_p$. The invariant subspaces (the subspaces of V taken into themselves by every group element) are then all the binary codes C for which G is a subgroup of $\mathrm{Aut}(C)$. Similarly we could produce codes over fields of characteristic p, where $p > 2$. This modulo-theoretic technique has been used in [13, 14, 83]. In [83], Knapp and Schmid consider $[n, k, d]_q$ codes where the monomial automorphism group is a particular group. The groups examined were the alternating groups A_n, the symmetric groups S_n and the Mathieu groups written as permutation groups of degree n and associated with codes of length n. Important information about these codes can be obtained from the theory of modular representations of groups. Using these ideas, Calderbank and Wales in [22] construct a binary $[176, 22, 50]_2$ code whose

automorphism group is the Higman-Sims (HS) group. Various arguments yield the Hoffman-Singleton graph on 50 vertices, a 2-$(176, 50, 14)$ design discovered by G. Higman, and the original rank-3 construction of HS.

Brooke in [13, 14] has found all codes obtainable this way from the primitive permutation representations of the simple groups $PSU_4(2)$ and $PSU_3(3)$. In particular are examined all binary codes arising from primitive permutation representations of these groups. The simple group $PSU_4(2)$ of order 25920 has an especially rich structure. It is the simple constituent of the groups $\mathrm{Sp}_4(3)$, $\mathrm{U}_4(2)$, $\Omega^-(6,2)$, $\Omega^+(5,3)$, and of $W(E_6)$, the Weyl group of type E_6. In [13], representations of $PSU_4(2)$ on the 27 lines of the general cubic surface, on the root system of type E_6 as well as some complex 4- and 5-dimensional representations are described. These are used to construct the five primitive permutation representations of degrees 27, 36, 40, 40 and 45. These representations lead to 6, 10, 6, 10 and 22 codes respectively (excluding the zero code and the ambient space). These codes are all inequivalent except for the repetition code $\langle \mathbf{1} \rangle$ and its dual which appear in both representations of degree 40. The group $PSU_3(3)$ has order 6040 and has four permutation representations of degrees 28, 36, 63 and 63 leading to 4, 10, 26 and 42 codes, respectively, all of which are inequivalent except for the repetition code and its dual appearing in both degree 63 representations. A detailed description of the corresponding modular representations over the field with two elements is presented. In each case the complete lattice of submodules is given. Irreducible modules of degrees 1, 6, 8, and 14 are involved. Further the weight distribution of subcodes (that is, submodules) with respect to the standard basis is determined.

Taking G to be a permutation group of degree n, and V the corresponding $\mathbb{F}_2$-permutation module. The submodules of V can be regarded as being G-invariant binary linear codes in V, and one may therefore ask for the weight distribution of these codes. In [14] a search is carried out when (G, V) corresponds to one of the four primitive permutation modules associated with the simple unitary group $G = U_3(3)$, of order 6048. The approach is to regard G as acting 2-transitively on a certain Steiner system $S(2, 4, 28)$, and then to obtain the other primitive representations of

G in terms of the action of $U_3(3)$ on various geometric and algebraic objects that live in $S(2,4,28)$. Of particular interest is the description of $S(2,4,28)$ in terms of the Cayley integers and therefore provide an explicit isomorphism between $U_3(3)$ and $G_2'(2)$.

In [95] a $[275,22,100]_2$ self-orthogonal doubly-even code left invariant by the McLaughlin simple group $\mathrm{M^cL}$ was constructed. Later in [96] a much larger code with a large error correction capability was obtained. This code has parameters $[2300,22,1024]_2$ and is left invariant by the simple group of Conway Co_2. For a collected list of references and more details on codes from permutation representations, the reader is encouraged to consult [35] and [67, Section 7.4].

6.3.2 Codes from maximal submodules

We are interested in finding all G-invariant codes from the primitive permutation representations, hence we shall consider the permutation module obtained from the action of the group on the cosets of its maximal subgroups and thus explore the corresponding $\mathbb{F}\Omega$-submodules (in particular 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). The G-invariant submodules of $\mathbb{F}\Omega$ can be regarded as linear codes in $\mathbb{F}\Omega$, (see Lemma 6.19) and one may therefore ask for the weight distribution of these codes. In this Section and further we combine the techniques discussed in Chapter 3 and Section 6.3 and propose a novel approach in which the modular irreducibles show up as submodules and not as factor submodules, and thus determine all binary codes invariant under a given group more directly, since we obtain explicit bases for the codes. Moreover, for each primitive representation of a given permutation group G, we use Meat-Axe recursively and Magma [27] to construct the associated permutation module over $\mathbb{F}_2$ and subsequently a chain of its maximal submodules. Each maximal submodule constitutes in turn the binary code that is invariant under G. After eliminating

isomorphic copies, we obtain a lattice of submodules, thus in some way responding to the classification and enumeration problems alluded to earlier. This approach can be seen as dual to that used in Section 6.3.1 with the advantage that the codes are intrinsically the submodules without having the tedious and cumbersome task of defining quotients of irreducible submodules.

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 (see Theorem 2.6 and Theorem 2.16) 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 $\mathbb{F}_q$ corresponding to this representation is constructed as described above. We shall consider these permutation modules which are vector spaces to construct subspaces. The G-invariant subspaces (i.e., submodules) of the permutation module give all the p-ary codes invariant under G. The approach offered by this section, which is at the core of the purpose of the thesis, is more inclusive than that presented in sections 6.2.1 and 6.2.2. The codes constructed using those methods are in general subcodes of the ones constructed using the method that we present in the ensuing section. Since this thesis is concerned with binary codes we restrict our attention to the field $\mathbb{F} = \mathbb{F}_2$ and prove the following lemma

Lemma 6.19. *[108] Let G be a finite group and Ω a finite G-set. Then the $\mathbb{F}_2G$-submodules of $\mathbb{F}\Omega$ are precisely the G-invariant codes (i.e., G-invariant subspaces of $\mathbb{F}\Omega$).*

Proof: 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 $\rho : G \longrightarrow GL(V)$ be a representation of G given by

$$\rho(g)(x) = g(x) \quad \text{for all } g \in G \quad \text{and } x \in V.$$

We can consider V as the $\mathbb{F}_2G$-module obtained from ρ. Let $\mathcal{S}$ be an $\mathbb{F}_2G$-submodule of the permutation module V. Then by Definition 6.12 of G-invariant code (see also

Definition 3.5) we have

$$\left(\sum_{g\in G}\alpha_g g\right)\cdot S\in\mathcal{S} \quad \text{for all } \sum_{g\in G}\alpha_g g\in\mathbb{F}_2G \text{ and } S\in\mathcal{S}.$$

In particular,

$$g\cdot S\in\mathcal{S} \text{ for all } g\in G \text{ and } S\in\mathcal{S}.$$

Thus, for all $g\in G$ and $S\in\mathcal{S}$ we obtain $\rho(g)(S)\in\mathcal{S}$ or $g(S)\in\mathcal{S}$ and so $\mathcal{S}$ is G-invariant. Conversely, if $\mathcal{S}$ is G-invariant, then for all $g\in G$ and $S\in\mathcal{S}$ we have $\rho(g)(S)\in\mathcal{S}$. Therefore for scalars $\alpha_g\in\mathbb{F}_2$ we have

$$\sum_{g\in G}\alpha_g\rho(g)(S)\in\mathcal{S}$$

by linearity. This implies that

$$\left(\sum_{g\in G}\alpha_g g\right)\cdot S\in\mathcal{S}. \blacksquare$$

6.4 Construction of G-invariant codes

Lemma 6.19 implicitly gives us the strategy of finding all codes with a group G acting as an automorphism group. We explicitly outline the steps. Given a permutation group G acting on a finite set Ω, and $\rho : G\longrightarrow GL(V)$ where $\rho(g)(x)=g(x)$ with $g\in G$ and $x\in V$. The steps are as follows:

1. Recognize $\mathbb{F}_2\Omega$ as a permutation module;
2. Using Meat-Axe find all the maximal $\mathbb{F}_2G$-submodules;
3. Using the submodules determine where possible the lattice structure of the permutation module;
4. By Lemma 6.19 the submodules are the G-invariant codes;
5. Test equivalence and filter isomorphic copies;
6. Test irreducibility of the code.

The construction therefore requires that we find all submodules of the permutation module. For this we decompose the permutation module into submodules. These constitutes the building blocks for the construction of a lattice of submodules where possible, thus attaining an answer to the enumeration problem. With the characterization of these codes we respond to the problem of classification of the codes. As was discussed in Chapter 3 decomposition of the modules into submodules depends on the field. Maschke's Theorem gives a characterization of decomposition over a field whose characteristic is 0 or relatively prime to the order of the group. In this case the permutation module is completely reducible and can be written as a direct sum of its irreducible submodules. When the characteristic p of the field divides the order of the group i.e., $p \mid |G|$, we apply Krull-Schmidt's Theorem (see Theorem 3.22) 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. In addition to Krull-Schmidt theorem, we have the composition series of the module which provides a way of breaking the module into simple components. These concepts have been used to develop different methods to construct submodules hence codes invariant under a group. Applying all these theories and techniques we set about constructing G-invariant codes which have certain classes of finite simple groups acting irreducibly on. In chapters 7, 8 and 10 we shall see how a combination of the techniques outlined in Sections 6.2.1, 6.2.2 and Section 6.3.2 help determine and classify a number of interesting codes invariant under the simple groups $L_3(4)$, A_8 and $S_6(2)$ respectively. Much of this work is presented in the chapters that follow and are the content of [29, 32, 31].

Chapter 7

Binary codes invariant under $L_3(4)$

7.1 Introduction

This chapter makes an attempt to answer the following general problem: given a prescribed group, determine all invariant p-ary codes under the group. This is an enumeration and classification problem which has a merit of its own, but it is also one that lends itself naturally to revealing an interplay between coding theory and modular representation theory. As a by-product one may therefore enumerate and classify all submodules and hence codes invariant under a given group. An earlier attempt in this direction was carried in [83] with a view of studying codes via monomial actions and projective representations of transitive permutation groups. Later in [13, 14] all binary codes obtainable from the primitive permutation representations of the simple groups $U_4(2)$ and $U_3(3)$ were found using irreducible modules. See also [28] for related results. More recently in [80], the authors looked particularly at those codes from the irreducible modules invariant under the Janko groups J_1 or J_2, and in particular those of small dimension. It is our view that the enumeration and classification of codes invariant under a prescribed finite group is an intricate problem and that a definite or complete answer to it is not easily attainable, due to there being many perspectives and approaches, and also due to current computational limitations, particularly when the degree of the primitive representations is significantly large. We construct and enumerate all non-trivial

binary linear codes from the 2-modular primitive representations of the simple group $L_3(4)$, using a chain of maximal submodules of a permutation module induced by the action of $L_3(4)$ on objects such as the lines, hyperovals, Baer subplanes and unitals of $PG_2(4)$. Several codes with interesting properties are obtained, among these optimal and self-orthogonal codes invariant under $L_3(4)$. We establish results on non-existence of $L_3(4)$-invariant self-dual codes of lengths 56, 120 and 280 respectively, and moreover that $L_3(4)$ is not realizable as the automorphism group of a binary linear code. A fundamental problem in coding theory is to optimize one of the parameters n, k, d given the other two (over a given field $\mathbb{F}_q$). Two versions of the problem are known, namely to find the smallest n for which an $[n,\, k,\, d]_q$ code exists; and to find the maximum distance d for which an $[n, k, d]_q$ code exists. In this chapter we deal with the second problem, for some linear codes over $\mathbb{F}_2$. Recall that a linear $[n,\, k]$ code C is called optimal if $n = n_q(k,\, d)$ or $d = d_q(n,\, k)$ (see [17] or [58, 59] for known bounds on the highest minimum weight). Optimal codes have been the object of research for some time. We prove that the binary codes with parameters $[21, 9, 8]$, $[21, 12, 5]$, $[21, 11, 6]$ (two inequivalent such codes), $[21, 10, 7]$, $[56, 46, 4]$, $[56, 19, 16]$, $[56, 20, 16]$, $[56, 36, 8]$, $[56, 35, 8]$, $[120, 100, 6]$, $[120, 100, 6]$, $[120, 101, 6]$ and $[120, 110, 4]$ are all optimal. We were unable to determine the optimality of the codes obtained from the 280-dimensional representation presented for this representation, since the current databases give optimality up to length 256.

7.2 Binary codes from primitive representations of $L_3(4)$

In this section we use the techn presented in Chapter 6 and in particular Section 6.3.2. We consider for illustration the simple linear group $PSL_3(4) = L_3(4)$ and $(L_3(4), V)$ corresponds to each of the four primitive permutation modules associated with $L_3(4)$, as described, for example in [34]. iquesWe choose to study this particular group for the following reasons: it is a subgroup of 15 of the 26 sporadic simple groups, especially of M_{24}, HS and $\mathrm{M^cL}$; it is a small member of the two classes

$L_3(q)$ and $L_3(q^2)$; and its rich geometrical structure would enable us explore further the interplay between geometries, designs, graphs and some classes of codes. In addition, the degrees of the representations of $L_3(4)$ are small enough to reveal the advantages of our approach, but sufficiently large to expose the computational difficulties involved in finding the lattice of the submodules, and hence enumerating and classifying all submodules invariant under a group. We examine the properties of these submodules as codes and present their weight distributions. Moreover, using the well-known Assmus-Mattson Theorem and the transitivity of the groups we determine some designs or graphs that are defined by codewords of several weights in the codes and we use the properties of these designs or graphs and their geometry to gain some insight into the nature of some classes of codewords, mainly those of minimum weight. In particular, we establish that the sets of codewords of several non-zero weights are single orbits stabilized by maximal subgroups of the automorphism groups, and hence several designs obtained from these sets are primitive. Using the Atlas of Brauer characters [70] to determine the irreducibility of the codes and the MacWilliams identities relating the weight enumerators of the dual codes. We are thus able to determine and enumerate all submodules, and hence all non-trivial binary codes invariant under $L_3(4)$ and consequently prove the following main result:

Theorem 7.1. *Let G be the linear group $L_3(4)$, Ω a primitive G-set and C a linear code over $\mathbb{F}_2$ admitting G as an automorphism group. The following holds:*
(a) C is obtainable up to isomorphism from one of the 2-modular primitive representations of G as a $\mathbb{F}_2G$-submodule of the permutation module $\mathbb{F}_2\Omega$.
(b) There exists a set of non-trivial codewords of C which constitutes a single orbit of $\mathrm{Aut}(C)$ that is stabilized by a maximal subgroup of $\mathrm{Aut}(C)$.
(c) There are no $L_3(4)$-invariant self-dual codes of lengths 56, 120, and 280 respectively.
(d) $\mathrm{Aut}(C) \ncong L_3(4)$ for all C, and there is no $L_3(4)$-invariant self-orthogonal code C such that $\mathrm{Aut}(C) \cong L_3(4)$.

7.3 The primitive permutation representations

We consider G to be the simple linear group $PSL_3(4)$ denoted in the $\mathbb{ATLAS}$ [34] as $L_3(4)$, the group of all non-singular 3×3 matrices whose determinant is 1, over $\mathbb{F}_4$. This group has order 20160, and its automorphism group is an extension of $L_3(4)$ by the dihedral group D_{12}. There are nine primitive permutation representations of degrees 21, 21, 56, 56, 56, 120, 120, 120 and 280 respectively (see [34]). The representations are shown in Table 7.1, where the first column gives the ordering of the primitive representations as given by Magma (or the $\mathbb{ATLAS}$) and as used in our computations; the second gives the degree (the number of cosets of the point stabilizer); the third gives the structure of the maximal subgroups; the fourth gives the number of orbits of the point-stabilizer, and the remaining columns give the length of the orbits.

no	Degree	Max Subgroup	no. of orbits	orbit length
1	21	$2^4 : A_5$	2	$1, 20$
2	21	$2^4 : A_5$	2	$1, 20$
3	56	A_6	3	$1, 10, 45$
4	56	A_6	3	$1, 10, 45$
5	56	A_6	3	$1, 10, 45$
6	120	$L_3(2)$	4	$1, 21, 42, 56$
7	120	$L_3(2)$	4	$1, 21, 42, 56$
8	120	$L_3(2)$	4	$1, 21, 42, 56$
9	280	$3^2 : Q_8$	8	$1, 9, 18(3), 72(3)$

Table 7.1: Maximal subgroups of $L_3(4)$.

We summarize the information obtained for the group and use notations for the objects which are permuted in each of its primitive permutation representations. The primitive representations may also be described (often in several ways, see for example the $\mathbb{ATLAS}$ [34]) in terms of the action of G on various sets of geometrical objects: we shall use the notations $g(m)(m = 21a, 21b, 56a, 56b, 56c, 120a, 120b, 120c, 280)$ to denote these orbit sets. We will use names in terms of the linear notation as provided in [34], namely point, line, hyperoval, and the notation given in [116], that is, Baer subplanes and unitals.

7.4 Incidence relations

The action of a group fixing an element of $g(m)$ may be transitive on the elements of $g(n)$ or may split these elements into several orbits or into two orbits if $m \neq n$, of which one has size one if $m = n$. The rows and columns of Table 7.2 represent the intersection of lines, hyperovals, subplanes and unitals. The sizes of the corresponding orbits are illustrated. If we denote the entries in Table 7.2 by a_{mn}, then the entry a_{33} corresponds to an intransitive action of an A_6 on an A_6 with three orbits of lengths 1, 10, and 45 respectively. However the entry a_{73} indicates that there are three orbits of an intransitive action of an $L_3(2)$ on an A_6, of which two are of length 7 and one is of length 42, and the entry a_{96} indicates that there are four orbits of an intransitive action of a $3^2{:}Q_8$ on an $L_3(2)$, one with length 12, two with length 18 and one of length 72.

	n								
m	$21a$	$21b$	$56a$	$56b$	$56c$	$120a$	$120b$	$120c$	280
$21a$	1-20	5-16	16-40	16-40	16-40	40-80	40-80	40-80	120-160
$21b$	5-16	1-20	16-40	16-40	16-40	40-80	40-80	40-80	120-160
$56a$	6-15	6-15	1-10-45	20-36	20-36	60^2	15^2-90	60^2	10-90-180
$56b$	6-15	6-15	20-36	1-10-45	20-36	15^2-90	60^2	60^2	10-90-180
$56c$	6-15	6-15	20-36	20-36	1-10-45	60^2	60^2	15^2-90	10-90-180
$120a$	7-14	7-14	28^2	7^2-42	28^2	1-21-42-56	8-28-84	8-28-84	28-42^2-168
$120b$	7-14	7-14	7^2-42	28^2	28^2	8-28-84	1-21-42-56	8-28-84	28-42^2-168
$120c$	7-14	7-14	28^2	28^2	7^2-42	8-28-84	8-28-84	1-21-42-56	28-42^2-168
280	9-12	9-12	2-18-36	2-18-36	2-18-36	12-18^2-72	12-18^2-72	12-18^2-72	1-9-18^3-72^3

Table 7.2: Orbits of $g(m)$ on $g(n)$.

7.5 The 2-modular representations

The elements of each $g(m)$ generate a permutation module over $\mathbb{F}_2$. We shall consider these $\mathbb{F}_2$-modules, and their invariant submodules under the action of G. The sections that follow present the calculations on these modules. According to Lemma 6.19, the vectors in each submodule form a code, over $\mathbb{F}_2$, whose length is the dimension of the permutation module and whose dimension is the dimension of the submodule.

The weight enumerators of the submodules are therefore also the weight enumerators of these codes which are invariant under the action of G. Observe that the rank-r representations of this group, for $2 \leq r \leq 3$, are pairwise equivalent under an outer automorphism (see Table 7.1 and [34]), and thus their submodules (resp. codes) are isomorphic (resp. equivalent). In all such cases we only consider the submodules (resp. codes) obtained from the first representation of that degree. Notice for example from Table 7.1, that there are two rank-2 representations of degree 21. In this case we examine only the submodules corresponding to the first representation as the submodules (resp. codes) obtained from the other representation of the same degree are isomorphic (resp. equivalent).

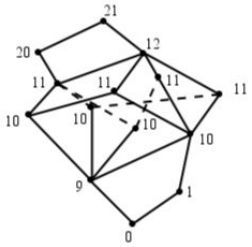
7.6 A 21-dimensional representation

Let $\Pi = PG_2(4)$ denote the (unique) projective plane of order four. Among the small finite projective planes, Π plays an outstanding role. Its combinatorics and the interplay between geometric objects like Baer subplanes, hyperovals, unitals, etc, have been studied often (see e.g. [55]) and the references therein). Notice from Table 7.2 (see also Table 7.1) that there are two non-conjugate classes of maximal subgroups of G of index 21 when G acts doubly transitively on the cosets of $2^4{:}A_5$ with orbits of lengths 1 and 20 respectively. Using this action and taking for m either $21a$ or $21b$ we form a 21-dimensional permutation module invariant under G. From the $\mathbb{ATLAS}$ [34] we observe that the constituents being permuted by the group in these representations are points and lines. Thus the action is that of G on the points and lines of Π. The permutation module splits into three absolutely irreducible constituents of dimensions 1, 9, and 9 with multiplicities 3, 1, and 1 respectively. There are only two irreducible submodules in this representation, one of dimension 1 and one of dimension 9. Moreover, the permutation module has two maximal submodules of dimensions 12 and 20 respectively. We take these submodules to be our working modules and recursively find all maximal submodules of each module. Note that the recursion terminates as soon as we reach an irreducible maximal

submodule. In so doing we determine all codes associated with the permutation module of dimension 21 and invariant under G. Now, from the 20-dimensional module we get one maximal submodule of dimension 11; and from the 12-dimensional module we get seven maximal submodules each of dimension 11. Four of these submodules (namely the 2nd, 4th, 6th and 7th) are isomorphic to the 11-dimensional submodule we got from the earlier 20-dimensional module, thus we have four non-isomorphic submodules of dimension 11. The 11-dimensional submodule from the 20-dimensional module has three non-isomorphic maximal submodules each of dimension 10. From each of these 10-dimensional submodules, we get one irreducible 9-dimensional submodule. From each of the three remaining non-isomorphic 11-dimensional submodules we get two maximal submodules of dimension 10. The first 10-dimensional submodlue contains an irreducible maximal submodule of dimension 9, and the other contains two irreducible maximal submodules of dimensions 1 and 9 respectively. All the 9-dimensional submodules are isomorphic and irreducible.

Putting this information together we find that the permutation module has submodules of dimensions $1, 9, 10, 10, 10, 10, 11, 11, 11, 11, 12, 20$ and 21 respectively, with the lattice of submodules as shown in Figure 7.1.

Figure 7.1: Submodule lattice for a 21-dimensional representation



In [13, 14] Brooke, uses a dual approach to the one described above. We briefly sketch that technique: he uses irreducible submodules to factor out the module and get the quotient modules. If the quotient modules are not irreducible, he finds the corresponding irreducible submodules and continues factoring out. This process is repeated until an irreducible quotient is found. Using Brooke's approach one has the added inconvenience of having to define the codes, since the quotient modules will

not provide an explicit basis. This makes the quotient method more cumbersome and tedious, although both methods yield similar results. The method presented here, however has the advantage that the modular irreducibles show up as submodules and not as factor submodules. In this case we produce the codes more directly, since we obtain an explicit basis.

From the earlier remarks note that there are four non-isomorphic 11-dimensional submodules in this representation which in turn give rise to four 11-dimensional codes. However, two of these codes have the same weight distribution. To distinguish the codes we look at codewords of the same weight and count the number of times a 1 occurs on every coordinate. These sets are known as multisets (see [62]). We list the results in Table 7.3 where we deduce that the first two codes have the same multiset for all weights, so we have isomorphic copies. The next two codes (those with minimum weight 6) have different multisets, and so are non-isomorphic. This method was used in all other instances of the work where a distinction of the codes was required, (see for example Sections 7.8 and 7.9). The notation a^b used in Table 7.3 means that there are a ones on b coordinates. For instance, in both cases for the codes with parameters $[21, 11, 5]_2$, for weight 5 we have 5 ones on 21 coordinates.

weight	$[21, 11, 5]_2$	$[21, 11, 5]_2$	$[21, 11, 6]_2$	$[21, 11, 6]_2$
5	5^{21}	5^{21}		
6	16^{21}	16^{21}	16^{21}	48^{21}
7	40^{21}	40^{21}	80^{21}	
8	80^{21}	80^{21}	80^{21}	80^{21}
9	120^{21}	120^{21}		
10	160^{21}	160^{21}	160^{21}	480^{21}
11	176^{21}	176^{21}	352^{21}	
12	160^{21}	160^{21}	160^{21}	160^{21}
13	130^{21}	130^{21}		
14	80^{21}	80^{21}	80^{21}	240^{21}
15	40^{21}	40^{21}	80^{21}	
16	16^{21}	16^{21}	16^{21}	16^{21}

Table 7.3: Multisets for the 11-dimensional codes.

We thus obtain ten non-trivial submodules, namely of dimensions 9, 10, 10, 10, 10, 11, 11, 11, 11 and 12 respectively. However using Table 7.3 and the preceding discussion we have that the codes $[21, 9, 8]$, $[21, 12, 5]$, $[21, 10, 5]$, $[21, 11, 6]$, $[21, 10, 6]$, $[21, 11, 5]$, $[21, 10, 7]$, $[21, 11, 6]$ are all binary codes obtainable in this way, from this

representation. In the above listing, each code is followed by the corresponding dual. We shall denote the codes $C_{21,i}$ and their duals $C_{21,i^\perp}$, with $i = 1, \ldots, 4$.

The weight distribution of these codes is given in Table 7.4 below.

Table 7.4: The weight distribution of the codes from a 21-dimensional representation.

name	dim	0	5	6	7	8	9	10	11	12	13	14	15	16	21
$C_{21,1}$	9	1				210				280				21	
$C_{21,2}$	10	1		56		210		336		280		120		21	
$C_{21,3}$	10	1	21			210	280			280	210			21	1
$C_{21,4}$	10	1			120	210			336	280			56	21	
${C_{21,4}}^\perp$	11	1		56	240	210		336	672	280		120	112	21	
${C_{21,3}}^\perp$	11	1		168		210		1008		280		360		21	
${C_{21,2}}^\perp$	11	1	21	56	120	210	280	336	336	280	210	120	56	21	1
${C_{21,1}}^\perp$	12	1	21	168	360	210	280	1008	1008	280	210	360	168	21	1

Remark 7.2. The eight codes are interrelated. Notice that $C_{21,1}$ is a subcode of all these codes while ${C_{21,1}}^\perp$ contains all of them. The containment as shown below can be immediately deduced from Table 7.4 or using Figure 7.1.

Proposition 7.3. (i) $C_{21,3} \subset {C_{21,2}}^\perp \subset {C_{21,1}}^\perp$,
(ii) $C_{21,2} \subset {C_{21,3}}^\perp \subset {C_{21,1}}^\perp$,
(iii) $C_{21,2} \subset {C_{21,4}}^\perp \subset {C_{21,1}}^\perp$,
(iv) $C_{21,4} \subset {C_{21,2}}^\perp \subset {C_{21,1}}^\perp$.

Using Table 7.4 and Proposition 7.3 we make some observations about the codes, in particular the minimum weight, structure of the automorphism groups and a description of the nature of the minimum words. These properties are examined with certain detail in Proposition 7.4.

Proposition 7.4. (i) *The code $C_{21,1}$ is self orthogonal and doubly-even, with minimum weight 8. It is a $[21, 9, 8]_2$ code, and its dual ${C_{21,1}}^\perp$ is a $[21, 12, 5]_2$ code. Moreover $C_{21,1}$, ${C_{21,1}}^\perp$ are optimal codes,* $\mathrm{Aut}(C_{21,1}) \cong L_3(4){:}S_3$, *and $L_3(4){:}S_3$ acts irreducibly on $C_{21,1}$ as an $\mathbb{F}_2$-module.*
(ii) *The code $C_{21,2}$ is a self orthogonal singly-even code, with minimum weight 6. It is a $[21, 10, 6]_2$ code, and its dual ${C_{21,2}}^\perp$ is a $[21, 11, 5]_2$ code. Moreover*

$\mathrm{Aut}(C_{21,2}) \cong L_3(4) \cdot 2_2 \cong P\Sigma L_3(4)$.

(iii) *$C_{21,3}$ is a $[21, 10, 5]_2$ decomposable code with 21 codewords of weight 5. Its dual ${C_{21,3}}^{\perp}$ is a $[21, 11, 6]_2$ optimal singly-even code, and* $\mathrm{Aut}(C_{21,3}) \cong L_3(4){:}S_3$.

(iv) *$C_{21,4}$ is a $[21, 10, 7]_2$ code. The dual ${C_{21,4}}^{\perp}$ of $C_{21,4}$ is a $[21, 11, 6]_2$ code. Moreover $C_{21,4}$ and ${C_{21,4}}^{\perp}$ are optimal codes, and* $\mathrm{Aut}(C_{21,4}) \cong L_3(4) \cdot 2_2 \cong P\Sigma L_3(4)$.

Proof: Since $L_3(4)$ acts 2-transitively on the set of coordinates of $C_{21,i}$, it follows that the support of a codeword of any fixed non-zero weight in $C_{21,i}$ yields a 2-design. Let L denote the set of weights of the non-zero codewords $w_l \in C_{21,i}$ and define $C_l = \{w_l \in C_{21,i} \mid \mathrm{wt}(w_l) = l, \text{ for } l \in L\}$ and $A_l = |C_l|$. Taking images under $L_3(4)$ of the support of $w_l \in C_l$ we form the blocks of a 2-$(21, l, \lambda)$ design $\mathcal{D}_{w_l}$ with A_l blocks.

The proof now proceeds by case examination, using the action of the group on the minimum weight codewords. Thus in case (i) we look at the words of minimum weight 8 in $C_{21,1}$. Since there are precisely 210 codewords of minimum weight 8 in $C_{21,1}$ and this is precisely the number of blocks of a 2-$(21, 8, 28)$ design $\mathcal{D}_{w_8}$, formed by taking the images under G of the support of those codewords, it follows that these are the incidence vectors of the blocks of the design, and so $C_{21,1}$ is span by its minimum weight codewords (see [112] for the uniqueness of D_{w_8}). Since the incidence vectors of the blocks of the design span the code, and the vectors have weight divisible by 4, $C_{21,1}$ is doubly-even, and thus self-orthogonal; consequently, we have that $\mathbf{1} \in {C_{21,1}}^{\perp}$ since the block size of D_{w_8} is even. Moreover, since the incidence matrix of $\mathcal{D}_{w_8}$ generates $C_{21,1}$ by applying [19, Theorem 11.13] we obtain $\mathrm{Aut}(\mathcal{D}_{w_8}) = \mathrm{Aut}(C_{21,1})$. We now describe the structure of the automorphism group. Let $\overline{G} = \mathrm{Aut}(C_{21,1})$. Using Magma we found that $\overline{G}$ is a non-abelian group generated by the permutations denoted

$$\begin{aligned} u &= (2,7)(3,21)(4,17)(6,9)(8,11)(12,14)(15,19), \\ v &= (1,16,17)(2,9,3)(4,20,12)(5,14,6)(7,11,15)(8,13,10)(18,19,21) \end{aligned}$$

and that $\overline{G}$ contains a unique non-abelian simple normal subgroup N of order 20160, isomorphic to $L_3(4)$. Thus $\overline{G} \cong L_3(4) \cdot H$ where H is a group of order 6. Since H

has no element of order 6, it follows that $H \cong S_3$, and so $\overline{G} \cong L_3(4) \cdot S_3$. In fact, a composition series for $\overline{G}$ is $\overline{G} \geq N \geq \mathbb{Z}_3 \geq \mathbb{Z}_2 \geq 1$, which is a chief series for $\overline{G}$. Hence $\overline{G} = L_3(4) \cdot 3 \cdot 2$. From [34] we have that there are two groups of type $L_3(4) \cdot 3 \cdot 2$, namely $L_3(4) \cdot 3 \cdot 2_1$ and $L_3(4) \cdot 3 \cdot 2_2$. But, since u and v satisfy $u^2 = v^3 = (uv)^{14} = 1$ and $\overline{G} = \langle u, v \rangle$ we conclude that $\overline{G} \cong L_3(4) \cdot 3 \cdot 2_2 \cong L_3(4){:}S_3$. Hence the result.

Furthermore, the 2-modular character table of $L_3(4)$ is completely known (see [70]) and it follows from it that the irreducible 9-dimensional $\mathbb{F}_2$-representation is unique and 9 is the smallest dimension for any non-trivial irreducible $\mathbb{F}_2$-module. Since $\mathrm{Aut}(C_{21,1})$ contains $L_3(4)$, using the weight distribution as given in Table 7.4 we can easily see that under the action of $L_3(4)$, $C_{21,1}$ does not contain an invariant subspace of dimension 1. So, if $C_{21,1}$ is reducible, it must contain an invariant irreducible subspace $\mathcal{M}$ of dimension m with $2 \leq m \leq 8$, which is not possible. Hence $C_{21,1}$ is irreducible and must be isomorphic to the 9-dimensional $\mathbb{F}_2$-module on which $L_3(4)$ acts irreducibly.

(ii) The claims on self-orthogonality, minimum weight and $\mathbf{1}$ in ${C_{21,2}}^{\perp}$ follow *mutatis mutandis* the arguments used in the proof of part (i). For the automorphism group notice that the minimum weight codewords span the code and these are also incidence vectors of a unique 2-$(21, 6, 4)$ design (see [112]) denoted $\mathcal{D}_{w_6}$ with 56 blocks, formed by taking the image under $L_3(4)$ of the support of the codewords of minimum weight 6. Let $\mathrm{Aut}(C_{21,2}) = \Gamma$. Since $L_3(4)$ acts on the code coordinates we have that $L_3(4) \subseteq \Gamma$ and since $|\Gamma| = 2 \times |L_3(4)| = |L_3(4){:}2|$ we have $\Gamma = L_3(4){:}2$. From [34] we note that there are three groups of shape $L_3(4){:}2$, namely $L_3(4){:}2_1$, $L_3(4){:}2_2$ and $L_3(4){:}2_3$ respectively. However, since Γ is a group generated by the permutations

$$\begin{aligned} a &= (1,3)(4,16)(5,11)(7,10)(9,20)(13,14)(18,19), \\ b &= (1,8,11,13,18)(2,15,12,3,16)(4,10,19,17,6)(5,9,21,7,20), \end{aligned}$$

satisfying

$$a^2 = b^5 = (ab)^{14} = (ab^2)^8 = 1,$$

we have $\Gamma \cong L_3(4){:}2_2$ and the assertion follows. For the proof of the automorphism group one could alternatively use the fact that $\mathcal{D}_{w_6}$ is a quasi-symmetric design and

that the block graph of this design is a graph isomorphic to the Gewirtz graph. The automorphism group of this graph is $L_3(4){:}2^2$ (see [16] or Proposition 7.12(ii) below). Moreover, the automorphism group of this code is a subgroup of index 2 in $L_3(4){:}2^2$

(iii) Notice from Proposition 7.3 that $C_{21,1} \subseteq C_{21,3}$ and that $C_{21,3}$ is a code obtained by adjoining the all-one vector $\mathbf{1}$ to $C_{21,1}$. Then $C_{21,3} = \langle C_{21,1}, \mathbf{1}\rangle = C_{21,1} \oplus \langle \mathbf{1}\rangle$ and $C_{21,1}$ and $\langle \mathbf{1}\rangle$ are $L_3(4){:}S_3$-invariant subspaces of $C_{21,3}$. Thus we deduce that $C_{21,3}$ is a decomposable 10-dimensional $\mathbb{F}_2$-module of $L_3(4){:}S_3$ containing the 9-dimensional $\mathbb{F}_2$-module $C_{21,1}$.

Now, if $\gamma \in \mathrm{Aut}(C_{21,1})$, then since $\gamma(\mathbf{1}) = \mathbf{1}$ and $C_{21,3} = \langle C_{21,1}, \mathbf{1}\rangle$, we have $\gamma \in \mathrm{Aut}(C_{21,3})$. So that $\mathrm{Aut}(C_{21,1}) \subseteq \mathrm{Aut}(C_{21,3})$. Since $|\mathrm{Aut}(C_{21,1})| = |\mathrm{Aut}(C_{21,3})|$ it follows from part (i) that $\mathrm{Aut}(C_{21,3}) = L_3(4){:}S_3$.

(iv) Notice first that ${C_{21,2}}^{\perp} = \langle C_{21,4}, \mathbf{1}\rangle$. Thus, arguing similarly as in the proofs of parts (iii) and (ii), for the automorphism group, the result follows.

Finally, it follows from [59] and also from Magma that the codes $C_{21,1}$, ${C_{21,1}}^{\perp}$, ${C_{21,3}}^{\perp}, C_{21,4}$, ${C_{21,4}}^{\perp}$, are optimal. The codes $C_{21,2}$, ${C_{21,2}}^{\perp}$ are a distance 1 less than the optimal, while the code $C_{21,3}$ is a distance 2 from the optimal. ■

Now if w_m is a word of weight i in C, in Section 7.7.1 below we determine the structures of $(\mathrm{Aut}(C))_{w_m}$, i.e, the stabilizers of w_m in $\mathrm{Aut}(C)$. These are listed in Table 7.5. Also for each w_m, we take the support of w_m and orbit it under $G = L_3(3){:}S_3$ or $L_3(4){:}2_2$ to form the blocks of the 2-$(21, m, k_m)$ designs $\mathcal{D}_{w_m}$ where $k_m = |(w_m)^G| \times \frac{m}{21}$. Information on these designs is listed in Table 7.6. Furthermore, Lemmas 7.5 and 7.6 deal with the action of $\mathrm{Aut}(C)$ on the codewords of C.

7.7 Designs held by the support of codewords in $C_{21,i}$

From Table 7.4 we observe that the non-zero codewords of the codes tabulated are single orbits stabilized by subgroups of the automorphism groups. Suppose that w_m is a codeword of non-zero weight m in $C = C_{21,i}$ where $i = 1, 2, 3, 4$. In this section

we determine the structures of $(\mathrm{Aut}(C))_{w_m}$, that is the stabilizers of w_m in $\mathrm{Aut}(C)$. The structures of these stabilizers are listed in Table 7.5.

7.7.1 Stabilizer in $\mathrm{Aut}(C)$ of a word w_i in C

We now examine the action of $\mathrm{Aut}(C) = L_3(4){:}S_3$ or $\mathrm{Aut}(C) = L_3(4) \cdot 2_2$ on the set W_m of non-trivial codewords of C and describe their nature. In addition we look at the structure of the stabilizers $(\mathrm{Aut}(C))_{w_m}$ where $m \in M$ or $\overline{M}$ with M and $\overline{M}$ as defined below. Consider $M = \{5, 6, 7, 9, 12, 14, 15, 16\}$ and $\overline{M} = \{8, 10, 11, 13\}$. For $m \in M \cup \overline{M}$ we define $W_m = \{w_m \in C_{21,i} \mid \mathrm{wt}(w_m) = m\}$. We show in Lemma 7.5 that for all $m \in M$, $(\mathrm{Aut}(C))_{w_m} = H$ where $H \underset{\max}{<} \mathrm{Aut}(C)$ is a maximal subgroup of $\mathrm{Aut}(C)$. In addition for $w_m \in W_m$ we take the image of the support of w_m under the action of $G = \mathrm{Aut}(C)$ to form the blocks of the 2-$(21, m, k_m)$ designs $\mathfrak{D} = \mathcal{D}_{w_m}$, where $k_m = |(w_m)^G| \times \frac{m}{21}$ and show that $\mathrm{Aut}(C)$ acts primitively on $\mathcal{D}_{w_m}$. Information on these designs is given in Table 7.6. Lastly, if $w_m \in W_m$ where $m \in \overline{M}$ we show in Lemma 7.6 that $(\mathrm{Aut}(C))_{w_m}$ is not a maximal subgroup of $\mathrm{Aut}(C)$ for all m.

Lemma 7.5. *Let $m \in M$ and $w_m \in W_m$. Then $(\mathrm{Aut}(C))_{w_m} = H$, where H is a maximal subgroup of $\mathrm{Aut}(C)$. Furthermore $\mathrm{Aut}(C)$ is primitive on $\mathcal{D}_{w_m}$ for each m.*

Proof: Notice from Proposition 7.4 that $\mathrm{Aut}(C) = L_3(4){:}2_2$ or $\mathrm{Aut}(C) = L_3(4){:}S_3$. We consider the following two cases.

Case I. $\mathrm{Aut}(C) = L_3(4){:}2_2$. Since W_m is invariant under the action of $L_3(4){:}2_2$ for all $m \in M$, Tables 7.4 shows that ${w_m}^{L_3(4):2_2} = W_m$. Thus each W_m is a single orbit under the action of $L_3(4){:}2_2$, so that $L_3(4){:}2_2$ is transitive on each W_m. From Table 7.4 and the orbit stabilizer theorem we deduce that $[L_3(4){:}2_2{:}(L_3(4){:}2_2)_{w_m}] \in \{21, 56, 120, 280\}$. Looking at the list of maximal subgroups of $L_3(4){:}2_2$ from the $\mathbb{ATLAS}$ [34] we deduce that $(L_3(4){:}2_2)_{w_m} \in \{2^4{:}A_5, A_6, L_3(2), 3^2{:}Q_8\}$. But by Proposition 7.4 we have that $L_3(4){:}2_2$ acts 2-transitively on the code coordinates, and the codewords of W_m form a 2-design $\mathcal{D}_{w_m}$ with the number of blocks being the indices of $(L_3(4){:}2_2)_{w_m}$ in $L_3(4){:}2_2$ (see Table 7.6 for the parameters of these designs). Hence $L_3(4){:}2_2$ acts primitively on the blocks of $\mathcal{D}_{w_m}$, and thus each $\mathcal{D}_{w_m}$

is primitive.

Case II. $\mathrm{Aut}(C) = L_3(4){:}S_3$. In this case $C = C_{21,1}$ or $C = C_{21,3}$ with $m = 12$ or $m = 16$. For either choices of m we have ${w_m}^{L_3(4):S_3} = W_m$. Thus, W_m is a single orbit of $L_3(4){:}S_3$, and arguing similarly as in CASE I and using the ATLAS [34] we show that $(L_3(4){:}S_3)_{w_m}$ is a maximal subgroup of $L_3(4){:}S_3$ isomorphic to $2^5{:}S_6$. Hence, $L_3(4){:}S_3$ is primitive on the blocks of $D_{w_{12}} = 2\text{-}(21, 12, 88)$ and on $\overline{\mathcal{D}}_{w_{12}} = \mathcal{D}_{w_{16}} = 2\text{-}(21, 16, 12)$, respectively. ■

Lemma 7.6. *Let $m \in \overline{M}$ and $w_m \in W_m$. Then $(\mathrm{Aut}(C))_{w_m}$ is a non-maximal subgroup of* $\mathrm{Aut}(C)$.

Proof: As in Lemma 7.5 we consider two cases for $\mathrm{Aut}(C)$, i.e., $\mathrm{Aut}(C) = L_3(4){:}2_2$ or $\mathrm{Aut}(C) = L_3(4){:}S_3$.

Consider $\mathrm{Aut}(C) = L_3(4){:}S_3$, in which case we have $m = 8$ or $m = 13$. It follows from Table 7.4 that ${w_m}^{L_3(4):S_3} = W_m$ and so $L_3(4){:}S_3$ is transitive on each W_m. From Table 7.4 and the orbit stabilizer theorem we deduce that $[L_3(4){:}S_3{:}(L_3(4){:}S_3)_{w_m}] \in \{210\}$. It follows from the ATLAS [34] that these are not maximal subgroups of $L_3(4){:}2_2$, and hence $\mathcal{D}_{w_m}$ is not primitive. Now, the 2-transitivity of $L_3(4){:}2_2$ on the code coordinates, implies that the codewords of W_m form a 2-design $\mathcal{D}_{w_m}$ with the number of blocks being the indices of $(L_3(4){:}S_3)_{w_m}$ in $L_3(4){:}S_3$. See Table 7.6 for the parameters of these designs.
Now, consider $\mathrm{Aut}(C) = L_3(4){:}2_2$. In this case we have $m = 10$ or $m = 11$. In either cases we deduce that ${w_m}^{L_3(4):2_2} = W_m$ so that $L_3(4){:}2_2$ is transitive on each W_m. Arguing as in Case I we deduce that $[L_3(4){:}2_2{:}(L_3(4){:}2_2)_{w_m}] \in \{336\}$ so that $(L_3(4){:}2_2)_{w_m}$ is not a maximal subgroup of $L_3(4){:}2_2$, and again $\mathcal{D}_{w_m}$ is not primitive. ■

In Table 7.5 the first column gives the codes $C_{21,i}$, the second column represents the codewords of weight m (the sub-indices of m represent the code from where the codeword is drawn), the third column gives the structure of the stabilizers in $\mathrm{Aut}(C)$ of a codeword w_m and the last column, tests the maximality $(\mathrm{Aut}(C))_{w_m}$.

In Table 7.6 the first column represents the codewords of weight m and the second

C	m	$(\mathrm{Aut}(C))_{w_m}$	Maximal	C	m	$(\mathrm{Aut}(C))_{w_m}$	Maximal
$C_{21,3}$	5_3	S_7	Yes	$C_{21,2}$	12_2	$(S_4 \times S_4) : 2$	Yes
$C_{21,2}$	6_2	S_7	Yes	$C_{21,3}$	12_3	$(S_4 \times S_4) : 2$	Yes
$C_{21,4}$	7_4	$S_6 \times 2$	Yes	$C_{21,4}$	12_4	$(S_4 \times S_4) : 2$	Yes
$C_{21,1}$	8_1	$S_6 \times 2$	No	$C_{21,3}$	13_3	$S_5 \times S_3$	No
$C_{21,2}$	8_2	$(S_4 \times S_4) : 2$	No	$C_{21,2}$	14_2	$S_5 \times S_3$	Yes
$C_{21,3}$	8_3	$(S_4 \times S_4) : 2$	No	$C_{21,4}$	15_4	$S_5 \times S_3$	Yes
$C_{21,4}$	8_4	$(S_4 \times S_4) : 2$	No	$C_{21,1}$	16_1	$2^5 : S_6$	Yes
$C_{21,3}$	9_3	$2^5 : S_6$	Yes	$C_{21,2}$	16_2	$(S_4 \times S_4) : 2$	Yes
$C_{21,2}$	10_2	$S_6 \times 2$	No	$C_{21,3}$	16_3	$(S_4 \times S_4) : 2$	Yes
$C_{21,4}$	11_4	$S_6 \times 2$	No	$C_{21,4}$	16_4	$(S_4 \times S_4) : 2$	Yes
$C_{21,1}$	12_1	$(S_4 \times S_4) : 2$	Yes				

Table 7.5: Stabilizer in $\mathrm{Aut}(C)$ of a codeword w_m

column gives the parameters of the 2-designs $\mathcal{D}_{w_m}$ as defined in Subsection 7.7.1. In the third column we list the number of blocks of $\mathcal{D}_{w_m}$, the fourth column gives the number s of elements that are common to pairs of blocks. The last column tests whether or not a design $\mathcal{D}_{w_m}$ is primitive under the action of $\mathrm{Aut}(C)$.

m	$\mathcal{D}_{w_m}$	No. of blocks	s	Prim	m	$\mathcal{D}_{w_m}$	No. of blocks	s	Prim
5_3	2-$(21, 5, 1)$	21	1	Yes	12_2	2-$(21, 12, 88)$	280	4, 6, 8	Yes
6_2	2-$(21, 6, 4)$	56	0, 2	Yes	12_3	2-$(21, 12, 88)$	280	4, 6, 8	Yes
7_4	2-$(21, 7, 12)$	120	1, 3	Yes	12_4	2-$(21, 12, 88)$	280	4, 6, 8	Yes
8_1	2-$(21, 8, 28)$	210	0, 2, 4	No	13_3	2-$(21, 13, 78)$	210	5, 7, 9	No
8_2	2-$(21, 8, 28)$	210	0, 2, 4	No	14_2	2-$(21, 14, 52)$	120	8, 10	Yes
8_3	2-$(21, 8, 28)$	210	0, 2, 4	No	15_4	2-$(21, 15, 28)$	56	9, 11	Yes
8_4	2-$(21, 8, 28)$	210	0, 2, 4	No	16_1	2-$(21, 16, 12)$	21	1	Yes
9_3	2-$(21, 9, 48)$	280	1, 3, 5	Yes	16_2	2-$(21, 16, 12)$	21	1	Yes
10_2	2-$(21, 10, 72)$	336	2, 4, 6	No	16_3	2-$(21, 16, 12)$	21	1	Yes
11_4	2-$(21, 11, 88)$	336	3, 5, 7	No	16_4	2-$(21, 16, 12)$	21	1	Yes
12_1	2-$(21, 12, 88)$	280	4, 6, 8	Yes					

Table 7.6: 2-designs $\mathcal{D}_{w_m}$ invariant under $\mathrm{Aut}(C)$

Remark 7.7. (i) The codes and groups discussed in part (i) of Proposition 7.4 can be described geometrically: with the notation of the proposition, $C_{21,1}$ is a $[21, 9, 8]_2$ code, and its dual ${C_{21,1}}^{\perp}$ is a $[21, 11, 5]_2$ code. The words of weight 5 in ${C_{21,1}}^{\perp}$ form a 2-$(21, 5, 1)$ design $\mathfrak{D}$, of points and lines in the projective geometry $PG_2(4)$; the automorphism group of the design is $L_3(4){\cdot}3 \cdot 2_2 \cong P\Gamma L_3(\mathbb{F}_4)$, by Theorem 4.26. The code of this design $\mathfrak{D}$ is not ${C_{21,1}}^{\perp}$; denoting it by $\mathcal{E}$, it is a $[21, 10, 5]_2$ code inside ${C_{21,1}}^{\perp}$. In fact it can be shown that $\mathcal{E} \cong C_{21,3}$. Thus ${C_{21,1}}^{\perp}$ is a code that is not generated by its minimum weight vectors. The dual $\mathcal{E}^{\perp}$ of $\mathcal{E}$, is a $[21, 11, 6]_2$ containing $C_{21,1}$. The automorphism group of all these designs and codes is $P\Gamma L_3(\mathbb{F}_4)$.

(ii) The code and groups found in part (iii) can also be described geometrically: with the notation of the propositions, $C_{21,3}$ is a $[21, 10, 5]_2$ code, and its dual ${C_{21,1}}^{\perp}$ is a $[21, 11, 6]_2$ code. The words of weight 5 in $C_{21,3}$ form a 2-$(21, 5, 1)$ design $\mathfrak{F}$, of points and lines in the projective geometry Π; the automorphism group of the design is $P\Gamma L_3(\mathbb{F}_4) \cong L_3(4){\cdot}3 \cdot 2_2$, by Theorem 4.26. The 21 words of weight 5 are the incidence vectors of the lines. The code $C_{21,3}$ is in fact a projective Reed-Muller code (see [4, Chapter 5]). The words of weight 6 in ${C_{21,3}}^{\perp}$ can also be described geometrically: these are all the incidence vectors of hyperovals in Π. Moreover, the automorphism group $\mathrm{Aut}(\mathfrak{F})$ of $\mathfrak{F}$ acts transitively on the hyperovals with stabilizer a group of order 720 isomorphic with S_6. Thus $|\mathrm{Aut}(\mathfrak{F})| = 168 \times |S_6|$. Since $\mathfrak{F}$ is isomorphic to Π, it is known that (up to isomorphism) the group $PGL_3(4) \cong L_3(4){\cdot}3$ is contained in $\mathrm{Aut}(\mathfrak{F})$. This group has order 60480 and is of index 2 in $\mathrm{Aut}(\mathfrak{F})$. The extra automorphism is induced by the field automorphism of order 2 of $\mathbb{F}_4$.

The rows of the incidence matrix of the 2-$(21, 5, 1)$ design can be used as orthogonal parity checks that allow majority decoding of the code ${C_{21,1}}^{\perp}$ and $C_{21,3}$ up to its full error-correcting capacity. The following proposition can now be proved

Proposition 7.8. *The codes ${C_{21,1}}^{\perp}$, ${C_{21,2}}^{\perp}$ and $C_{21,3}$ can correct up to 2 errors by majority decoding.*

Proof: By applying the Rudolph's decoding algorithm [107] to the design 2-$(21, 5, 1)$ we obtain that $\left\lfloor \frac{r+\lambda-1}{2\lambda} \right\rfloor = \left\lfloor \frac{5+1-1}{2\times 1} \right\rfloor = 2$, and so the result. ■

Remark: In addition to the above, we also obtain a residual design of $\mathfrak{F}$ with respect to a block, namely a 2-$(16, 4, 1)$ design, denoted $\overline{\mathfrak{F}}$. The design $\overline{\mathfrak{F}}$ is a quasi-symmetric design with 20 blocks and each two distinct blocks intersecting in 0 or 1 point. In fact, $\overline{\mathfrak{F}}$ is an affine resolvable design provided by the family of all hyperplanes in an affine n-dimensional space ($n \geq 2$) over a finite field $\mathbb{F}_q$. The parameters of this design are 2-$\left(q^n,\, q^{n-1},\, \dfrac{q^{n-1}-1}{q-1}\right)$. Substituting $n = 2$ and $q = 4$ in the earlier expression we obtain a design isomorphic to $\overline{\mathfrak{F}}$.

We now examine the properties of this design and those of its binary codes denoted $C_{\overline{\mathfrak{F}}}$ and $C_{\overline{\mathfrak{F}}}{}^{\perp}$ respectively, and prove

Proposition 7.9. (i) $\overline{\mathfrak{F}}$ *is a quasi-symmetric design.*
(ii) $C_{\overline{\mathfrak{F}}}$ *is a self-orthogonal* $[16, 9, 4]_2$ *code and* $\mathbf{1} \in C_{\overline{\mathfrak{F}}}$.
(iii) $C_{\overline{\mathfrak{F}}}{}^{\perp}$ *is a* $[16, 7, 6]_2$ *code with 48 words of weight 6. Moreover* $C_{\overline{\mathfrak{F}}}$, $C_{\overline{\mathfrak{F}}}{}^{\perp}$ *are optimal codes and* $\mathrm{Aut}(\overline{\mathfrak{F}}) = \mathrm{Aut}(C_{\overline{\mathfrak{F}}}) \cong 3^3 : (A_5 \times 2)$.

Proof: Since blocks meet in 0 or 1 point, it is clear that $C_{\overline{\mathfrak{F}}} \subseteq C_{\overline{\mathfrak{F}}}{}^{\perp}$. Also note that the all-one vector $\mathbf{1}$ is in $C_{\overline{\mathfrak{F}}}$ since the sum of all the blocks in a parallel class will give $\mathbf{1}$. From this it follows that any vector in $C_{\overline{\mathfrak{F}}}$ will have weight divisible by 2, and the sum of the non-zero coordinate entries of any word of $C_{\overline{\mathfrak{F}}}{}^{\perp}$ must be 0. The automorphism group of the designs and of the corresponding codes is $3^3 : (A_5 \times 2)$. Since the automorphism group acts 2-transitively on the set of coordinates of these codes, it follows that the support of a codeword of any fixed non-zero weight in the code and its dual yields a 2-design.■

Remark 7.10. (i) It is well-known that the block graph of a quasi-symmetric design is a strongly regular graph (see [110]). It follows then that the block graph of $\overline{\mathfrak{F}}$ is a $(20, 16, 12, 16)$ strongly regular graph and its complement is a $(20, 3, 2, 0)$ graph. These graphs are known as the complete multipartite graph with block size $m(= 4)$ and the disjoint union of $r(= 5)$ complete graphs each on $m(= 4)$ vertices, denoted $r \cdot K_m$ (see [26]).

(ii) The hull $\mathcal{H}$ of $\overline{\mathfrak{F}}$ is an optimal self-orthogonal doubly-even two-weight code with parameters $[16, 5, 8]_2$ and weight enumerator:

$$W_{\mathcal{H}} = 1 + 30x^8 + x^{16}.$$

(iii) The automorphism group of $\mathcal{H}$ is the subgroup of S_{16} (acting on the sixteen code coordinates) which leaves $\mathcal{H}$ invariant. It is the triply transitive affine group of $\mathbb{F}_4$. It now follows from the Assmus-Matson Theorem that the thirty codewords of weight 8 in $\mathcal{H}$ form the blocks of a 3-$(16, 8, 3)$ design. In fact the code $\mathcal{H}$ is isomorphic to the first Reed-Muller code. The dual $\mathcal{H}^\perp$ of $\mathcal{H}$ is the extended binary Hamming code, whose weight distribution is

$$W_{\mathcal{H}^\perp} = 1 + 140x^4 + 448x^6 + 870x^8 + 448x^{10} + 140x^{12} + x^{16}.$$

Based on the parameters of $\mathcal{H}$, we obtain according to [23] a strongly regular graph with parameters $(32, 16, 0, 16)$ whose complement is a $(32, 15, 14, 0)$. As above this graph is the disjoint union of $r(= 2)$ complete graphs each on $m(= 16)$ vertices, denoted $r \cdot K_m$ and the former is the complete multipartite graph with block size m.

The discussion in Section 7.6 and a careful examination of Proposition 7.3 affords us results on non-existence of codes with certain properties. In particular we deduce the following

Proposition 7.11. *Let C be a binary linear code from the permutation module $\mathbb{F}_2\Omega$ of dimension 21 invariant under $L_3(4)$. Then the following holds:*
(a) *Up to isomorphism there are exactly 8 non-trivial codes of length 21 invariant under G.*
(b) *If C is self-orthogonal, then* $\mathrm{Aut}(C) \ncong G$.
(c) *Moreover, there is no C subcode of $\mathbb{F}_2\Omega$ such that* $\mathrm{Aut}(C) = G$.

Proof: Follows from Proposition 7.3 and Proposition 7.4. See also the detailed results given in Section 7.6 which describe the construction of the non-trivial submodules of the permutation module $\mathbb{F}_2\Omega$. ■

In preparation for the next section, note that we have seen in the proof of part (i) of Proposition 7.4 that the group $L_3(4)$ is normal in $P\Gamma L_3(4)$ and has index 6 in

this group. In fact it intersects the stabilizer of a hyperoval in a non-trivial normal subgroup of S_6. Hence this intersection is isomorphic to A_6. Thus $L_3(4)$ has 3 orbits of length $56 = \frac{168}{3}$ on hyperovals.

7.8 A 56-dimensional representation

Consider $\mathcal{A} = PG_2(q)$ be the desarguesian projective plane over $\mathbb{F}_q$. A set Θ of $q+1$ points is called an *oval* if no three points in Θ are collinear. By definition, there is exactly one tangent t of Θ (i.e., a line t with $|\Theta \cap t| = 1$) through every point of Θ. If q is odd, then Θ is maximal, i.e., for every point $p \in \mathcal{A} - \Theta$, the set $\{p\} \cup \Theta$ contains three collinear points. If q is even, then all tangents of Θ meet at a point p, so that the set $\mathcal{V} = \{p\} \cup \Theta$ is also a set in which no three points are collinear. The set $\mathcal{V}$ is generally known as a *hyperoval* in $\mathcal{A}$. Moreover, Π defined earlier, has hyperovals. Each hyperoval $\mathcal{V}$ consists of six points and there are 15 lines meeting $\mathcal{V}$ in two points and six meeting in no points. These six lines form a hyperoval of the dual projective plane. If $\mathcal{Q}$ is a quadrangle in Π, then there is a unique hyperoval through $\mathcal{Q}$ (see [55, 116]). Thus the group $PGL_3(4)$ acts transitively on the set of 168 hyperovals in Π. Following [34], we have that G has three orbits, each of size 56, on the set of hyperovals in Π; and these can be characterized as classes of the equivalence relation

$$\mathcal{V}_1 \sim \mathcal{V}_2 :\Leftrightarrow |\mathcal{V}_1 \cap \mathcal{V}_2| \text{ is even}^1.$$

Now, for a hyperoval $\mathcal{V}$ in Π we have that $G_{\mathcal{V}} \cong A_6$ and $G_{\mathcal{V}}$ is a maximal subgroup of G. From [34] we know that there exists a polarity τ of Π such that $\langle G_{\mathcal{V}}, \tau \rangle \cong M_{10}$, containing only one copy of A_6. Thus, τ maps $\mathcal{V}$ to the dual hyperoval consisting of the six lines passing through $\mathcal{V}$.

As stated above, G acts primitively as a rank-3 group of degree 56 on each of the orbits of A_6 and for each of these three inequivalent representations the orbits have lengths 1, 10 and 45 respectively. From the above discussion it is clear that the elements being permuted under this action are the hyperovals. The

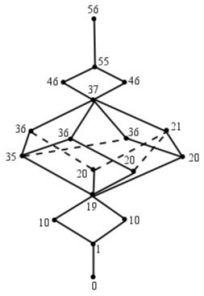
[1] a purely combinatorial proof is given in [116]

permutation module splits into 4 irreducible constituents of dimensions $1, 9, 9$, and 16 with multiplicities $4, 2, 2$, and 1 respectively. The only irreducible submodule in this representation is of dimension 1. The 56-dimensional permutation module has only one maximal submodule of dimension 55. From this submodule we get two non-isomorphic maximal submodules of dimension 46 each. Each of the 46-dimensional submodules contains only one maximal submodule of dimension 37, and these are all isomorphic. Now, from the 37-dimensional module we get four maximal submodules of dimensions 21, 36, 36 and 36. The 36-dimensional submodules are all non-isomorphic. From the 21 dimensional submodule we get three non-isomorphic maximal submodules of dimension 20 each. From each of the 36 dimensional submodule we get two maximal submodules, one of dimension 35 and the other of dimension 20. The three 35-dimensional submodules are isomorphic. However, the three 20-dimensional submodules are all non-isomorphic, although each being isomorphic to a 20-dimensional submodule obtained from the 21-dimensional submodule.

Each of the three 20-dimensional submodules and each of the 35-dimensional submodules contains only one maximal submodule of dimension 19. Moreover, all six 19-dimensional submodules are isomorphic. Furthermore, the 19-dimensional submodule contains two non-isomorphic maximal submodules of dimension 10 and each of these submodules contains a maximal submodule of dimension 1. Thus, we have submodules of dimensions $1, 10, 10, 19, 20, 20, 20, 21, 35, 36, 36, 36, 37, 46$ and 55 respectively. Putting this information together we determine the lattice of submodules as shown in Figure 7.2.

In Table 7.7 below we list only the weight distributions of the non-trivial submodules, namely, those of dimensions $10, 19, 20, 20, 20, 21, 35, 36, 36, 36, 37$ and 46. We note however that the 10-dimensional codes are isomorphic, and so are the second and third 20-dimensional codes (see listing above); and similarly the second and third 36-dimensional ones. We denote the codes and their duals $C_{56,i}$ and $C_{56,i}^{\perp}$ respectively, where $i = 1, \ldots, 5$ and list them in Table 7.7 together with the corresponding weight distributions. Note that $\mathbf{1} \in C_{56,i}$ and in $C_{56,i}^{\perp}$ for all

Figure 7.2: Submodule lattice for a 56-dimensional representation



i and that $\langle \mathbf{1} \rangle$ is an 1-dimensional $L_3(4)$-invariant subspace of $C_{56,i}$ or $C_{56,i}^{\perp}$. Also $A_{56-l} = |\{w_l + \mathbf{1} : w_l \in C_{56,i} \text{ or } C_{56,i}^{\perp}\}| = |\{w_l : w_l \in C_{56,i} \text{ or } C_{56,i}^{\perp}\}| = A_l$ where l represents the weight of a codeword w_l and A_l denotes the number of codewords in $C_{56,i}$ or $C_{56,i}^{\perp}$ of weight l. In Table 7.7 the codes are listed in increasing order of their dimensions.

Our results for the first representation of degree 56 are summarized in Propositions 7.12 and 7.13. From Figure 7.2 and Table 7.7 we can assert the inclusions depicted in Proposition 7.12. We note that $C_{56,1}$ is a subcode of all these codes, while $C_{56,1}^{\perp}$ contains all of them.

Proposition 7.12. (i) $C_{56,1} \subset C_{56,2} \subset C_{56,4} \subset C_{56,5} \subset C_{56,2}^{\perp} \subset C_{56,1}^{\perp}$,
(ii) $C_{56,2} \subset C_{56,4} \subset C_{56,4}^{\perp} \subset C_{56,2}^{\perp}$,
(iii) $C_{56,2} \subset C_{56,3} \subset C_{56,3}^{\perp} \subset C_{56,2}^{\perp}$,
(iv) $C_{56,3} \subset C_{56,5}$,
(v) $C_{56,5} \subset C_{56,5}^{\perp} \subset C_{56,4}^{\perp}$.

Proposition 7.13. (i) $C_{56,1}$ *is self-orthogonal doubly-even with minimum weight* 16. *It is a* $[56, 10, 16]_2$ *code and its dual* $C_{56,1}^{\perp}$ *is a* $[56, 46, 4]_2$ *singly-even and optimal code, and* $\mathrm{Aut}(C_{56,1}) \cong L_3(4){:}2_2$.
(ii) $C_{56,2}$ *is self-orthogonal doubly-even and optimal. It is a* $[56, 19, 16]_2$ *code and its dual* $C_{56,2}^{\perp}$ *is a* $[56, 37, 6]_2$ *singly-even code, and* $\mathrm{Aut}(C_{56,2}) \cong L_3(4){:}2^2$.

Table 7.7: The weight distribution of the codes from a 56-dimensional representation.

		0	4	6	8	10	12	14	16
name	dim	56	52	50	48	46	44	42	40
$C_{56,1}$	10	1							21
$C_{56,2}$	19	1							1722
$C_{56,3}$	20	1				56		120	1722
$C_{56,4}$	20	1							2394
$C_{56,5}$	21	1				56		120	3066
${C_{56,5}}^{\perp}$	35	1			2835	67200	535920	5475840	39911361
${C_{56,4}}^{\perp}$	36	1			2835	322560	1073520	11018880	79736769
${C_{56,3}}^{\perp}$	36	1		336	2835	75824	1046640	10994160	79607745
${C_{56,2}}^{\perp}$	37	1		336	2835	145712	2121840	220802240	159258561
${C_{56,1}}^{\perp}$	46	1	1050	63168	2762235	69577536	1090743780	11336324160	81348170505

	18	20	22	24	26	28
name	38	36	34	32	30	
$C_{56,1}$				210		560
$C_{56,2}$		19936		1304085		212800
$C_{56,3}$	5600	19936	63840	1304085	192528	212800
$C_{56,4}$		46368		251685		447680
$C_{56,5}$	5600	72800	63840	369285	192528	682560
${C_{56,5}}^{\perp}$	201922560	751815232	2034923520	4170444075	6314025984	7321559200
${C_{56,4}}^{\perp}$	403468800	1504254528	4070545920	8339209515	12627659520	14645401760
${C_{56,3}}^{\perp}$	405253520	1497767488	4086220320	8308028715	12677325024	14586831520
${C_{56,2}}^{\perp}$	808346000	3002646080	8157465120	16645559595	25304592096	29234516640
${C_{56,1}}^{\perp}$	414699902400	1534404517254	4184722792320	8505948911355	12981290275968	14938916094200

(iii) $C_{56,3}$ *is a self-orthogonal singly-even and decomposable code. It is a* $[56, 20, 10]_2$ *code and its dual* $C_{56,3}^{\perp}$ *is a* $[56, 36, 6]_2$ *singly-even code, and* $\mathrm{Aut}(C_{56,3}) \cong L_3(4){:}2^2$.
(iv) $C_{56,4}$ *is a self-orthogonal doubly-even and optimal. It is a* $[56, 20, 16]_2$ *code and its dual* $C_{56,4}^{\perp}$ *is* $[56, 36, 8]_2$ *optimal code, and* $\mathrm{Aut}(C_{56,4}) \cong L_3(4){:}2_1$.
(v) $C_{56,5}$ *is self-orthogonal singly-even and decomposable code. It is a* $[56, 21, 10]_2$ *code and its dual* $C_{56,5}^{\perp}$ *is a* $[56, 35, 8]_2$ *singly-even and optimal code, and* $\mathrm{Aut}(C_{56,5}) \cong L_3(4){:}2^2$.

Proof: For the proof of the automorphism group in parts (i) and (iv) we make use of the classification of the primitive groups of degree 56. Since $G \subseteq \mathrm{Aut}(C_{56,1})$ and G is primitive it follows that $\mathrm{Aut}(C_{56,1})$ is primitive. By the classification of primitive groups of degree 56 we have that $\mathrm{Aut}(C_{56,1})$ is one of $A_8, S_8, L_3(4), L_3(4){:}2_1, L_3(4){:}2_2, L_3(4){:}2_3, L_3(4){:}2^2, A_{56}$, or S_{56} (see [105]). However, since $C_{56,1}$ is $L_3(4)$-invariant, we have that all but $L_3(4), L_3(4){:}2_1, L_3(4){:}2_2, L_3(4){:}2_3, L_3(4){:}2^2$ can be excluded from the list. Furthermore, since by Magma we have $|\mathrm{Aut}(C_{56,1})| = 2 \times |L_3(4)| = |L_3(4){:}2|$ it follows that $\mathrm{Aut}(C_{56,1}) = L_3(4){:}2$, and so $\mathrm{Aut}(C_{56,1})$ is one of $L_3(4){:}2_1, L_3(4){:}2_2$ or $L_3(4){:}2_3$. Moreover, considerations of type of elements of the conjugacy classes distinguishes the groups, and we deduce that $\mathrm{Aut}(C_{56,1}) \cong L_3(4){:}2_2$. Similarly, we deduce that $\mathrm{Aut}(C_{56,4}) \cong L_3(4){:}2_1$, since $\mathrm{Aut}(C_{56,4})$ has no elements of order 14.

For parts (ii), (iii) and (v) notice that if we choose a G-orbit of hyperovals as vertices and define two hyperovals to be adjacent if and only if they are disjoint, we obtain a strongly regular $(56, 10, 0, 2)$ graph Λ isomorphic to the Gerwitz graph. In fact, the edges of Λ are the unitals of Π (see Section 7.10). In [16, 15] the reader will find other geometric constructions of Λ. It is shown in [16] that the automorphism group of Λ is $L_3(4){:}2^2$, which is G extended by a polarity and a Baer involution (see Section 7.9). The code of Λ is denoted $C_{56,3}$ in Table 7.7. Since $\mathrm{Aut}(\Lambda) \subseteq \mathrm{Aut}(C_{56,3})$ and $|\mathrm{Aut}(\Lambda)| = |\mathrm{Aut}(C_{56,3})|$ we have $\mathrm{Aut}(C_{56,3}) \cong L_3(4){:}2^2$. The 2-rank 20 of $C_{56,3}$ follows readily from [16] or [18, item 10, p. 342]. Now, since the non-zero codewords of weight divisible by four in $C_{56,3}$ form a self-orthogonal doubly-even subcode of codimension 1, with parameters $[56, 19, 16]_2$ this code must

be $C_{56,2}$. Since $|\mathrm{Aut}(C_{56,2})| = |\mathrm{Aut}(C_{56,3})|$ the rest follows. Also, we have that $C_{56,3}$ is a subcode of codimension 1 in $C_{56,5}$ spanned by the words of weight 10. By considerations of inclusions of the codes as given in Proposition 7.12 and the order of the groups we deduce that $\mathrm{Aut}(C_{56,5}) \cong L_3(4){:}2^2$.

We now give a reason for the self-orthogonality of all non-trivial codes obtained from this representation. For any choice of $C_{56,i}$, $i = 1, \ldots, 5$, note that with the exception of $C_{56,5}$ all other codes are spanned by their minimum weight codewords. $C_{56,5}$ is spanned by the words of weight 16, the code spanned by the words of weight 10 is a subcode of $C_{56,5}$ isomorphic to $C_{56,1}$. Now, we take the images of the support of the words of minimum weight for each of the first four cases, and the support of the words of weight 16 for $C_{56,5}$ under the corresponding automorphism groups we can form the blocks of a design 1-$(56, k, \lambda)$ design $\mathcal{D}$ where k =16, 16, 10, 16, 16, and λ =6, 492, 10, 684, 876, with $21, 1722, 56, 2394$ and 3066 blocks respectively. Now, if $i \neq j$ consider B_i and B_j two distinct blocks in each $\mathcal{D}$. Since $|B_i \cap B_j| = \{0, 2, 4, 6, 8\} \equiv 0 \pmod 2$ and $k \in \{10, 16\} \equiv 0 \pmod 2$, we have that $\mathcal{D}$ is a self-orthogonal design in each case, and hence the code $C_{56,i}$ spanned by the point-block incidence matrix of $\mathcal{D}$ is self-orthogonal. ■

As an immediate consequence of Proposition 7.13 and the results given in Section 7.8 we deduce the following result.

Proposition 7.14. *Up to isomorphism there are exactly 10 non-trivial codes of length 56 invariant under $L_3(4)$. There is no self-orthogonal $[56, k, d]_2$ code C such that $\mathrm{Aut}(C) \cong L_3(4)$, and no code C of length 56 such that $\mathrm{Aut}(C) \cong L_3(4)$. Furthermore, there is no $L_3(4)$-invariant self-dual code C of length 56.*

Remark 7.15. (i) The code $C_{56,3}$ can be described geometrically: $L_3(4){:}2^2$ fixes the 56 codewords of weight 10 into a single orbit with stabilizer isomorphic to $A_6 \cdot 2^2$. The codewords of weight 10 are in fact the rows of the adjacency matrix of the graph Λ. The codewords of weight 14 form the 120 subgraphs isomorphic to the Heawood graph on 14 vertices (i.e., the point-line incidence graph of the Fano plane), and those of weight 42 form the complement, namely the co-Heawood graph on 42 vertices (i.e., the point-line non-incidence graph of the Fano plane, see [16, Section 7]). These

form a single orbit, and the stabilizer of one is $L_2(7){:}2 \times 2$ with vertex orbit sizes $7 + 7 + 42$ (see Table 7.2, for the orbit splitting). Their presence shows the M_{24} construction of the Gewirtz graph (see [16, Section 5]). Further, notice that the 336 codewords of weight 6 in $C_{56,3}^{\perp}$ represent the extended bipartite doubles of the Petersen graph (also known as Desargues graph, see [16, Section 7]). They form a single orbit, with the stabilizer of one isomorphic to $S_5 \times 2$ and vertex orbit sizes $6 + 20 + 30$ (see Table 7.2). This shows the presence of the Higman-Sims graph (for more details, see [16]). The graph Λ alluded to in the proofs of parts (ii), (iii) and (v) of Proposition 7.13 also occurs as the block graph of the quasi-symmetric 2-$(21, 6, 4)$ design or of its complementary quasi-symmetric 2-$(21, 15, 28)$ design given in Table 7.6.

(ii) Now, if we take the adjacency matrix of Λ and adjoin to it the identity matrix I we obtain $A+I$. Each row and column of $A+I$ contains exactly 11 non-zero entries. Two rows or columns that correspond to non-adjacent vertices of Λ have exactly two common non-zero entries, corresponding to the two common neighbours of those vertices, and two rows or columns corresponding to adjacent vertices of Λ also have two common non-zero entries, corresponding to themselves and each other. Thus $A + I$ is the incidence matrix of a symmetric 2-design, with parameters 2-$(56, 11, 2)$. A symmetric design with $\lambda = 2$ is called a biplane. Taking the row span over $\mathbb{F}_2$ of $A + I$ we construct a self-dual doubly-even $[112, 56, 12]_2$ code invariant under G.

7.9 A 120-dimensional representation

An involution $\tau \in P\Gamma L_3(q^2) - PGL_3(q^2)$ is called a *Baer involution*. The set of fixed points and lines of τ forms a subplane of $\mathcal{A} = PG_2(q^2)$ isomorphic to $PG_2(q)$, known as a *Baer subplane* of $\mathcal{A}$. If K denotes the group $L_3(q^2)$, then $K_{\mathcal{S}} \cong L_3(q)$ for a Baer subplane $\mathcal{S}$ (here $K_{\mathcal{S}}$ is the stabilizer of $\mathcal{S}$ in K). As in the previous section, if $\mathcal{Q}$ is taken to be a quadrangle of $\mathcal{A}$, then there exists a unique Baer subplane through $\mathcal{Q}$ and so, $PGL_3(q^2)$ acts transitively on the set of all Baer subplanes. Moreover, if $\mathcal{Q}$ is a quadrangle in Π, then a construction of Baer subplanes using $\mathcal{Q}$ is given in

[56] or [116]. Also, the set of all 360 Baer subplanes in Π splits into three orbits of size 120 each, under the action of G (see [68]). From [68], or [116] we have that the orbits can be characterized as classes of the following equivalence relation:

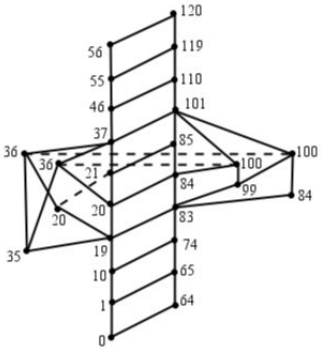
$$\mathcal{S}_1 \sim \mathcal{S}_2 :\Leftrightarrow |\mathcal{S}_1 \cap \mathcal{S}_2| \text{ is odd.}$$

If we take for $\mathcal{J}$, one of these equivalence classes, then it is shown in [56] using results of [115] that there are exactly 42 members of $\mathcal{J}$ intersecting a given subplane $\mathcal{S} \in \mathcal{J}$ in a single point, 21 intersecting $\mathcal{S}$ in three collinear points and 56 intersecting in a triangle. Now, from [34], it follows that there exits a unitary polarity $\tau \in \Pi$ such that $\langle G_{\mathcal{S}}, \tau \rangle \cong PGL_2(7)$. In addition, $G_{\mathcal{S}}$ has four orbits of lengths $1, 21, 42$ and 56 respectively (see Table 7.2 for the splitting of orbits) on the vertices of the unique strongly regular graph Γ whose vertices are the Baer subplanes of Π in an orbit of G and in which two vertices are adjacent if and only if two subplanes intersect in a point. It is clear from the discussion that the elements being permuted by the group are the Baer subplanes in Π. The permutation module splits into five irreducible constituents of dimensions $1, 9, 9, 16$ and 64 with multiplicities $4, 2, 2, 1$ and 1 respectively with the 16-dimensional constituent not absolutely irreducible. There are two irreducible submodules in this representation, one with dimension 1 and the other of dimension 64. Both irreducible submodules are absolutely irreducible. The permutation module contains two maximal submodules of dimension 56 and 119. From the 119-dimensional submodule we obtain two maximal submodules of dimension 110 and 55; and from the 56-dimensional submodule we obtain one maximal submodule of dimension 55. Continuing in a manner similar to that described in Sections 7.6 and 7.8 for the 21 and 56-dimensional permutation modules, for the 120-dimensional representation we determined submodules of dimensions $1, 10, 19, 20, 20, 21, 35, 36, 36, 37, 46, 55, 56, 64, 65, 74, 83, 84, 84, 85, 99, 100, 101, 110, 119,$ and 120.

The lattice of submodules is as shown in Figure 7.3.

In all, we determined 24 non-trivial codes of length 120 which are invariant under G. Due to computer time limitations, we do not calculate the weight distributions of the codes of dimension larger than 37. In Table 7.8 we list the codes and duals

Figure 7.3: Lattice of submodules for a 120-dimensional representation



whose weight distributions we are able to calculate. These codes and respective duals are denoted $C_{120,i}$ and $C_{120,i}^{\perp}$, for $i = 1, \ldots, 9$. Where we are unable to calculate the full weight distribution we give the codes's parameters, the total number of codewords of minimum weight and check whether or not the all-ones vector is present in the code. The remaining three codes and their duals denoted $C_{120,i}$ and $C_{120,i}^{\perp}$, with $i = 10, 11, 12$ are given with parameters $[n, k, d, w]_2$ where w represents the number of codewords of minimum weight d in each case. Hence, we have the codes $C_{120,10} = [120, 46, 12, 210]_2$, $C_{120,11} = [120, 55, 12, 840]_2, C_{120,12} = [120, 56, 12, 840]_2$, and $C_{120,10}^{\perp} = [120, 74, 8, 180]_2$, $C_{120,11}^{\perp} = [120, 65, 8, 240]_2$ and $C_{120,12}^{\perp} = [120, 64, 8, 240]_2$. Moreover $\mathbf{1} \in C_{120,i}$ and $\mathbf{1} \in {C_{120,i}}^{\perp}$ for all i except for $i = 12$. Furthermore $\langle \mathbf{1} \rangle$ is an 1-dimensional $L_3(4)$-invariant subspace of $C_{120,i}$, and $\mathbf{1} \in C_{120,i}$ if $i \neq 12$ and so $A_{120-l} = |\{w_l + \mathbf{1} : w_l \in C_{120,i} \text{ or } w_l \in {C_{120,i}}^{\perp}\}| = |\{w_l : w_l \in C_{120,i} \text{ or } w_l \in {C_{120,i}}^{\perp}\}| = A_l$, where l represents the weight of a codeword $w_l \in C_{120,i\neq 12}$ and A_l denotes the number of codewords in $C_{120,i}$ of weight l. Further, we can assert from the Tables below that several of the codes of length 120 are decomposable. In particular, for $i = 12$ we have $C_{120,12} \oplus C_{120,12}^{\perp} = \mathbb{F}_2^{120}$, i.e., $\mathbb{F}_2^{120}$ is a decomposable code. Since the dimension of the hull is zero, we have $\text{Hull}(C_{120,12}) = \varnothing$, thus we obtain $C_{120,12} \oplus C_{120,12}^{\perp} = \mathbb{F}_2^{120}$ as claimed.

In Table 7.9 below, we give a partial listing of the weight distribution for the dual codes presented in Table 7.8. The complete weight distribution can be obtained from the authors.

Table 7.8: The weight distribution of the codes from a 120-dimensional representation.

		0	16	24	28	30	32	34	36	38	40	42	44
name	dim	120	104	96	92	90	88	86	84	82	80	78	76
$C_{120,1}$	10	1									21		
$C_{120,2}$	19	1					105		280		42		1680
$C_{120,3}$	20	1					105		400		714		3360
$C_{120,4}$	20	1				56	105		280		42	680	1680
$C_{120,5}$	21	1				56	105		520		1386	680	5040
$C_{120,6}$	35	1	315	3150	23040	20160	11865	342720	710080	1189440	6434106	20811840	62830320
$C_{120,7}$	36	1	315	3150	23040	20160	11865	342720	821920	2103360	11288634	4184000	133598640
$C_{120,8}$	36	1	315	3150	23040	20888	11865	408240	1106560	3186960	13761594	43723400	130151280
$C_{120,9}$	37	1	315	3150	23040	20888	11865	408240	1330240	5014800	23470650	85667720	271687920

	46	48	50	52	54	56	58	60
name	74	72	70	68	66	64	62	60
$C_{120,1}$						210		560
$C_{120,2}$		5040		68040		130620		112672
$C_{120,3}$		11760		136080		241500		260736
$C_{120,4}$	5880	5040	22848	68040	100800	130620	131880	112672
$C_{120,5}$	5880	184800	22848	136080		241500		260736
$C_{120,6}$	187104960	463324575	952747200	1744740480	2737465920	3826108740	4656697920	5038604704
$C_{120,7}$	380708160	929719455	1906772160	3466246560	5442400320	7653889860	9338629440	10102749216
$C_{120,8}$	369985560	904237215	1906483056	3486383040	5525084880	7659941700	9330976200	9968498848
$C_{120,9}$	75719160	1837026975	3814532976	6929395200	10934953680	15315503940	18694839240	20096787872

Table 7.9: Partial listing of the weight distribution for the duals of the codes in Table 7.8.

		0	4	6	8	10	12	14	...
name	dim	120	116	114	112	110	108	106	...
$C_{120,9}{}^{\perp}$	83	1			4440	30240	1311520	28177920	
$C_{120,8}{}^{\perp}$	84	1		560	4440	82488	2474080	57317880	
$C_{120,7}{}^{\perp}$	84	1			9480	70560	2479680	57016320	
$C_{120,6}{}^{\perp}$	85	1		560	14520	163128	4810400	114994680	
$C_{120,5}{}^{\perp}$	99	1		16800	857355	112336224	10053237040	638318369760	
$C_{120,4}{}^{\perp}$	100	1		24080	1779915	224871024	20102311600	1276679233200	
$C_{120,3}{}^{\perp}$	100	1		23520	1646475	222368160	20101205040	1276741020960	
$C_{120,2}{}^{\perp}$	101	1		37520	3358155	444934896	40198247600	2553524535600	
$C_{120,1}{}^{\perp}$	110	1	19530	7152320	1640747475	226691803968	20591594667700	1307448287929920	

Remark: (i) Consider $\mathcal{J}$ as above to be an orbit of a subplane of G in Π, then a strongly regular $(120, 42, 8, 18)$ graph Γ can be constructed as follows: the vertices of

Γ are the members of $\mathcal{J}$ and two subplanes $\mathcal{S}$ and $\mathcal{S}'$ are adjacent if and only if their intersection contains a single point. A construction of this graph using a Steiner system $S(4, 7, 23)$ can be found in [18, pp. 343] and from there the connection with the M^{c}Laughlin graph is evident. It has been proven in [43, Theorem 1] that any such graph is uniquely determined by its parameters. The automorphism group of Γ is a group isomorphic to $L_3(4){:}2^2$. In Table 7.8 the code of Γ is labeled $C_{120,4}$. Self-orthogonality of $C_{120,4}$ follows readily from [62, Proposition 3.2(v)], and the 2-rank 20, follows from [18, item 15, p. 343]. The code ${C_{120,4}}^{\perp}$ has minimum distance 6, which coincides with the known record distance for a code of the given length and dimension. Similar to Section 7.8, a geometrical significance for the code $C_{120,4}$ in terms of the graph Γ can be given. More details on the code $C_{120,4}$ and its connection with the M^{c}Laughlin graph can be found in [85]
(ii) The graph Γ described in item (i) occurs also as the block graph of the quasi-symmetric 2-$(21, 7, 12)$ design or of its complementary quasi-symmetric 2-$(21, 14, 52)$ design given in Table 7.6.

A result similar to those described in Propositions 7.11 and 7.14 is also obtained for the codes of the representation of degree 120. We thus state

Proposition 7.16. *Up to isomorphism there are exactly 24 non-trivial codes of length 120 invariant under G. There is no self-orthogonal $[120, k, d]_2$ code C such that $\mathrm{Aut}(C) \cong G$, and no code C of length 120 such that $\mathrm{Aut}(C) \cong G$. Furthermore, there is no G-invariant self-dual code C of length 120.*

7.10 The 280-dimensional representation

As in Section 7.9, now consider $\mathcal{A} = PG_2(q^2)$ be the desarguesian plane over $\mathbb{F}_{q^2}$ and let $\mathcal{T}$ to be a set of $q^3 + 1$ points of P such that $\mathcal{T}$ does not contain a full line. If every line meets $\mathcal{T}$ either in one or $q + 1$ points, then $\mathcal{T}$ is called a *unital* in $\mathcal{A}$ and $\mathcal{T}$ together with the lines meeting it in $q + 1$ points form a $S(2, q + 1, q^3 + 1)$ Steiner system. Moreover, if $\mathcal{T}$ is a unital in Π, then $\mathcal{T}$ is also an $S(2, 3, 9)$ unital and hence isomorphic to $AG_2(3)$ (see [55, Section 3]). Now $G_{\mathcal{T}} \cong 3^2{:}Q_8$ (where Q_8

represents the quaternion group of order 8) and $G_{\mathcal{T}}$ is a maximal subgroup of G with orbits of lengths $1, 9, 18, 18, 18, 72, 72$, and 72 respectively (see Table 7.2 for the orbit splitting). The elements being permuted are the unitals of Π. The 280-dimensional permutation module splits into five irreducible constituents of dimensions $1, 9, 9, 16$ and 64 with multiplicities $10, 7, 7, 5$ and 1 respectively. The permutation module has four irreducible submodules of dimension $1, 9, 9$ and 64 all of which are absolutely irreducible.

Remark 7.17. (i) The complete list of $L_3(4)$-invariant subcodes of the permutation module $\mathbb{F}_2\Omega$ of length 280 consists of 32844 codes whose dimensions k are as follows:

k	#	k	#	k	#	k	#
0	1	61	26	98	19	125	775
1	1	62	14	99	257	126	1619
9	2	64	3	100	525	127	713
10	2	65	7	101	215	128	65
18	1	66	2	102	14	129	7
19	7	69	11	103	1	130	2
20	7	70	61	104	63	133	11
21	1	71	137	105	651	134	77
25	2	72	33	106	1395	135	293
26	2	73	4	107	652	136	337
34	5	74	2	108	140	137	92
35	47	78	6	109	702	138	6
36	35	79	90	110	1417		
37	5	80	304	111	651		
44	14	81	156	112	63		
45	50	82	17	113	1		
46	22	83	7	114	15		
50	1	84	7	115	217		
51	7	85	1	116	497		
52	7	87	1	117	213		
53	3	88	63	118	47		
54	33	89	715	119	85		
55	85	90	1607	120	33		
56	33	91	749	121	2		
57	2	92	69	123	1		
60	6	93	1	124	75		

Table 7.10: Number of codes of length 280 invariant under $L_3(4)$

The number of submodules of dimension $280 - k$ is equal to the number of those of dimension k.

(ii) The 32844 codes (including duals) described in Table 7.10 are only claimed to be distinct and not necessarily inequivalent. We have checked isomorphism up to dimension 37. In general distinct G-invariant codes are inequivalent. In

particular, if C and $\mathcal{C}$ are two equivalent codes (i.e., there exists $\sigma \in S_{280}$ with $\sigma(C) = \mathcal{C}$) for which $\mathrm{Aut}(C) = \mathrm{Aut}(\mathcal{C}) = G$, then it follows that $C = \mathcal{C}$. In fact, $\mathrm{Aut}(\mathcal{C}) = \sigma\mathrm{Aut}(C)\sigma^{-1} = \mathrm{Aut}(C) = G$, which implies that $\sigma \in N_{S_{280}}(G)$. But, since G is equal to its normalizer we deduce that $\sigma \in G$, and so $C = \mathcal{C}$.
(iii) Due to computer time limitations, for the 280-dimensional representation we determined the weight distributions of the codes up to dimension 37. Thus, we present a partial enumeration on the codes obtainable from this representation. In Tables 7.11, 7.12, 7.13 and 7.14 we list the codes which do not contain the all-one vector, and in Tables 7.15 and 7.16 we list those that contain the all-one vector; finally in Table 7.17 we give a partial list of the weight distribution of the corresponding duals.

We note that as the degree of the permutation module increases the lattice of submodules becomes very complex. We present our computations of the submodules up to the fourth layer. The diagram below depicts a partial view of the lattice diagram, yet demonstrating how complex it can get. We illustrate the complexity by layers, moving downwards in the lattice tree.
First layer: The 280-dimensional permutation module has four maximal submodules of dimensions $216, 271(2)$ and 279. The submodules of dimension 271 are non-isomorphic.
Second layer: From the maximal submodule of dimension 216 we obtain three non-isomorphic maximal submodules of which two are of dimension 207 and one is of dimension 215. Each of the 271-dimensional submodules produces four maximal submodules and these are of dimensions $207, 255, 262$ and 270. The 207-dimensional submodule is isomorphic to an earlier submodule gotten from the module of dimension 216. Further, the 262-dimensional submodules are all isomorphic. From the 279-dimensional submodule, we get three non-isomorphic maximal submodules, two of which are of dimension 270 and one of dimension 215. The submodules of dimension 270 are respectively isomorphic to the submodules we got from the module of dimension 271. In this layer we obtain in total eight non-isomorphic submodules, whose dimensions are $207(2), 215, 255(2), 262$ and $270(2)$.

Third layer: From each of the submodules of dimension 207 we get three non-isomorphic maximal submodules of dimensions $191, 198$, and 206, respectively. From the 215-dimensional submodule we get two non-isomorphic submodules of dimension 206. These are isomorphic to the maximal submodule of this dimension obtained earlier from the maximal submodules of dimension 207. Each of the submodules of dimension 255 produces three maximal submodules, which are of dimensions $191, 246$ and 254, and the 262-dimensional produces thirteen maximal submodules, ten of which are non-isomorphic. These submodules are of dimensions 246(6) and 261(7). Finally, each of the submodules of dimension 270 produces three maximal submodules, whose dimensions are $206, 254$ and 261. Therefore we have in total nineteen non-isomorphic submodules with dimensions 191(2), 198, 206(2), 246(5), 254(2) and 261(7).

Fourth layer: The pattern of maximal submodules in the fourth layer is as follows: From each of the 191-dimensional modules we get two maximal submodules of dimensions 182 and 190, and from the 198-dimensional submodule we obtain twelve maximal submodules, five of these of dimension 180 and seven of dimension 197. Each of the 206-dimensional modules produces two maximal submodules, namely of dimensions 190 and 197. Moreover, from each of the five 246-dimensional submodules we obtain nine maximal submodules, of which seven are of dimension 245, one of dimension 182 and another of dimension 230. Each of the 254-dimensional submodules give eight maximal submodules, seven of which are of dimension 245 and one has dimension 190, and lastly each of the seven 261-dimensional submodules produces nine maximal submodules. Five of these submodules are of dimension 245, three are of dimension 260, and one has dimension 197. Upon filtering isomorphic copies we get a total of sixty-seven non-isomorphic submodules in the fourth layer with dimensions, and total number of submodules of that dimension given in brackets, as follows: $182(5), 190(2), 197(7), 230, 245(48), 260(7)$. The partial lattice diagram given below is complete up to the third layer, as it would be be impossible to draw the complete diagram. Moreover, doing so would not clearly convey any meaningful information. The non-isomorphism relations can be deduced from the diagram.

Figure 7.4: Partial lattice of submodules for the 280-dimensional representation

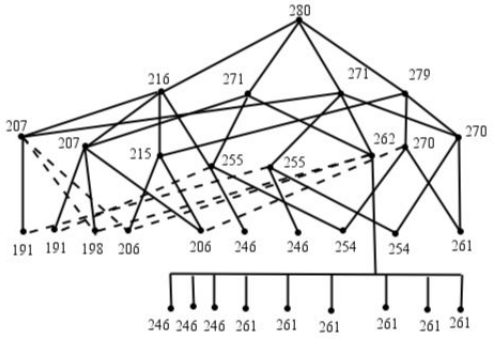


Table 7.11: The weight distribution of the codes from the 280-dimensional representation.

name	dim	60	64	80	84	88	92	96	100	104	108	112
$C_{280,1}$	9											
$C_{280,3}$	18											2940
$C_{280,5}$	19								672			2940
$C_{280,6}$	19				120				56		560	2940
$C_{280,8}$	20				120				1400		560	2940
$C_{280,9}$	20				360				168		1680	2940
$C_{280,11}$	25		315					7875		30240		8640
$C_{280,13}$	34		315			30240		34755		866880	1572480	13794090
$C_{280,14}$	34		1575	13356		120960				5775840		40069380
$C_{280,16}$	35		315	630		30240		34755	130872	1048320	3606960	23941290
$C_{280,17}$	35		1575	41580	5040	127680	312480	1290240	576912	8557920	8994720	60557700
$C_{280,18}$	35		1575	13356		120960		860160	4368	5775840	3247440	40069380
$C_{280,20}$	35		1575	13356	120	120960		860160	55496	5937120	1988000	51721860
$C_{280,21}$	35		315	630	120	30240		34755	202496	987840	3562160	23905770
$C_{280,22}$	35	336	1575	13356	80160	120960	226800	860160	2188592	5775840	108475920	315245952

Table 7.12: Table 7.11 continued

name	116	120	124	128	132	136	140	144	148
$C_{280,1}$						280		210	
$C_{280,3}$		5376		18900		109760		93100	
$C_{280,5}$	2520	5376	6720	18900	74760	109760	97776	93100	62160
$C_{280,6}$		5376	16800	18900	62160	109760	97776	93100	74760
$C_{280,8}$	5040	5376	30240	18900	211680	109760	293328	93100	199080
$C_{280,9}$		5376	50400	18900	186480	109760	293328	93100	224280
$C_{280,11}$	161280	409920	846720	1941660	3548160	7110880	6223104	5960640	3548160
$C_{280,13}$	43706880	197812944	498758400	1284712695	1879879680	3156413120	3005111808	3192870730	1876492800
$C_{280,14}$	0	315245952		2312824815		6019684160		5742112180	
$C_{280,16}$	99509760	373398480	1082356800	2371014135	4054418760	5865231680	6599193120	5885977930	4053678720
$C_{280,17}$	52262280	471496704	472167360	3463557615	2152878840	9024142400	3305232576	8592877300	2029184640
$C_{280,18}$	118404720	315245952	1072513680	2312824815	4054948800	6019684160	6571471248	5742112180	4297181280
$C_{280,20}$	57697920	516222336	542132640	3470472495	2029184640	8870449280	3305232576	8746570420	2152878840
$C_{280,21}$	99678600	372441552	1080690240	2378110455	4057065600	5849520320	6599193120	5901689290	4051031880
$C_{280,22}$	15221360	40069380	935899440	2312824815	4297181280	6019684160	6571471248	5742112180	4054948800

Table 7.13: Table 7.12 continued.

name	152	156	160	164	168	172	176	180	184	188
$C_{280,1}$			21							
$C_{280,3}$	20160		11802							
$C_{280,5}$	20160	16800	11802			560		56		
$C_{280,6}$	20160	6720	11802	2520				672		
$C_{280,8}$	20160	40320	11802	2520		1120		784		
$C_{280,9}$	20160	20160	11802	7560				2016		
$C_{280,11}$	2217600	846720	465717	161280	60480		5040			
$C_{280,13}$	1262620800	502145280	205513266	42255360	12458880	1814400	897750	95760		
$C_{280,14}$	2315093760		403119360		24699360		248220			
$C_{280,16}$	2356018560	1084077120	380141874	98227080	22570560	3804080	1018710	202496	95760	8925
$C_{280,17}$	3472741440	542132640	604095744	57697920	36351840	1988000	409500	55496		
$C_{280,18}$	2315093760	935899440	403119360	108475920	24699360	15221360	248220	2188592		226800
$C_{280,20}$	3465826560	472167360	559370112	52262280	45187680	8994720	3030300	576912	430080	312480
$C_{280,21}$	2348922240	1085743680	381098802	98058240	22606080	3848880	1079190	130872	95760	
$C_{280,22}$	2315093760	1072513680	403119360	118404720	24699360	3247440	248220	4368		

Table 7.14: Table 7.13 continued.

name	192	196	200	204	216	220	224
$C_{280,1}$							
$C_{280,3}$	105						
$C_{280,5}$	105						
$C_{280,6}$	105						
$C_{280,8}$	105	240					
$C_{280,9}$	105						
$C_{280,11}$							
$C_{280,13}$							315
$C_{280,14}$	105						
$C_{280,16}$	120						315
$C_{280,17}$	105	120					
$C_{280,18}$		80160		5040			
$C_{280,20}$	6825	5040	28224				
$C_{280,21}$	8925						315
$C_{280,22}$	105						

Table 7.15: The weight distribution of the codes from the 280-dimensional representation containing the all-one vector.

name	dim	0 280	56 224	60 220	64 216	76 214	80 200	84 196	88 192	92 188	96 184	100 180	104 186	108 172
$C_{280,2}$	10	1												
$C_{280,4}$	19	1							105					
$C_{280,7}$	20	1						120	105			728		560
$C_{280,10}$	21	1						360	105			2184		1680
$C_{280,12}$	26	1			315						7875		35280	
$C_{280,15}$	35	1	315		315		630		39165		130515		1764630	3386880
$C_{280,19}$	35	1			1575		13356		121065		860160		6024060	
$C_{280,23}$	36	1		1575			41580	5160	127785	312480	1290240	632408	8967420	10982720
$C_{280,24}$	36	1	315		315		630	120	39165		130515	333368	2067030	7411040
$C_{280,25}$	36	1		336	1575	5040	13356	80160	121065	226800	860160	2192960	6024060	18468800
$C_{280,26}$	37	1		336	1575	5040	69804	90480	134505	851760	1720320	3457776	11910780	40434240
$C_{280,27}$	37	1	315		315		630	360	39165		130515	1000104	2671830	15459360

Table 7.16: Table 7.15 continued.

	112	116	120	124	128	132	136	140
name	168	164	160	156	152	148	144	140
$C_{280,2}$			21				490	
$C_{280,4}$	2940		17178		39060		202860	
$C_{280,7}$	2940	2520	17178	23520	39060	136920	202860	195552
$C_{280,10}$	2940	7560	17178	70560	39060	410760	202860	586656
$C_{280,12}$	69120	322560	875637	1693440	4159260	7096320	13071520	12446208
$C_{280,15}$	26252970	85962240	403326210	1000903680	2547333495	3756372480	6349283850	6010223616
$C_{280,19}$	64768740		718365312		4627918575		11761796340	
$C_{280,23}$	96909540	109960200	1075592448	1014300000	6936299055	4182063480	17617019700	6610465152
$C_{280,24}$	46511850	197736840	753540354	2166433920	4727032695	8108097480	11751209610	13198386240
$C_{280,25}$	64768740	226880640	718365312	2008413120	4627918575	8352130080	11761796340	13142942496
$C_{280,26}$	129050340	446801040	1432819584	4037013120	9244679535	16716257040	23472243060	26363872800
$C_{280,27}$	87029610	421286040	1453968642	4497494400	9086431095	16811547480	22555061130	27574711488

A careful examination of the properties of the codes tabulated in Tables 7.10, 7.11, 7.12, 7.13, 7.14, 7.15, 7.16 and Table 7.17 from the 280-dimensional representation allow us to establish non-existence results on codes with certain properties. For example it emerges immediately that there is no self-orthogonal G-invariant code whose automorphism group is precisely G. In particular using Table 7.10 we obtain that there is no self-dual G-invariant code of length 280.

Proposition 7.18. *Let G be the linear group $L_3(4)$ and Ω a primitive G-set. Let C be a linear code over $\mathbb{F}_2$ obtained from the 2-modular primitive representation as an $\mathbb{F}_2G$-submodule of the permutation module $\mathbb{F}_2\Omega$ of dimension 280 admitting G as an automorphism group. The following occurs:*
(i) $\mathrm{Aut}(C) \ncong G$.
(ii) *If C is self-orthogonal, then* $\mathrm{Aut}(C) \ncong G$.
(iii) *There is no G-invariant self-dual code C of length 280.*

By determining all G-invariant submodules, the distinct codes of lengths 21, 56, 120 and 280 respectively are known, and as a result we conclude that there is no $L_3(4)$-invariant binary code whose full automorphism is $L_3(4)$. Thus we state

Theorem 7.19. *The simple group $L_3(4)$ is not realizable as the full automorphism group of a binary linear code.*

Table 7.17: A partial listing of the weight distribution of the dual codes from the 280-dimensional representation.

		0	3	4	5	6	7	8	...
name	dim	280	277	276	275	274	273	272	...
$C_{280,27}{}^{\perp}$	243	1						520695	
$C_{280,26}{}^{\perp}$	243	1		630		47040		2791215	
$C_{280,25}{}^{\perp}$	244	1		630		47040	88574400	3288639375	
$C_{280,24}{}^{\perp}$	244	1				3360		681975	
$C_{280,23}{}^{\perp}$	244	1		630		47040		2791215	
$C_{280,22}{}^{\perp}$	245	1		630	8064	47040	345600	2932335	
$C_{280,21}{}^{\perp}$	245	1				3360	6720	681975	
$C_{280,20}{}^{\perp}$	245	1		630		47040	17280	2791215	
$C_{280,19}{}^{\perp}$	245	1		630		47040		2932335	
$C_{280,18}{}^{\perp}$	245	1		630		47040		2932335	
$C_{280,17}{}^{\perp}$	245	1		630	8064	47040	328320	2791215	
$C_{280,16}{}^{\perp}$	245	1				3360		681975	
$C_{280,15}{}^{\perp}$	245	1				10080		1004535	
$C_{280,14}{}^{\perp}$	246	1		630	8064	47040	345600	2932335	
$C_{280,13}{}^{\perp}$	246	1				10080	6720	1004535	
$C_{280,12}{}^{\perp}$	254	1		2520		245280		77874615	
$C_{280,11}{}^{\perp}$	255	1		2520	20160	245280	4307520	77874615	
$C_{280,10}{}^{\perp}$	259	1		6930		1706880		934878735	
$C_{280,9}{}^{\perp}$	260	1		6930	20160	1706880	29367360	934878735	
$C_{280,8}{}^{\perp}$	260	1		6930	8064	1706880	19735680	934878735	
$C_{280,7}{}^{\perp}$	260	1		6930		2049600		2049600	
$C_{280,6}{}^{\perp}$	261	1		6930	28224	2049600	49103040	1719465615	
$C_{280,5}{}^{\perp}$	261	1		6930	16128	2049600	39471360	1719465615	
$C_{280,4}{}^{\perp}$	261	1		6930		2735040		3288639375	
$C_{280,3}{}^{\perp}$	262	1		6930		2735040		3288639375	
$C_{280,2}{}^{\perp}$	270	1		494970		1238354880		1654446113775	
$C_{280,1}{}^{\perp}$	271	1	6720	494970	27042624	1238354880	48481451520	1654446113775	

Proof: The proof follows from Propositions 7.11, 7.14, 7.16 and 7.18. ■

7.11 Binary codes from $\mathrm{Aut}(L_3(4))$

In this section we deal with some codes obtained from the automorphism group of $L_3(4)$. The full automorphism group of $L_3(4)$ is $L_3(4){:}D_{12}$ which we shall denote by $\mathrm{Aut}(L_3(4))$. It has order 241920 and 8 conjugacy classes of maximal subgroups, and hence 8 primitive permutation representations, and these have degrees 2, 2, 2, 3, 105, 280, 336 and 960 respectively. These primitive representations are shown in Table 7.18: the first column gives the ordering of the primitive representations as given by Magma (or the ATLAS) and as used in our computations; the second gives

the degree (the number of cosets of the point stabilizer); the third gives the maximal subgroups; the fourth gives the number of orbits, and the remaining columns give the length of the orbits of the point-stabilizer. We shall examine the irreducible binary codes and designs from these representations.

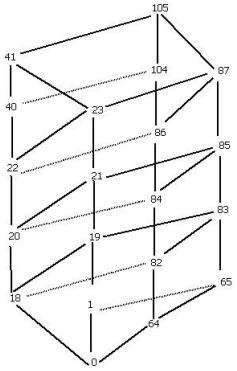
no	Degree	Max Subgroup	no. of orbits	orbit length
1	2	120960	2	$1, 1$
2	2	120960	2	$1, 1$
3	2	120960	2	$1, 1$
4	3	80640	2	$1, 2$
5	105	2304	4	$1, 18, 32, 64$
6	280	864	5	$1, 9, 54, 72, 144$
7	336	720	6	$1, 20, 30, 45, 120(2)$
8	960	252	10	$1, 14, 21, 84, 84, 126(4), 252$

Table 7.18: Maximal subgroups of $\mathrm{Aut}(L_3(4))$.

7.12 The 105-dimensional primitive permutation representation

In this section we give a brief account on the codes obtained from the permutation representation of degree 105. The permutation module of degree 105 splits into three absolutely irreducible constituents of dimensions 1, 2, 18 and 64 with multiplicities of 1, 2, 2 and 1 respectively. There are only three irreducible submodules of dimension 1,18 and 64. The permutation module obtained from the action of $L_3(4) \cdot D_{12}$ has three maximal submodules of dimension 41, 87 and 104. By working recursively through the submodules structure of the modules given above we obtain maximal submodules of dimensions 1, 18, 19, 20, 21, 22, 23, 40, 64, 65, 82 83, 84, 85, 86, 87 and 104. The full lattice of submodules is as shown in Figure 7.5. Notice from these that we obtain fourteen non-trivial

Figure 7.5: Lattice of submodules for a 105-dimensional representation



submodules of dimension 18, 19, 20, 21, 22, 23, 40, 64, 65, 82 83, 84, 85, 86, 87 that give in turn the following 14 binary codes viz: $[105, 18, 32]_2$, $[105, 19, 25]_2$, $[105, 20, 28]_2$, $[105, 21, 25]_2$, $[105, 22, 30]_2$, $[105, 40, 8]_2$, $[105, 41, 5]_2$, $[105, 64, 6]_2$, $[105, 65, 6]_2$, $[105, 83, 6]_2$, $[105, 84, 6]_2$, $[105, 85, 5]_2$, $[105, 86, 6]_2$, $[105, 87, 5]_2$. The automorphism group of all these codes is $L_3(4){:}D_{12}$.

7.13 Binary codes related to the strongly regular $(105, 32, 4, 12)$ graph

It has recently been proven in [37, Theorem 3] that all strongly regular graphs with parameters $(105, 32, 4, 12)$ are isomorphic. Later in [43, Theorem 1] the authors showed that any such graph is uniquely determined by its parameters. A graph with these parameters can be constructed from the second subconstituent of the McLaughlin graph, that is, the unique strongly regular graph with parameters $(162, 56, 10, 24)$, as follows: the 162 vertices form a single orbit. The vertex stabilizer in that graph is $L_3(4){:}2^2$ with vertex orbit sizes 1, 56 and 105. The orbit of size 56 induces a Gewirtz graph. On the other hand the orbits of size 105 are the flags of $PG_2(4)$, where two flags (x, R) and (y, S) are adjacent when x, y are distinct and R, S are distinct, and x is on S or y on R. The induced subgraph is strongly regular with parameters $(105, 32, 4, 12)$, spectrum $\{[32]^1, [2]^{84}, [-10]^{20}\}$ and eigenvalues 32, 2, -10 with multiplicities 1, 84 and 20 respectively. That the resulting graph is isomorphic

with the graph in discussion follows from [37, Theorem 3]. In [85] a study was carried of the binary code of this graph. We quote these results and look further at the action of the automorphism group on the codewords as well as determine the stabilizers of this action.

Lemma 7.20. *$C_{\Gamma_{105}}$ is a $[105, 18, 32]_2$ self-orthogonal doubly-even code, and its dual $C_{\Gamma_{105}}^{\perp}$ is a $[105, 87, 5]_2$ with 336 words of weight 5. Moreover* $\mathrm{Aut}(\Gamma_{105}) = \mathrm{Aut}(C_{\Gamma_{105}}) \cong L_3(4){\cdot}D_{12}$.

Proof: See [85]. ■

Table 1: The weight distribution of $C_{\Gamma_{105}}$

m	A_m	m	A_m
0	1	56	52500
32	105	60	40880
40	6636	64	3360
44	11760	72	280
48	69300	80	42
52	77280		

7.13.1 Designs held by the support of codewords in $C_{\Gamma_{105}}$

Suppose that w_m is a codeword of non-zero weight m in $C_{\Gamma_{105}}$. In this section we determine the structures of $(L_3(4){:}D_{12})_{w_m}$, that is the stabilizers of w_m in $L_3(4){:}D_{12}$. The structures of these stabilizers are listed in Table 2. In addition for each w_m we take image of the support of w_m under the action of $G = L_3(4){:}D_{12}$ to form the blocks of the $1-(105, m, k_m)$ designs $\mathcal{D}_{w_m}$, where $k_m = |(w_m)^G| \times \frac{m}{105}$. Information on these designs is given in Table 3.

7.13.2 Stabilizer in $L_3(4){:}D_{12}$ of a word w_m in $C_{\Gamma_{105}}$

We now examine the action of $\mathrm{Aut}(C_{\Gamma_{105}}) = L_3(4){:}D_{12}$ on the set of non-zero codewords of $C_{\Gamma_{105}}$ and describe their nature. In addition we look at the structure

of the stabilizers $(L_3(4){:}D_{12})_{w_m}$ where $m \in M$ or $m \in \overline{M}$ with M, $\overline{M}$ as follows.

Consider $M = \{32, 72\}$ and $\overline{M} = \{40, 44, 48, 52, 56, 60, 64, 80\}$. For $m \in M \cup \overline{M}$ we define $W_m = \{w_m \in C_{\Gamma_{105}} \mid \mathrm{wt}(w_m) = m\}$. We show in Lemma 7.21 if $m \in M$ then $(L_3(4){:}D_{12})_{w_m} = K$ where $K \underset{\max}{\leq} L_3(4){:}D_{12}$, is a maximal subgroup of $L_3(4){:}D_{12}$. In addition, for $w_m \in W_m$ we determine the image under $L_3(4){:}D_{12}$ of the support of w_m and form the blocks of a 1-design $\mathcal{D}_{w_m}$ and show that for $m \in M$, $L_3(4){:}D_{12}$ acts primitively on $\mathcal{D}_{w_m}$.

Subsequently if $w_m \in W_m$ and $m \in \overline{M}$ we show in Lemma 7.22 that $(L_3(4){:}D_{12})_{w_m}$ is not a maximal subgroup of $L_3(4){:}D_{12}$ for all m except when $m = 40$. In particular, for $m = 40$, W_{40} splits into four orbits namely $W_{(40)_1}$, $W_{(40)_2}$, $W_{(40)_3}$ and $W_{(40)_4}$ of lengths 336, 420, 2520, and 3360 respectively. If $w_m \in W_{(40)_1}$ we show that $(L_3(4){:}D_{12})_{w_m}$ is a maximal subgroup of $L_3(4){:}D_{12}$ isomorphic to $S_3 \times S_5$, and that in all the remaining cases $(L_3(4){:}D_{12})_{w_m}$ is not maximal. Table 2 presents a detailed structure description of these groups.

Lemma 7.21. *Let $m \in M$ and $w_m \in W_m$. Then $(L_3(4){:}D_{12})_{w_m} = K$, where K is a maximal subgroup of $L_3(4){:}D_{12}$. Moreover $L_3(4){:}D_{12}$ is primitive on $\mathcal{D}_{w_m}$ for each m.*

Proof: Notice from Lemma 7.20 that $\mathrm{Aut}(C_{\Gamma_{105}}) = L_3(4){:}D_{12}$. Since W_m is invariant under the action of $\mathrm{Aut}(C_{\Gamma_{105}})$ for all $m \in M$, Table 1 implies that ${w_m}^{(L_3(4):D_{12})} = W_m$, for all $m \in M$. Therefore each W_m is a single orbit under the action of $L_3(4){:}D_{12}$ and thus $L_3(4){:}D_{12}$ is transitive on each W_m. Using Table 1 and the orbit stabilizer theorem we deduce that $[(L_3(4){:}D_{12}){:}(L_3(4){:}D_{12})_{w_m}] \in \{105, 280\}$, and so we have $(L_3(4){:}D_{12})_{w_m} \in \{2^{2+4} \cdot 3^2 \cdot 2^2,\ 3^2{:}2S_4 \times 2\}$. Now by the $\mathbb{ATLAS}$ [34] we have that these stabilizers are maximal subgroups of $L_3(4){:}D_{12}$. Since $L_3(4){:}D_{12}$ is transitive on the code coordinates, the codewords of W_m form a 1-design $\mathcal{D}_{w_m}$ with A_m blocks (the number of blocks are the indices of $(L_3(4){:}D_{12})_{w_m}$ in $L_3(4){:}D_{12}$). This implies that $L_3(4){:}D_{12}$ is transitive on the blocks of D_{w_m} for each w_m and since $(L_3(4){:}D_{12})_{w_m}$ is a maximal subgroup of $L_3(4){:}D_{12}$ for $m \in M$, we deduce that $L_3(4){:}D_{12}$ acts primitively on $\mathcal{D}_{w_m}$. See Table 2 and Table 3. ■

Lemma 7.22. *Let $m \in \overline{M}$ and $w_m \in W_m$. If $m \neq 40$ then $(L_3(4){:}D_{12})_{w_m}$ is not a maximal subgroup of $L_3(4){:}D_{12}$. If $m = 40$ then $(L_3(4){:}D_{12})_{w_m} \cong S_3 \times S_5$, $2^4 : (S_3 \times S_3)$, $Q_8 : D_{12}$ or $3^2 : 2^3$, where $S_3 \times S_5$ is a maximal subgroup of $L_3(4){:}D_{12}$.*

Proof: Suppose that $m = 40$. Then W_{40} splits into four orbits namely $W_{(40)_1}$, $W_{(40)_2}$, $W_{(40)_3}$ and $W_{(40)_4}$ of lengths 336, 420, 2520, and 3360 respectively. Let $a = w_{(40)_1} \in W_{(40)_1}$, $b = w_{(40)_2} \in W_{(40)_2}$, $c = w_{(40)_3} \in W_{(40)_3}$, and $d = w_{(40)_4} \in W_{(40)_4}$. Then $(L_3(4){:}D_{12})_a$ is a subgroup of order 720 and from the list of maximal subgroups of $L_3(4){:}D_{12}$ (see $\mathbb{ATLAS}$ [34]) we deduce that $(L_3(4){:}D_{12})_a \cong S_3 \times S_5$. Here $\mathcal{D}_a$ is a 1-$(105, 40, 128)$ design having 336 blocks, and $L_3(4){:}D_{12}$ acts primitively on $\mathcal{D}_a$. Now, $(L_3(4){:}D_{12})_b$, $(L_3(4){:}D_{12})_c$, and $(L_3(4){:}D_{12})_d$ are subgroups of orders 576, 96, and 72 respectively. Thus these subgroups are not maximal. Direct calculations show that $(L_3(4){:}D_{12})_b \cong 2^4 : (S_3 \times S_3)$, $(L_3(4){:}D_{12})_c \cong Q_8 : D_{12}$ and $(L_3(4){:}D_{12})_d \cong 3^2 : 2^3$.

A case-by-case analysis shows that if $m \neq 40$, then $(L_3(4){:}D_{12})_{w_m}$ is not a maximal subgroup of $L_3(4){:}D_{12}$. The details describing the structure of $(L_3(4){:}D_{12})_{w_m}$ are listed in Table 2 and Table 3. ■

In Table 2 the first column represents the codewords of weight m (the sub-indices on the codewords indicates the number of orbits of W_m for a codeword of weight m under the action of $L_3(4){:}D_{12}$), and the second column gives the structure of the stabilizers in $L_3(4){:}D_{12}$ of a codeword w_m. The last column, tests the maximality $(L_3(4){:}D_{12})_{w_m}$.

Table 2: Stabilizer of a word w_m

m	$(L_3(4) \cdot D_{12})_{w_m}$	Maximality	m	$(L_3(4) \cdot D_{12})_{w_m}$	Maximality
32	$2^{10}{:}M_{22}{:}2$	Yes	$(52)_3$	D_6	No
$(40)_1$	$S_3 \times S_5$	Yes	$(56)_1$	$2^4 : (S_3 \times S_3)$	No
$(40)_2$	$2^4 : (S_3 \times S_3)$	No	$(56)_2$	$S_4 \times S_3$	No
$(40)_3$	$Q_8 : D_{12}$	No	$(56)_3$	$2 \times S_4$	No
$(40)_4$	$3^2 : 2^3$	No	$(56)_4$	D_{24}	No
$(44)_1$	$Q_8 : D_6$	No	$(56)_5$	D_{16}	No
$(44)_2$	$3^2 : 2^2$	No	$(56)_6$	D_{12}	No
$(48)_1$	$8 \cdot 2^3$	No	$(60)_1$	$AGL(2, 3)$	No
$(48)_2$	$2 \times S_4$	No	$(60)_2$	D_{12}	No
$(48)_3$	D_{12}	No	$(60)_3$	D_{12}	No
$(48)_4$	D_{12}	No	64	$(6 \times 2) : S_3$	No
$(48)_5$	D_{12}	No	72	$3^2{:}2S_4 \times 2$	Yes
$(52)_1$	$3^2 : 2^2$	No	80	$(2^4 : A_5) : S_3$	No
$(52)_2$	D_8	No			

In Table 3 the first column represents the codewords of weight m and the second column gives the parameters of the 1-designs $\mathcal{D}_{w_m}$ as defined in Subsection 7.13.1. In the third column we list the number of blocks of $\mathcal{D}_{w_m}$. The final column shows whether or not a design $\mathcal{D}_{w_m}$ is primitive under the action of $L_3(4) \cdot D_{12}$.

Table 3: 1-designs $\mathcal{D}_{w_m}$ from $L_3(4){:}D_{12}$

m	$\mathcal{D}_{w_m}$	No. of blocks	Prim	m	$\mathcal{D}_{w_m}$	No. of blocks	Prim
32	1-$(105, 32, 32)$	105	Yes	$(52)_3$	1-$(105, 52, 19968)$	40320	No
$(40)_1$	1-$(105, 40, 128)$	336	Yes	$(56)_1$	1-$(105, 56, 224)$	420	No
$(40)_2$	1-$(105, 40, 160)$	420	No	$(56)_2$	1-$(105, 56, 896)$	1680	No
$(40)_3$	1-$(105, 40, 960)$	2520	No	$(56)_3$	1-$(105, 56, 2688)$	5040	No
$(40)_4$	1-$(105, 40, 1280)$	3360	No	$(56)_4$	1-$(105, 56, 5376)$	10080	No
$(44)_1$	1-$(105, 44, 2112)$	5040	No	$(56)_5$	1-$(105, 56, 8064)$	15120	No
$(44)_2$	1-$(105, 44, 2816)$	6720	No	$(56)_6$	1-$(105, 56, 10752)$	20160	No
$(48)_1$	1-$(105, 48, 1728)$	3780	No	$(60)_1$	1-$(105, 60, 320)$	560	No
$(48)_2$	1-$(105, 48, 2304)$	5040	No	$(60)_2$	1-$(105, 60, 11520)$	20160	No
$(48)_3$	1-$(105, 48, 9216)$	20160	No	$(60)_3$	1-$(105, 60, 11520)$	20160	No
$(48)_4$	1-$(105, 48, 9216)$	20160	No	64	1-$(105, 64, 2048)$	3360	No
$(48)_5$	1-$(105, 48, 9216)$	20160	No	72	1-$(105, 72, 192)$	280	Yes
$(52)_1$	1-$(105, 52, 3328)$	6720	No	80	1-$(105, 80, 32)$	42	No
$(52)_2$	1-$(105, 52, 14976)$	30240	No				

Remark: 1. The words of minimum weight 32 in $C_{\Gamma_{105}}$ have a geometric description, i.e., they are the rows of the adjacency matrix of Γ_{105}. Under the action of $\mathrm{Aut}(C_{\Gamma_{105}})$ the set of codewords of weight 32 form a single orbit. Viewing $L_3(4)$ as the Mathieu group M_{21} we have that the words of weight 32 correspond to points in the action of the stabilizer. Thus the stabilizer of a point is a maximal subgroups of $L_3(4){:}D_{12}$ of order 2304 isomorphic to $2^{2+4} \cdot 3^2 \cdot 2^2$. The transitivity of the automorphism group gives rise to a primitive 1-$(105, 32, 32)$ design whose binary code is $C_{\Gamma_{105}}$. This shows that the set of points under the action of $L_3(4){:}D_{12}$ spans the code.

Remark: 2. The words of weight 5 in $C^{\perp}_{\Gamma_{105}}$ forms a single orbit under $L_3(4) \cdot D_{12}$, with stabilizer of a codeword being a maximal subgroup of $L_3(4){:}D_{12}$ of type $S_3 \times S_5$. The support of a codeword of weight 5 in $C_{\Gamma_{105}}$ holds a 1-$(105, 5, 16)$ design $\mathcal{T}$ with 336 blocks whose code is not $C^{\perp}_{\Gamma_{105}}$. The code of $\mathcal{T}$ is a $[105, 83, 5]_2$, say $\mathcal{L}$ with 336 codewords of weight 5, which is a subcode of $C^{\perp}_{\Gamma_{105}}$. The dual $\mathcal{L}^{\perp}$ of $\mathcal{L}$ is a $[105, 22, 28]_2$ with 360 codewords of weight 28 and whose hull is $C_{\Gamma_{105}}$. The words of weight 28 in $\mathcal{L}$ span a self-orthogonal doubly-even subcode $[105, 20, 28]_2$.

Chapter 8

2-modular codes of the group A_8

8.1 Introduction

In Section 6.3.2 we described a method to investigate all non-trivial codes from the primitive 2-modular permutation representations of certain finite simple groups. In Chapter 7, using a chain of maximal submodules of a permutation module induced by the action of the simple linear group $L_3(4)$ on objects like lines, hyperovals, Baer subplanes and unitals of $\mathrm{PG}(2,4)$ we obtained most of the non-trivial binary codes invariant under the group. However, it is well known, see for example [34, 51], that there are two non-isomorphic simple groups of order 20160, respectively $L_3(4)$ and the alternating group A_8. It seems thus natural to ask for the codes invariant under A_8 and their weight distribution. Moreover, the isomorphism $A_8 \cong L_4(2) \cong \Omega^+(6,2)$ adds a rich geometrical structure that can be used to explore the connections with objects such as combinatorial designs, graphs, groups and irreducible modules.

In this chapter, in a manner similar to that in Section 7 we consider the primitive representations of A_8, as described, for example, in [34]. Using Meat-Axe and Magma [27], we determine the irreducible constituents of the primitive 2-modular permutation representations and from these we determine the dimensions and constituents of all submodules of each of the subspaces. The incidences between the constituents are determined and used to describe the nature of the codewords of

several weights. In addition, we used the Atlas of Brauer characters [70] to determine the irreducibility of the codes and the MacWilliams identities relating the weight enumerators of the dual codes. Unlike in Chapter 7, in this chapter we are able to determine and enumerate all submodules, and hence all non-trivial binary codes invariant under A_8 and prove the following main result:

Theorem 8.1. *Let G be the alternating group A_8 and Ω be a primitive G-set. Then up to equivalence there are exactly 52 non-trivial binary codes obtained from the 2-modular primitive representations of G as $\mathbb{F}_2G$-submodules of the permutation module $\mathbb{F}_2\Omega$ and admitting G as an automorphism group. The sets of non-trivial codewords of several of these codes constitute single orbits of the automorphism groups that are stabilized by maximal subgroups. Moreover, there is no A_8 and S_8-invariant self-orthogonal $[56, k, d]_2$ code C with $k = 10, 19, 20, 20, 21$ and $d = 16, 16, 10, 16, 10$, and no self-dual codes of lengths 28 and 56 invariant under A_8 and S_8.*

8.2 The primitive permutation representations of A_8

We consider G to be A_8, the alternating group on eight letters, ie, the subgroup consisting of all even permutations of the symmetric group S_8, which is of order 20160, and its maximal subgroups and primitive permutation representations via the coset action on these subgroups [34]. There are 6 primitive permutation representations of degrees 8, 15, 15, 28, 35 and 56 respectively (see [34]). We use the $\mathbb{ATLAS}$ notation for the names of the geometric objects on which A_8 acts, namely points, Steiner $S(3, 4, 8)$ systems, duads, bisections and triads. These representations are depicted in Table 9.1: the first column gives the ordering of the primitive representations as given by Magma (or the $\mathbb{ATLAS}$) and as used in our computations; the second gives the maximal subgroups; the third gives the degree (the number of cosets of the point stabilizer).

We summarize the information obtained from the group and find notations for

No.	Max. sub.	Deg.
1	A_7	8
2	$2^3 : L_3(2)$	15
3	$2^3 : L_3(2)$	15
4	S_6	28
5	$2^4 : (S_3 \times S_3)$	35
6	$(A_5 \times 3) : 2$	56

Table 8.1: Maximal subgroups of A_8

the objects which are permuted in each of its primitive permutation representations. The primitive representations may also be described (often in several ways, see for example the $\mathbb{ATLAS}$[34]) in terms of the action of G on various sets of geometrical objects: we shall use the notations $g(m)(m = 8, 15a, 15b, 28, 35, 56)$ to denote these sets. We will use names for all objects in terms of their alternating notation from [34], namely point, $S(3, 4, 8)$, duad, bisection and triad.

8.3 Incidence relations

The action of a group fixing an element of $g(m)$ may be transitive on the elements of $g(n)$ or may split these elements into several orbits or into two orbits if $m \neq n$, of which one has size one if $m = n$. The rows and columns of Table 8.2 represent the intersections of objects being permuted as named above. Denoting the entries as a_{mn}, the entry a_{42} corresponds to the transitive action of S_6 on 2^3:$L_3(2)$. The entry a_{64} indicates that there are 3 orbits of an intransitive action of $(A_5 \times 3)$:2 on S_6. The sizes of the orbits of the remaining actions are illustrated in Table 8.2.

	n					
m	8	15a	15b	28	35	56
8	1 - 7	15	15	7 - 21	35	21 - 35
15a	8	1 - 14	7 - 8	28	7 - 28	56
15b	8	7 - 8	1 - 14	28	7 - 28	56
28	2 - 6	15	15	1 - 12 - 15	15 - 20	6 - 20 - 30
35	8	3 - 12	3 - 12	12 - 16	1 - 16 - 18	8 - 48
56	3 - 5	15	15	3 - 10 - 15	5 - 30	1 - 10 - 15 - 30

Table 8.2: Orbits of $g(m)$ on $g(n)$.

8.4 The 2-modular representations of A_8

Each conjugacy class of maximal subgroups of A_8 generates a permutation module over $\mathbb{F}_2$. We shall consider these $\mathbb{F}_2$-modules, and a chain of all their invariant maximal submodules under the action of A_8. Each maximal submodule constitutes in turn the binary code that is invariant under A_8. After eliminating isomorphic copies, we obtain a lattice of submodules. In this way, we classify and enumerate all submodules, hence codes invariant under A_8. Taking the submodules as the working modules, its corresponding maximal submodules are found recursively. The recursion terminates as soon as we reach an irreducible maximal submodule or a maximal submodule of dimension 1. In so doing we determine all codes associated with the permutation module of a given dimension and invariant under the group. Our construction is based on a method outlined in [29] and in Chapter 6. The sections that follow present the calculations on these modules. The vectors in each submodule form a code, over $\mathbb{F}_2$, whose length is the dimension of the permutation module and whose dimension is the dimension of the submodule. The weight enumerators of the submodules are therefore also the weight enumerators of these codes which are invariant under the action of A_8. Observe that the rank-2 representations of this group are pairwise equivalent under an outer automorphism (see Table 9.1 and [34]), and thus their submodules (resp. codes) are isomorphic (resp. equivalent). In this case we only consider the submodules (resp. codes) obtained from the first representation of that degree.

8.5 The 8-dimensional representation

In its natural representation on a set $\Omega = \{1, 2, \ldots, 8\}$ the group A_8 has for point stabilizer A_7 which has two orbits of lengths 1 and 7 respectively. Using the ATLAS [34], we notice that the constituents being permuted by the group are the 8 symbols (points) of the set Ω. The permutation module splits into two absolutely irreducible constituents of dimensions 1 and 6 with multiplicities 2 and 1 respectively. There are only two irreducible maximal submodules of dimension 1 and 7. The permutation module has therefore just one composition series, and the lattice of submodules is as shown in Figure 8.1.

Figure 8.1: Submodule lattice for the 8-dimensional representation

It is evident that the codes of this representation are the trivial codes of length 8.

8.6 A 15-dimensional representation

Notice from Table 8.2 (see also Table 9.1) that there are two non-conjugate classes of maximal subgroups of A_8 of index 15 when G acts on the cosets of $2^3 : L_3(2)$. Under this action $2^3 : L_3(2)$ has two orbits, one of length 1 and another of length 14. Using this action and taking for m either $15a$ or $15b$ we form a 15-dimensional permutation module invariant under G. From the ATLAS [34] we observe that the constituents being permuted by the group in these representations are Steiner $S(3, 4, 8)$ systems. The permutation module splits into four absolutely irreducible constituents of dimensions 1, 4, 4, and 6. There are only two irreducible submodules, one of dimension 1 and the other of dimension 4. These submodules are absolutely

irreducible. By recursively determining a chain of maximal submodules of the permutation module (see [29]) we find that the permutation module has two maximal submodules of dimensions 11 and 14. From the 11-dimensional module we obtain two maximal submodules one of dimension 5 and the other of dimension 10. From the 14-dimensional module we get only one maximal submodule which is of dimension 10. This submodule is isomorphic to the submodule of dimension 10 obtained earlier from the 11-dimensional maximal submodule. The 10-dimensional submodule contains an irreducible maximal submodule of dimension 4, and the 5-dimensional submodule contains two irreducible maximal submodules, one of dimensions 1 and the other of dimension 4 respectively. We found that the 4-dimensional submodules are all isomorphic and irreducible. In all, from this permutation module we obtain four non-trivial submodules invariant under A_8 of dimensions 11, 10, 5 and 4. The lattice of the submodules is as given in Figure 8.2.

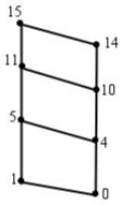


Figure 8.2: Submodule lattice for a 15-dimensional representation

Form the submodules described above we derive four non-trivial codes, namely $[15, 4, 8]_2$, $[15, 11, 3]_2$, $[15, 5, 7]_2$, and $[15, 10, 4]_2$. We denote the codes (resp. duals) as $C_{15,i}$ ($C_{15,i}{}^{\perp}$) where $i = 1, 2$ and list them in Table 8.3.

Name	dim	0	3	4	5	6	7	8	9	10	11	12	15
$C_{15,1}$	4	1						15					
$C_{15,2}$	5	1					15	15					1
$C_{15,2}{}^{\perp}$	10	1		105		280		435		168		35	
$C_{15,1}{}^{\perp}$	11	1	35	105	168	280	435	435	280	168	105	35	1

Table 8.3: Weight distributions of the codes from a 15-dimensional representation.

From Table 8.3 we deduce some obvious properties of the codes which we examine with certain detail in Proposition 8.2.

Proposition 8.2. (i) *The code* $C_{15,1} = [15, 4, 8]_2$ *is self-orthogonal doubly-even, and its dual is a* $[15, 11, 3]_2$ *code.* $\mathrm{Aut}(C_{15,1}) \cong A_8$, *and* A_8 *acts irreducibly on* $C_{15,1}$ *as an* $\mathbf{F}_2$*-module.*
(ii) *The code* $C_{15,2} = [15, 5, 7]_2$ *is self-complementary, and its dual* $[15, 10, 4]_2$ *is singly-even. Moreover,* $\mathrm{Aut}(C_{15,2}) \cong A_8$, *and* $C_{15,1}$, $C_{15,2}$, *and their duals are optimal codes.*

Proof: By construction we have that the code $C_{15,1}$ is a 4-dimensional code of length 15 and invariant under A_8, so $A_8 \subseteq \mathrm{Aut}(C_{15,1})$, this also follows since A_8 acts 2-transitively on the set of code coordinates. So $\mathrm{Aut}(C_{15,1})$ is a primitive permutation group of degree 15. Excluding the natural action, the primitive groups of degree 15, are $A_6, A_6{\cdot}2_1, A_7, S_7, A_8$ and S_8, see [52, p. 324]. From $A_8 \subseteq \mathrm{Aut}(C_{15,1})$, we eliminate all but A_8 and S_8 possibilities from the previous list. Moreover, direct calculations show that $C_{15,1}$ is not S_8-invariant, and since $|A_8| = |\mathrm{Aut}(C_{15,1})|$, the result follows. Now, from $C_{15,1} \subseteq {C_{15,1}}^{\perp}$ we deduce that $C_{15,1}$ is self-orthogonal. In addition, it can be observed from Table 8.3 that $C_{15,1}$ has precisely 15 non-zero vectors, and the zero vector. Also, note that the non-zero vectors (codewords) have weight divisible by four, hence $C_{15,1}$ is doubly-even. From [70] we have that 4 is the smallest dimension for any non-trivial irreducible $\mathbb{F}_2$-invariant module under A_8 and this gives yet another illustration of the isomorphism between A_8 and $L_4(2)$. Further, $C_{15,2}$ is the code obtained from $C_{15,1}$ by adjoining to it the all-ones vector $\mathbf{1}$, so if $\alpha \in \mathrm{Aut}(C_{15,1})$ then since $\alpha(\mathbf{1}) = \mathbf{1}$ and $C_{15,2} = \langle C_{15,1}, \mathbf{1} \rangle$, we have $\alpha \in \mathrm{Aut}(C_{15,2})$, and thus $\mathrm{Aut}(C_{15,1}) \subseteq \mathrm{Aut}(C_{15,2})$. Now $|\mathrm{Aut}(C_{15,1})| = |\mathrm{Aut}(C_{15,2})|$ gives $\mathrm{Aut}(C_{15,2}) = A_8$. The optimality of the codes can be verified from [17] or [59]. ■

Remark 8.3. The codes and groups found in Proposition 8.2 can be described geometrically: viewing A_8 as $L_4(2)$, notice that the action is that of $L_4(2)$ on the points of $\mathrm{PG}(3, 2)$. The codewords of weight 8 in $C_{15,1}$ form a single orbit under the automorphism group, with stabilizer isomorphic to $2^3{:}L_3(2)$, the affine subgroup of $GL_4(2)$. Taking the image of this orbit under the automorphism group we obtain a 2-$(15, 8, 4)$ design, which is the complement of the design of points and planes in $\mathrm{PG}(3, 2)$. By Theorem 4.26, the automorphism group of the design is $L_4(2)$. Since

this design is self-orthogonal, it follows that its point-block incidence matrix spans a self-orthogonal code. In addition, the codes are spanned by their minimum weight codewords, so the assertion on the automorphism group follows as ${C_{15,1}}^{\perp}$ is the well-known Hamming code of length 15. A geometric significance of the codewords of non-zero weight could also be given for the remaining codes.

8.7 The 28-dimensional representation

Recall from Theorem 2.34 that the alternating group A_n where $n \geq 5$ acts as a rank-3 group of degree $\binom{n}{2}$ on the 2-subsets of $\Omega = \{1, 2, 3, \ldots, n\}$ known as duads. The stabilizer of a point (duad) $\mathcal{P} = \{a, b\} \in \Omega$ is a group isomorphic to the symmetric group S_{n-2}, and the orbits of the stabilizer consist of $\mathcal{P}$, one of length $2(n-2)$ and the other of length $\binom{n-2}{2}$. In this action A_n defines a strongly regular graph on $\binom{n}{2}$ isomorphic to the triangular graph $T(n)$. In particular for $n = 8$, we have that S_6 has orbits of lengths 1, 12, and 15. The orbit of length 12 defines the graph $T(8)$ whose parameters are $(28, 12, 6, 4)$. The permutation module splits into three irreducible constituents of dimensions 1, 6, and 14 with multiplicities 2, 2, and 1 respectively. We found that the permutation module has two maximal submodules, one of dimension 22 and the other of dimension 27. From the 27-dimensional submodule we obtain one maximal submodule of dimension 21, while from the 22-dimension submodule we get four maximal submodules, one of which has dimension 8 and the remaining three have each dimension 21. These latter submodules are all non-isomorphic. From the 8-dimensional submodule we obtain three maximal submodules of dimension 7, no two of which are isomorphic. From each of the 21-dimensional submodules we obtain two maximal submodules, one being of dimension 7, and the other of dimension 20. The 20-dimensional submodules are all isomorphic. Each one of the three 7-dimensional submodules are isomorphic to one of those obtained from the earlier 8-dimensional submodule. The first 7-dimensional submodule contains two irreducible submodules, one of dimension 1 and the other of dimension 6. The remaining 7-dimensional submodules contain each an irreducible maximal submodule of dimension 6. We

obtain in all four isomorphic and irreducible maximal submodules of dimension 6. Hence, we have a total of twelve maximal submodules invariant under A_8 from this permutation module, namely of dimensions 27, 22, 21, 21, 21, 20, 8, 7, 7, 7, 6 and 1. In Figure 8.3 we depict the lattice of submodules.

In all, we have obtained ten non-trivial codes invariant under A_8. The weight distributions of these codes are listed in Tables 8.4 and 8.5, and in Proposition 8.4 we summarize the 2-modular codes of this representation.

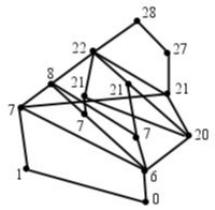


Figure 8.3: Submodule lattice for the 28-dimensional representation

Name	dim	0	3	4	5	6	7	8	9	10	11	12	13	
$C_{28,1}$	6	1										28		
$C_{28,2}$	7	1										28	56	
$C_{28,3}$	7	1										63		
$C_{28,4}$	7	1					8					28		
$C_{28,5}$	8	1					8					63	56	
$C_{28,5}{}^{\perp}$	20	1		210		2800		24087		103936		235228		
$C_{28,4}{}^{\perp}$	21	1	56	210	672	2800	9320	24087	53760	103936	169008	235228	289856	
$C_{28,3}{}^{\perp}$	21	1		315		6048		47817		206976		472059		
$C_{28,2}{}^{\perp}$	21	1		210	840	2800	9248	24087	54040	103936	166656	235228	295120	
$C_{28,1}{}^{\perp}$	22	1	56	315	1512	6048	18568	47817	107800	206976	335664	472059	584976	

Table 8.4: Weight distributions of the codes from the 28-dimensional representation.

name	14	15	16	17	18	19	20	21	22	23	24	25	28
$C_{28,1}$			35										
$C_{28,2}$			35					8					
$C_{28,3}$			63										1
$C_{28,4}$		56	35										
$C_{28,5}$		56	63					8					1
$C_{28,5}{}^{\perp}$	315360		236831		103040		23730		3248		105		
$C_{28,4}{}^{\perp}$	315360	295120	236831	166656	103040	54040	23730	9248	3248	840	105		
$C_{28,3}{}^{\perp}$	630720		472059		206976		47817		6048		315		1
$C_{28,2}{}^{\perp}$	315360	289856	236831	169008	103040	53760	23730	9320	3248	672	105	56	
$C_{28,1}{}^{\perp}$	630720	584976	472059	335664	206976	107800	47817	18568	6048	1512	315	56	1

Table 8.5: Table 8.4 continued.

Proposition 8.4. (i) *The code $C_{28,1}$ is a self-orthogonal doubly-even, projective and optimal 2-weight $[28, 6, 12]_2$ code. Its dual ${C_{28,1}}^{\perp}$ is a $[28, 22, 3]_2$ uniformly packed code. $C_{28,1}$ is an irreducible A_8-invariant $\mathbb{F}_2$-module, and $\mathrm{Aut}(C_{28,1}) \cong S_8$.*
(ii) *$C_{28,2}$ is a $[28, 7, 12]_2$ code, and ${C_{28,2}}^{\perp} = [28, 21, 4]_2$. $C_{28,2}$ and ${C_{28,2}}^{\perp}$ are optimal, and $\mathrm{Aut}(C_{28,2}) \cong S_8$.*
(iii) *$C_{28,3}$ is a self-orthogonal, doubly-even $[28, 7, 12]_2$ code. Its dual ${C_{28,3}}^{\perp}$ is a $[28, 21, 4]_2$ code. $C_{28,3}$ is a decomposable code, $C_{28,3}$ and ${C_{28,3}}^{\perp}$ are optimal self-complementary codes, and $\mathrm{Aut}(C_{28,3}) \cong S_6(2)$.*
(iv) *$C_{28,4}$ is a projective $[28, 7, 7]_2$ code, and its dual ${C_{28,4}}^{\perp}$ is a $[28, 21, 3]_2$ code. Moreover, $\mathrm{Aut}(C_{28,4}) \cong S_8$.*
(v) *The code $C_{28,5}$ is a $[28, 8, 7]_2$ self-complementary code and its dual ${C_{28,5}}^{\perp}$ is a $[28, 20, 4]_2$ code. Moreover, $C_{28,5}$ is a decomposable code, $\mathrm{Aut}(C_{28,5}) \cong S_8$ and ${C_{28,5}}^{\perp}$ is an optimal code.*

Proof: (i) Notice first that $C_{28,1}$ forms part of an infinite family of codes with parameters $[\binom{n}{2}, n-2, 2n-4]_2$ obtained from the binary row span of the adjacency matrix of the triangular graph $T(n)$. The codes of the triangular graphs have been studied in [62], and with a view for permutation decoding these codes have been examined further in [82], see also [102]. Our aim here is to give an illustration that explores the geometry of the graph and reveals the connections with modular representation theory. Thus, taking the images of the orbit of length 12 under A_8 on the duads of $\Omega = \{1, 2, \ldots, 8\}$ we obtain $C_{28,1}$ as the binary row span of the adjacency matrix of the triangular graph $T(8)$. Since $n = 28, k = 12, \lambda = 6$ and $\mu = 4$ are all even, it follows that $C_{28,1}$ is self-orthogonal. It is well-known and follows from [99] that $T(8)$ is the unique regular graph with spectrum $12^1, 4^7, -2^{20}$ for which the 2-rank is 6. Now, if we add two different vectors of the adjacency matrix M of $T(8)$ we obtain a vector of weight 12 if the corresponding vectors are adjacent and a vector of weight 16 if the vectors are not adjacent. Since there are 210 pairs of non-adjacent vertices, the binary row span of M has at least $\frac{210}{6}$ vectors of weight 16. Since the minimum weight codewords span the code and these have weight divisible by four, the code is doubly even. Further notice that $C_{28,1}$ has only two non-zero weights, i.e.,

it is a two-weight code. Let w_1 and w_2 (where $w_1 < w_2$) be the weights of a q-ary two-weight code C of length n and dimension k. To C we may associate a graph $\Gamma(C)$ on q^k vertices as follows. The vertices of the graph are identified with the codewords and two vertices corresponding to the codewords x and y are adjacent if and only if $d(x, y) = w_1$. From the above we obtain a strongly regular graph $\Gamma(C_{28,1})$ associated to $C_{28,1}$ with parameters $(64, 35, 18, 20)$ and its complement, a strongly regular $(64, 28, 12, 12)$ graph $\overline{\Gamma(C_{28,1})}$. Since $\lambda = \mu$ we have that $\overline{\Gamma(C_{28,1})}$ is in fact a 2-$(64, 28, 12)$ design with no absolute polarities. Designs with the parameters of $\overline{\Gamma(C_{28,1})}$ belong to a family of

$$v = 2^{2m},\ k = 2^{2m-1} - 2^{m-1},\ \lambda = 2^{2m-2} - 2^{m-1},\ n = 2^{2m-2}$$

symmetric designs (see [98]) termed symmetric difference property design following [73]. Recall that a code is called projective if its dual distance is at least 3. Moreover, a code with minimum distance $d = 3$ and covering radius 2 is called uniformly packed if every vector which is not a codeword is at distance 1 or 2 from a constant number of codewords [113]. It then follows that ${C_{28,1}}^{\perp}$ is projective and $C_{28,1}$ is uniformly packed. Moreover ${C_{28,1}}^{\perp}$ has precisely $\binom{8}{3} = 56$ codewords of minimum weight 3 and the minimum weight codewords span the code. Now, from the 2-modular character table of A_8 (see [70, 119]), we have that the irreducible 6-dimensional $\mathbb{F}_2$-representation is unique. Since $\mathrm{Aut}(C_{28,1})$ contains A_8, by using the above weight enumerator we can easily see that $C_{28,1}$, under the action of A_8, does not contain an invariant subspace of dimension 1. Thus, if $C_{28,1}$ were reducible, it would contain an invariant irreducible subspace E of dimension d with $2 \leq d \leq 5$, which is not possible. Hence, C_Γ is irreducible and must be isomorphic to the 6-dimensional $\mathbb{F}_2$-module on which A_8 acts irreducibly. That the automorphism group of the code is the symmetric group S_8, follows by the classification of primitive groups [105], as this is the only primitive group of degree 28, and order 40320.

(ii) For the dimension of $C_{28,2}$, notice from Table 8.4 that $C_{28,1}$ is a subcode of codimension 1 in $C_{28,2}$ spanned by the words of weight divisible by four. Furthermore $C_{28,2}$ is not spanned by its minimum weight codewords; it is spanned by the words of weight 13. Moreover, and using Magma we verified that $\mathrm{Aut}(C_{28,2}) \cong S_8$. Under the

action of S_8, the codewords of weight 13 form a single orbit, with the stabilizer of such a codeword a maximal subgroup isomorphic to $S_5 \times S_3$. Similarly, the codewords of weight 21 form a single orbit invariant under S_8 and these codewords are stabilized by a maximal subgroup isomorphic to S_7.

(iii) Notice first that $C_{28,3} = \langle C_{28,1}, \mathbf{1} \rangle = C_{28,1} \oplus \langle \mathbf{1} \rangle$. Hence $C_{28,3}$ is a decomposable module. Now, suppose that $\alpha \in \mathrm{Aut}(C_{28,1})$. Since $\alpha(\mathbf{1}) = \mathbf{1}$ and $C_{28,3} = \langle C_{28,1}, \mathbf{1} \rangle$, we have $\alpha \in \mathrm{Aut}(C_{28,3})$, so that $\mathrm{Aut}(C_{28,1}) \subseteq \mathrm{Aut}(C_{28,3})$. Hence we have by part (i) that $S_8 \leq \mathrm{Aut}(C_{28,3})$. Since $[\mathrm{Aut}(C_{28,3}){:}S_8] = 36$ and by Magma we have that S_8 is a maximal subgroup of $\mathrm{Aut}(C_{28,3})$, in order to describe the structure of $\mathrm{Aut}(C_{28,3})$ we need to determine a primitive group of degree 36 which contains S_8 maximally. Of the 20 primitive groups of degree 36 (see [105]) only one satisfies the above conditions, this being the symmpletic group $S_6(2)$. Hence $\mathrm{Aut}(C_{28,3}) \cong S_6(2)$. In addition, observe that $C_{28,2}$ and $C_{28,3}$ have the same parameters, however they are easily distinguished using their weight distributions.

In part (iv), for the dimension of $C_{28,4}$, notice from Table 8.4 that $C_{28,1}$ is a subcode of codimension 1 in $C_{28,4}$ spanned by the words of weight divisible by four. Furthermore, since $C_{28,4}$ is spanned by its minimum weight codewords, we can easily deduce its automorphism group. In fact we can show that $\mathrm{Aut}(C_{28,4}) \cong S_8$.

Finally, part (v) follows at once by noticing that $C_{28,5} = C_{28,3} \cup C_{28,4}$, and moreover $C_{28,4}$ is the subcode of $C_{28,5}$ spanned by any set of codewords of odd weight, while $C_{28,3}$ is the subcode generated by words of weight divisible by four. The codes $C_{28,3}$ and $C_{28,4}$ intersect in their doubly-even subcode of dimension 6, which is in fact $C_{28,1}$. Moreover, since $C_{28,5} = \langle C_{28,4}, \mathbf{1} \rangle = C_{28,4} \oplus \langle \mathbf{1} \rangle$ the assertions on the dimension and minimum weight follow. Considering the latter inclusion and the order of the groups, we obtain that $\mathrm{Aut}(C_{28,5}) \cong S_8$. Optimality of all codes can be verified in [17] or [59] and also using Magma [27]. Finally, the codes $C_{28,2}, {C_{28,2}}^{\perp}, C_{28,4}, {C_{28,4}}^{\perp}, C_{28,5}$ and ${C_{28,5}}^{\perp}$ are all optimal. ■

8.8 Designs held by the support of codewords in $C_{28,i}$

A careful examination of Tables 8.4 and 8.5 shows that the non-zero codewords of the codes tabulated are single orbits stabilized by maximal subgroups of the automorphism groups. Suppose that w_m is a codeword of non-zero weight m in $C = C_{28,i}$ where $i = 1, 2, \ldots, 5$. In this section we determine the structures of $(\mathrm{Aut}(C))_{w_m}$, that is the stabilizers of w_m in $\mathrm{Aut}(C)$. The structures of these stabilizers are listed in Table 8.6.

8.8.1 Stabilizer in $\mathrm{Aut}(C)$ of a word w_i in C

We now examine the action of $\mathrm{Aut}(C) = S_8$ or $\mathrm{Aut}(C) = S_6(2)$ on the set W_m of non-trivial codewords of C and describe their nature. In addition we look at the structure of the stabilizers $(\mathrm{Aut}(C))_{w_m}$ where $m \in M$ with M defined as follows.

Consider $M = \{7, 12, 13, 15, 16, 21\}$. For $m \in M$ we define $W_m = \{w_m \in C_{28,i} \mid \mathrm{wt}(w_m) = m\}$. We show in Lemma 8.5 that for all $m \in M$, $(\mathrm{Aut}(C))_{w_m} = H$ where $H \underset{\max}{<} \mathrm{Aut}(C)$ is a maximal subgroup of $\mathrm{Aut}(C)$. In addition for $w_m \in W_m$ we take image of the support of w_m under the action of $G = S_8$ or $G = S_6(2)$ to form the blocks of the t-$(28, m, k_m)$ $(1 \leq t \leq 2)$ designs $\mathfrak{D} = \mathcal{D}_{w_m}$, where $k_m = |(w_m)^G| \times \frac{m}{28}$ and show that $\mathrm{Aut}(C)$ acts primitively on $\mathcal{D}_{w_m}$. Information on these designs is given in Table 8.7.

Lemma 8.5. *Let C be a code of Proposition 8.4, and $0 \neq w \in C$. Then $\mathrm{Aut}(C)_w$ is a maximal subgroup of $\mathrm{Aut}(C)$. Moreover, the design $\mathfrak{D}$ obtained by orbiting the images of the support of any non-trivial codeword in C is primitive.*

Proof: Notice from Proposition 8.4 that $\mathrm{Aut}(C) = S_8$ or $\mathrm{Aut}(C) = S_6(2)$. We consider the following two cases.

Case I. $\mathrm{Aut}(C) = S_8$. Since W_m is invariant under the action of S_8 for all $m \in M$, Tables 8.4 and 8.5 show that ${w_m}^{S_8} = W_m$ except when $C = C_{28,5}$ and

$m = 12$ or $m = 16$. Therefore each W_m is a single orbit under the action of S_8, so that S_8 is transitive on each W_m. From Tables 8.4 and 8.5 and the orbit stabilizer theorem we deduce that $[S_8{:}(S_8)_{w_m}] \in \{8, 28, 35, 56\}$. Looking at the list of maximal subgroups of S_8 (see $\mathbb{ATLAS}$ [34]) and furthermore, using results of [103] we deduce that $(S_8)_{w_m} \in \{S_7, S_6 \times 2, (S_4 \times S_4){:}2, S_5 \times S_3\}$. Since S_8 is transitive on the code coordinates, the codewords of W_m form a 1-design $\mathcal{D}_{w_m}$ with the number of blocks being the indices of $(S_8)_{w_m}$ in S_8. This implies that S_8 is transitive on the blocks of $\mathcal{D}_{w_m}$ for each w_m and since $(S_8)_{w_m}$ is a maximal subgroup of S_8 for $m \in M$, we deduce that S_8 acts primitively on $\mathcal{D}_{w_m}$. See Table 8.6 and Table 8.7 for the parameters of these designs. Now, consider $C = C_{28,5}$ and $m = 12$. In this case $|W_{12}| = 63$ and W_{12} splits into two orbits of lengths 28 and 35, namely $W_{(12)_1}$ and $W_{(12)_2}$ under $\mathrm{Aut}(C)$. If $m = 16$ we have $|W_{16}| = 63$ and as earlier W_{16} also splits into two orbits of lengths 28 and 35, namely $W_{(16)_1}$ and $W_{(16)_2}$ respectively.

Case II. $\mathrm{Aut}(C) = S_6(2)$. In this case $C = C_{28,3}$ with $m = 12$ or $m = 16$. For either choices of m we have ${w_m}^{S_6(2)} = W_m$. Thus, W_m is a single orbit of $S_6(2)$, and arguing similarly as in CASE I, we can show that $(S_6(2))_{w_m}$ is a maximal subgroup of $S_6(2)$ isomorphic to $2^5{:}S_6$. Lastly, $S_6(2)$ is primitive on the designs $D_{w_{12}} = 2\text{-}(28, 12, 11)$ and its complement $\overline{\mathcal{D}}_{w_{16}} = 2\text{-}(28, 16, 20)$ obtained by orbiting the images of the supports of the codewords of weight 12 and 16 respectively. ■

In Table 8.6 the first column gives the codes $C_{28,i}$, the second column represents the codewords of weight m (the sub-indices of m represent the code from where the codeword is drawn), the third column gives the structure of the stabilizers in $\mathrm{Aut}(C)$ of a codeword w_m and the last column, tests the maximality $(\mathrm{Aut}(C))_{w_m}$.

In Table 8.7 the first column represents the codewords of weight m and the second column gives the parameters of the t-designs $\mathcal{D}_{w_m}$ as defined in Section 8.8. In the third column we list the number of blocks of $\mathcal{D}_{w_m}$. The final column shows whether or not a design $\mathcal{D}_{w_m}$ is primitive under the action of $\mathrm{Aut}(C)$.

In Remark 8.6, below we use Lemma 8.5 to give a geometric description of the nature of the codewords in each of the codes of Proposition 8.4. A geometric significance of the minimum weight codewords of the respective duals could also be

C	m	$(\mathrm{Aut}(C))_{w_m}$	Maximal	C	m	$(\mathrm{Aut}(C))_{w_m}$	Maximal
$C_{28,4}$	7_4	S_7	Yes	$C_{28,4}$	15_4	$S_5 \times S_3$	Yes
$C_{28,5}$	7_5	S_7	Yes	$C_{28,5}$	15_5	$S_5 \times S_3$	Yes
$C_{28,1}$	12_1	$S_6 \times 2$	Yes	$C_{28,1}$	16_1	$(S_4 \times S_4) : 2$	Yes
$C_{28,2}$	12_2	$S_6 \times 2$	Yes	$C_{28,2}$	16_2	$(S_4 \times S_4) : 2$	Yes
$C_{28,3}$	12_3	$2^5 : S_6$	Yes	$C_{28,3}$	16_3	$2^5 : S_6$	Yes
$C_{28,4}$	12_4	$S_6 \times 2$	Yes	$C_{28,4}$	16_4	$(S_4 \times S_4) : 2$	Yes
$C_{28,5}$	$(12_5)_1$	$S_6 \times 2$	Yes	$C_{28,5}$	$(16_5)_1$	$S_6 \times 2$	Yes
	$(12_5)_2$	$(S_4 \times S_4) : 2$	Yes		$(16_5)_2$	$(S_4 \times S_4) : 2$	Yes
$C_{28,2}$	13_2	$S_5 \times S_3$	Yes	$C_{28,2}$	21_2	S_7	Yes
$C_{28,5}$	13_5	$S_5 \times S_3$	Yes	$C_{28,5}$	21_5	S_7	Yes

Table 8.6: Stabilizer in $\mathrm{Aut}(C)$ of a codeword w_m

m	$\mathcal{D}_{w_m}$	No. of blocks	Prim	m	$\mathcal{D}_{w_m}$	No. of blocks	Prim
7_4	1-$(28, 7, 2)$	8	Yes	15_4	1-$(28, 15, 30)$	56	Yes
7_5	1-$(28, 7, 2)$	8	Yes	15_5	1-$(28, 15, 30)$	56	Yes
12_1	1-$(28, 12, 12)$	28	Yes	16_1	1-$(28, 16, 16)$	35	Yes
12_2	1-$(28, 12, 12)$	28	Yes	16_2	1-$(28, 16, 20)$	35	Yes
12_3	2-$(28, 12, 11)$	63	Yes	16_3	2-$(28, 16, 20)$	63	Yes
12_4	1-$(28, 12, 12)$	28	Yes	16_4	1-$(28, 16, 20)$	35	Yes
$(12_5)_1$	1-$(28, 12, 12)$	28	Yes	$(16_5)_1$	1-$(28, 16, 16)$	28	Yes
$(12_5)_2$	1-$(28, 12, 15)$	35	Yes	$(16_5)_2$	1-$(28, 16, 20)$	35	Yes
13_2	1-$(28, 13, 26)$	56	Yes	21_2	1-$(28, 21, 6)$	8	Yes
13_5	1-$(28, 13, 26)$	56	Yes	21_5	1-$(28, 21, 6)$	8	Yes

Table 8.7: Primitive t-designs $\mathcal{D}_{w_m}$ invariant under $\mathrm{Aut}(C)$

given.

Remark 8.6. (i) Notice that the minimum weight of of $C_{28,1}$ is precisely the valency of the graph, and that the minimum weight codewords are the rows of the adjacency matrix of $T(8)$ and these span the code. From a purely geometric perspective one can regard the minimum weight codewords as the duads $\mathcal{P} = \{a, b\}$ (2-element subsets) of the set $\Omega = \{1, 2, \ldots, 8\}$ and those of weight 16 as the lines of the projective space PG$(3, 2)$. Observe that all weights in $C_{28,2}$ are $\equiv 0, 1 \pmod 4$. Consequently, since $C_{28,1} \subseteq C_{28,2}$ we have that the words of weight $\equiv 0 \pmod 4$ in $C_{28,2}$ have the same geometrical significance as those of $C_{28,1}$, hence they are the duads of Ω, while the words of weight $\equiv 1 \pmod 4$ represent the set of triads $\mathcal{P} = \{a, b, c\}$ of Ω (see Section 8.9) and the points using the alternating notation (see Section 8.2 or the $\mathbb{ATLAS}$ [34]).

For the code $C_{28,3}$ the codewords of minimum weight 12 represent the 63 isotropic points of the orthogonal space, and since the dimension of the code is 7, this provides an illustration of the isomorphism $S_6(2) \cong \Omega^+(7, 2)$. Moreover, the minimum weight codewords constitute the 63 rows of the incidence matrix of a quasi-symmetric 2-$(28, 12, 11)$ design $\mathcal{D}$ formed by taking the images of the support of the codewords of minimum weight under the action of the automorphism group. This is in fact a derived design with respect to a block of the 2-$(64, 28, 12)$ design given earlier. That the automorphism group of this design is isomorphic to $S_6(2)$ is well-known (see for example, [53], [98]). Since $\mathrm{Aut}(\mathcal{D}) \subseteq \mathrm{Aut}(C_{28,3})$, and have the same order, it follows at once that $\mathrm{Aut}(C_{28,3}) \cong S_6(2)$. Since $\mathbf{1} \in C_{28,5}$ we have that the number of codewords of any weight w equals the number of words of weight $28 - w$. Moreover, all weights in $C_{28,5}$ are $\equiv 0, 1 \pmod 4$. Since $C_{28,5} = C_{28,3} \cup C_{28,4}$ and also $C_{28,5} = C_{28,4} \oplus \langle \mathbf{1} \rangle$ a geometric description of the codewords of $C_{28,5}$ can be given in terms of either $C_{28,3}$ and $C_{28,4}$ or simply using $C_{28,4}$.

(ii) The full set of minimum weight four vectors of ${C_{28,3}}^{\perp}$ defines a 2-$(28, 4, 5)$ design with 315 blocks, which we denote $\mathsf{H}(q)$. This design which was found by Hölz is in a class of well-known designs with parameters 2-$(q^3 + 1, q + 1, q + 2)$. It is known that $\mathsf{H}(q)$ contains the 2-rank 21 Hermitian and the 2-rank 19 Ree unitals

i.e., 2-$(28, 4, 1)$ designs as subdesigns, see [4, 92], and also [121] for a more recent account. The 315 vectors of minimum weight include the characteristic functions of the design forming these two unitals. Acting the subgroups $P\Gamma L_2(8)$ and $P\Gamma U_3(9)$ of $S_6(2)$ will isolate the weight four vectors that make up the blocks of copies of each of these unitals. When $q = 3$ the codes of the Hermitian and Ree unitals coincide with the code of $\mathsf{H}(q)$, which is in fact a code isomorphic to $C_{28,3}$ i.e., the dual code of the unital of order 3.

(iii) It was proved by Jungnickel and Tonchev in [71] that there exist four non-isomorphic symmetric 2-$(64, 28, 12)$ designs characterized by symmetric difference property and minimality of their 2-rank. Moreover, these designs have large full automorphism groups, and also large 2-subgroups. In particular, the orders of the full automorphism groups are divisible by 2^6, and their derived 2-$(28, 12, 11)$ quasi-symmetric designs give rise to four inequivalent $[28, 7, 12]_2$ codes whose weight distributions equals that of $C_{28,3}$. This shows that the code of the unital of order 3 is not unique. For more details, consult [98] and [53]. It has recently been proved (see [11, Theorem 5.1]) that there is exactly one primitive symmetric design with parameters 2-$(64, 28, 12)$ whose automorphism group is a maximal subgroup of index 694980 of the sporadic simple group Fi_{22} isomorphic to $2^6{:}S_6(2)$. Furthermore, using tactical decompositions Crnković and Pavčević [38] constructed forty-six non-isomorphic symmetric 2-$(64, 28, 12)$ designs from orbit matrices having the Frobenius group of order 21 as an automorphism group. These designs do not satisfy the symmetric difference property, 2^6 is not a divisor of the order of their full automorphism groups, and their derived 2-$(28, 12, 11)$ designs are not quasi-symmetric. We refer the reader to Chapter 9 where we examine the binary codes of these designs.

8.9 The 35-dimensional representation

The group A_8, acts as a primitive rank-3 group of degree 35 on the set of lines of $V_4(2)$ (see $\mathbb{ATLAS}$ [34]); with line stabilizer isomorphic to $2^4{:}(S_3 \times S_3)$. The orbits of

the stabilizer of a line $\mathfrak{L}$ consist of $\{\mathfrak{L}\}, \Psi$ and Φ of lengths 1, 16 and 18 respectively. In addition, since A_8 acts as a rank-3, it is clear that the image of Ψ (or Φ) under A_8 defines a strongly regular graph. We denote this graph Γ and its complement $\overline{\Gamma}$. Note that Γ has parameters $(35, 16, 6, 8)$ and its complement is a $(35, 18, 9, 9)$ graph, which is in fact a 2-$(35, 18, 9)$ design whose polarity has no absolute points. According to the $\mathbb{ATLAS}$ [34] the elements being permuted are the 35 bisections. The permutation module splits into five absolutely irreducible constituents of dimensions 1, 4, 4, 6 and 14 with multiplicities of 1, 1, 1, 2 and 1 respectively.

There are only two irreducible submodules in this representation, one of dimension 1 and the other of dimension 6. The permutation module has two maximal submodules of dimensions 29 and 34 respectively. From the 29 dimensional submodule we get four non-isomorphic maximal submodules of dimensions 15, 25, 25, and 28. The 34-dimensional submodule has one maximal submodule isomorphic to the 28 dimensional submodule given above. Chopping the modules recursively and filtering out the isomorphic copies, as it was for the representations of degrees 15 and 28 we get submodules of dimensions 34, 29, 28, 25, 25, 24, 24, 21, 20, 15, 14, 11, 11, 10, 10, 7 and 6. The two codes from submodules of dimension 25 are isomorphic and so are those from the submodules of dimensions 24, 11 and 10. Hence, we obtain twelve non-trivial binary codes. We denote the codes as $C_{35,i}$ and the duals $C_{35,i}{}^{\perp}$, where $i = 1, 2, \ldots, 6$. The lattice of submodules is given in Figure 8.4 and the weight distributions are given in Tables 8.8, 8.9 and 8.10 respectively.

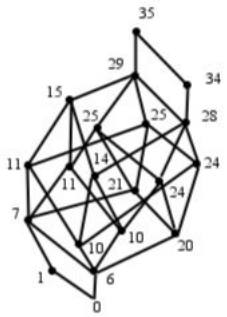


Figure 8.4: Submodule lattice for the 35-dimensional representation

In Proposition 8.7 which follows, we summarize the properties of the codes.

Name	dim	0	3	4	5	6	7	8	9	10	11	12
$C_{35,1}$	6	1										
$C_{35,2}$	7	1										
$C_{35,3}$	10	1										105
$C_{35,4}$	11	1					15					105
$C_{35,5}$	14	1						105				105
$C_{35,6}$	15	1					30	105			315	630
${C_{35,6}}^{\perp}$	20	1				280		735		11648		52290
${C_{35,5}}^{\perp}$	21	1			56	280	210	735	4480	11648	26145	52290
${C_{35,4}}^{\perp}$	24	1		105		1960		21525		179648		813645
${C_{35,3}}^{\perp}$	25	1		105	56	1960	6735	21525	71680	179648	401415	813645
${C_{35,2}}^{\perp}$	28	1		840		25480		366660		2872688		13027560
${C_{35,1}}^{\perp}$	29	1	105	840	5096	25480	104760	366660	1104880	2872688	6513780	13027560

Table 8.8: Weight distributions of the codes from the 35-dimensional representation.

Proposition 8.7. (i) $C_{35,1} = [35, 6, 16]_2$ *is a self-orthogonal, doubly-even and projective code. Its dual* ${C_{35,1}}^{\perp} = [35, 29, 3]_2$ *is a uniformly packed code. Moreover,* $C_{35,1}$ *and* ${C_{35,1}}^{\perp}$ *are optimal and* $\mathrm{Aut}(C_{35,1}) \cong S_8$ *acts irreducibly on* $C_{35,1}$ *as an* $\mathbb{F}_2$*-module.*

(ii) $C_{35,2} = [35, 7, 15]_2$ *and* ${C_{35,2}}^{\perp} = [35, 28, 4]_2$ *is an optimal and singly-even code. Furthermore* $\mathbf{1} \in C_{35,2}$ *and* $C_{35,2}$ *is a decomposable code, and* $\mathrm{Aut}(C_{35,2}) \cong S_8$.

(iii) $C_{35,3} = [35, 10, 12]_2$ *is a self-orthogonal and doubly-even code. Its dual* ${C_{35,3}}^{\perp}$ *is a* $[35, 25, 4]_2$ *code. Moreover,* $\mathrm{Aut}(C_{35,3}) \cong A_8$ *and* $C_{35,3}$ *and* ${C_{35,3}}^{\perp}$ *are optimal.*

(iv) $C_{35,4} = [35, 11, 7]_2$ *and* $\mathbf{1} \in C_{35,4}$. *The dual* ${C_{35,4}}^{\perp} = [35, 24, 4]_2$ *is singly-even. Moreover,* $C_{35,4}$ *is decomposable, and* $\mathrm{Aut}(C_{35,4}) \cong A_8$.

(v) $C_{35,5} = [35, 14, 8]_2$ *is a self-orthogonal and singly-even code. The dual* ${C_{35,5}}^{\perp} = [35, 21, 5]_2$ *and* $\mathrm{Aut}(C_{35,5}) \cong S_8$.

(vi) $C_{35,6} = [35, 15, 7]_2$ *and* $\mathbf{1} \in C_{35,6}$*, and the dual* ${C_{35,6}}^{\perp} = [35, 20, 6]_2$ *is singly-even. Moreover,* $C_{35,6}$ *is decomposable, and* $\mathrm{Aut}(C_{35,6}) \cong S_8$.

Proof: We start by observing that $C_{35,2} = C_{35,1} \oplus \langle \mathbf{1} \rangle$, $C_{35,4} = C_{35,3} \oplus \langle \mathbf{1} \rangle$, and $C_{35,6} = C_{35,5} \oplus \langle \mathbf{1} \rangle$. Consequently, it follows that $\mathrm{Aut}(C_{35,1}) \subseteq \mathrm{Aut}(C_{35,2})$, $\mathrm{Aut}(C_{35,3}) \subseteq \mathrm{Aut}(C_{35,4})$ and $\mathrm{Aut}(C_{35,5}) \subseteq \mathrm{Aut}(C_{35,6})$. Further, $C_{35,2}, C_{35,4}$ and $C_{35,6}$ are all decomposable codes (resp. decomposable $\mathbb{F}_2$-modules) invariant under A_8. For parts (i) and (ii), note that $C_{35,1}$ is the code defined by the row span over $\mathbb{F}_2$ of

name	13	14	15	16	17	18	19	20	21	22
$C_{35,1}$				35				28		
$C_{35,2}$			28	35			35	28		
$C_{35,3}$				455				448		
$C_{35,4}$			448	455			455	448		
$C_{35,5}$		2640		4235		3360		3388		1680
$C_{35,6}$	1680	2640	3388	4235	3360	3360	4235	3388	2640	1680
${C_{35,6}}^{\perp}$		140360		244895		282240		195916		89320
${C_{35,5}}^{\perp}$	89320	140360	195916	244895	282240	282240	244895	195916	140360	89320
${C_{35,4}}^{\perp}$		2283560		3924515		4468800		3155131		1448440
${C_{35,3}}^{\perp}$	1448440	2283560	3155131	3924515	4468800	4468800	3924515	3155131	2283560	1448440
${C_{35,2}}^{\perp}$		36268760		63410270		70926240		50728216		23080120
${C_{35,1}}^{\perp}$	23080120	36268760	50728216	63410270	70926240	70926240	63410270	50728216	36268760	23080120

Table 8.9: Table 8.8 continued.

name	23	24	25	26	27	28	29	30	31	32	35
$C_{35,1}$											
$C_{35,2}$											1
$C_{35,3}$						15					
$C_{35,4}$	105					15					1
$C_{35,5}$		315				30					
$C_{35,6}$	630	315			105	30					1
${C_{35,6}}^{\perp}$		26145		4480		210		56			
${C_{35,5}}^{\perp}$	52290	26145	11648	4480	735	210	280	56			1
${C_{35,4}}^{\perp}$		401415		71680		6735		56			
${C_{35,3}}^{\perp}$	813645	401415	179648	71680	21525	6735	1960	56	105		1
${C_{35,2}}^{\perp}$		6513780		1104880		104760		5096		105	
${C_{35,1}}^{\perp}$	13027560	6513780	2872688	1104880	366660	104760	25480	5096	840	105	1

Table 8.10: Table 8.9 continued

the adjacency matrix of the graph Γ (or equivalently of the row span of the adjacency matrix of a 1-design $\mathfrak{D}$ with parameters 1-$(35, 16, 16)$ formed by taking the vertices of Γ as the blocks of the design, and incidence in the design as adjacency in the graph). Thus, $C_{35,2}$ is the code of the complementary design $\overline{\mathfrak{D}}$ of $\mathfrak{D}$ and so the difference of any two codewords in $C_{35,1}$ is in $C_{35,2}$. As these differences span a subcode of dimension 6 in $C_{35,2}$, this subcode must be $C_{35,1}$. Moreover, from the weight distribution (see Table 8.8) we deduce that $C_{35,1}$ is the subcode of $C_{35,2}$ spanned by words of weight divisible by four. The above inclusion now follows, as $C_{35,2}$ is $C_{35,1}$ adjoined by the vector $\mathbf{1}$. Since Γ is a graph that appears in a partition of the symplectic graph $\mathcal{S}_6^+(2)$ it follows from [99, Theorem 5.3] that Γ possesses the triangle property and as such it is uniquely determined by its parameters and by the minimality of its 2-rank, which is 6. Thus the dimension of $C_{35,1}$ is 6. For completeness, we give a brief overview of the symmplectic graph. Let $\mathcal{A}$ be a $2n \times 2n$ nonsingular alternate

matrix over $\mathbb{F}_q$, the symplectic graph relative to $\mathcal{A}$ over $\mathbb{F}_q$ is the graph with the set of one-dimensional subspaces of ${\mathbb{F}_q}^{(2n)}$ as its vertex set and with adjacency defined by $[u] \sim [v]$ if and only if $u\mathcal{A}^t v \neq 0$ for any $u \neq 0$ and $v \neq 0 \in {\mathbb{F}_q}^{(2n)}$, where $[u]$ and $[v]$ are one-dimensional subspaces of ${\mathbb{F}_q}^{(2n)}$, and $[u] \sim [v]$ means that $[u]$ and $[v]$ are adjacent. Furthermore, the minimum-weight 16 of $C_{35,1}$ can be deduced using results from [62, Section 4.4]. We note in addition that all codewords of $C_{35,1}$ are linear combinations of at most two rows of the adjacency matrix of Γ, and since there are exactly 35 codewords of minimum weight in $C_{35,1}$ and these are precisely all the rows of the adjacency matrix of Γ, these must span the code. Since the spanning vectors have weight 16, we have that $C_{35,1}$ is doubly-even and hence self-orthogonal. In addition $C_{35,1}$ is a two-weight code, and by an argument similar to that used in the proof of Proposition 8.4(i) we obtain a strongly regular $(64, 28, 12, 12)$ and its complement. Since ${C_{35,1}}^{\perp}$ has minimum weight 3 it follows from [23] that $C_{35,1}$ is a projective code, and moreover $C_{35,1}$ is uniformly packed [113]. Optimality of $C_{35,1}$ and ${C_{35,1}}^{\perp}$ follows by Magma [27] and also from [59, 58]. Further, using [59, 58] we obtain that $C_{35,2}$ is a distance 1 less than the optimal. The assertion on irreducibility of $C_{35,1}$ follows an argument similar to that used in the proof of Proposition 8.4(i). Finally, $C_{35,1}$ is isomorphic as an $\mathbb{F}_2$-module to $C_{28,1}$ and $C_{35,2}$ is a decomposable 7-dimensional $\mathbb{F}_2$-module invariant under S_8. For the automorphism of the code we will use the knowledge on the design $\mathfrak{D}$ given above. Let $\overline{G} = \mathrm{Aut}(\mathfrak{D})$. By construction we have that $A_8 \subseteq \overline{G}$. However $|\overline{G}| = 2 \times |A_8|$ and $\overline{G}$ is a group generated by permutations such as $(1, 28)(3, 12)(4, 16)(6, 8)(10, 17)(13, 35)(15, 27)(18, 34)(23, 26)(30, 33)$ and $(1, 24, 33, 34, 26, 20, 5)(2, 4, 11, 18, 31, 8, 6)(3, 25, 14, 23, 16, 27, 19)(7, 21, 35, 12, 28, 13, 9)$ $(10, 30, 32, 29, 15, 17, 22)$, which we denote x and y. Since these satisfy $x^2 = y^7 = (xy)^8 = 1$ and $\overline{G} = \langle x, y \rangle$ we have that $\overline{G} \cong S_8$. Moreover $\overline{G} \subseteq \mathrm{Aut}(C_{35,1})$ and since the minimum weight codewords are the blocks of $\mathfrak{D}$ and span $C_{35,1}$ we have that $\overline{G} \cong \mathrm{Aut}(C_{35,1})$.

For parts (iii) and (iv), we note that $C_{35,4}$ is the code spanned by the rows of the 35×15 triple symbol incidence matrix of the design $\mathcal{D}$ of points and lines of $\mathrm{PG}(3, 2)$. This is a quasi-symmetric 2-$(15, 3, 1)$ design with 35 blocks, and blocks

meeting in 0 or 1 point respectively. It is well-known that the block graph of a quasi-symmetric design is a strongly regular graph, in this case we have a strongly regular $(35, 18, 9, 9)$ graph (see [110, Theorem 3.7]). The design $\mathcal{D}$ is the only 2-$(15, 3, 1)$ design for which the 2-rank is 11, as suggested by the well-known Hamada's conjecture on the minimality of the p-rank of geometric codes amongst those of the same parameters which reads as follows:

Conjecture 8.8. *(Hamada's Conjecture) Let $\mathcal{D}$ be a design with the parameters of a geometric design $PG_d(n, q)$ or $AG_d(n, q)$, where q is a power of a prime p. Then the p-rank of the incidence matrix of $\mathcal{D}$ is greater than or equal to the p-rank of the corresponding geometric design. Moreover, equality holds if and only if $\mathcal{D}$ is isomorphic to the geometric design.*

For more information about the Hamada conjecture we refer the reader to [63]. Moreover, the minimum weight codewords span $C_{35,4}$ and since $r = 7$ is odd we obtain that $C_{35,4}$ contains the all-one vector $\mathbf{1}$. In addition from $r = 7 \neq 2\lambda = 2$ and ${C_{35,4}}^{\perp} \neq 0$ it follows using [93, Lemma 5] that the minimum-weight of ${C_{35,4}}^{\perp}$ is at least 4. That the automorphism groups is as claimed follows using the fundamental theorem of projective geometry, and also considering the earlier inclusions and taking orders of the groups. Now, the words of weight divisible by four in $C_{35,4}$ form a linear subspace of codimension 1, so by the earlier containment we deduce that this code must be isomorphic to $C_{35,3}$(recall that $C_{35,4}$ is $C_{35,3}$ adjoined by the all-one vector). Further, since $C_{35,3}$ is spanned by its minimum weight codewords the assertion on the automorphism group follows.

Finally, for parts (v) and (vi) the dimension of the codes can be deduced immediately from the structures of the submodules, and the automorphism group follows from the earlier inclusions discussed at the beginning of the proof, and considering the orders. The codes $C_{35,5}, {C_{35,5}}^{\perp}, C_{35,6}$ and ${C_{35,6}}^{\perp}$ are all optimal. ■

It can be deduced from Tables 8.8, 8.9 and 8.10 that the stabilizers of the codewords of the codes given in Proposition 8.7 are not always maximal subgroups of the automorphism group. However, in most cases a result along the lines of Lemma 8.5 could be derived. Such result although of interest would consist of

many cases and its proof depend on a tedious case-by-case analysis. Thus, in Remark 8.9 below we concentrate only on examining the nature of the minimum weight codewords in each of the codes of Proposition 8.7. We give a geometric significance of those codewords and show in addition that they constitute single orbits of the corresponding automorphism groups.

Remark 8.9. (i) The words of weight 16 in $C_{35,1}$ have a geometrical significance: they are the rows of the adjacency matrix of Γ or equivalently the incidence vectors of the blocks of a 1-$(35, 16, 16)$ design formed by the images of the supports of the codewords of this weight. Since the symmetric group S_8 is the automorphism group of the code, we consider this action and provide a geometrical significance of some classes of codewords. From the $\mathbb{ATLAS}$ [34] we have that the words of weight 16 in $C_{35,1}$ represent the bisections, while those of weight 20, represent the duads. The stabilizers in S_8 of a bisection, and of a duad are maximal subgroups isomorphic to $(S_4 \times S_4)$:2 and to $S_6 \times 2$, respectively. We thus have shown that S_8 acts primitively on the set of duads, and on the set of bisections.

Furthermore, since A_8 acts on $C_{35,1}$ we can interpret the codewords of this code using A_8. Viewing A_8 as $L_4(2)$ we have from $\mathbb{ATLAS}$ [34] that the objects permuted by the automorphism group are lines and copies of $S_4(2)$. The codewords of weight 16 represent the lines of $\mathrm{PG}(3, 2)$ while those of weight 20 are copies of $S_4(2)$, thereby explaining the connection with the symplectic graph $\mathcal{S}_6^+(2)$ found in the proof of Proposition 8.7. The stabilizers of a line, and of a copy of an $S_4(2)$ are maximal subgroups of A_8 isomorphic respectively to $2^4{:}(S_3 \times S_3)$ and S_6. Thus we have a primitive action of A_8 on the lines of $\mathrm{PG}(3, 2)$, and on the set of conjugates of $S_4(2)$ respectively.

The dimension 6 of $C_{35,1}$ provides a nice illustration of the isomorphism between A_8 and $\Omega^+(6, 2)$ (similar interpretation could be given for $C_{28,1}$). Therefore using $A_8 \cong \Omega^+(6, 2)$ we can regard the non-zero codewords of $C_{35,1}$ respectively as the sets of isotropic and the non-isotropic points of the orthogonal geometry. This in turn indicates that the objects being permuted are respectively the isotropic and non-isotropic points. The stabilizer of an isotropic point is a maximal subgroup of S_8

isomorphic to $(S_4 \times S_4)$:2 (resp. maximal subgroup of A_8 isomorphic to 2^4:$(S_3 \times S_3)$) and that of a non-isotropic point is a maximal subgroup isomorphic with $S_6 \times 2$ (resp. maximal subgroup of A_8 isomorphic to S_6). Now, since $C_{35,2} = C_{35,1} \oplus \langle \mathbf{1} \rangle$ the geometrical significance of the words of $C_{35,2}$ can be deduced in terms of the words of $C_{35,1}$.

(ii) The codewords of minimum weight in $C_{35,4}$ are precisely the 15 points of PG$(3, 2)$, and the isotropic planes in the orthogonal geometry. The stabilizer of a codeword of minimum weight is a maximal subgroup of A_8 isomorphic to $2^3 : L_3(2)$. The codewords of minimum weight 12 in $C_{35,3}$ are invariant under A_8, and have for stabilizer a non-maximal subgroup isomorphic to $2^3 : S_4$. Using a result of Neumaier [97] (see also [36]), Haemers [61] gives an elegant geometric connection between PG$(3, 2)$ and the Hoffman-Singleton graph, by taking the points and lines of PG$(3, 2)$ to be the vertices of the graph. Points are mutually non-adjacent; lines are mutually adjacent if and only if the corresponding triples are disjoint. A point is adjacent to a line if and only if they are incident in PG$(3, 2)$.
(iii) Finally, the 30 codewords of minimum weight 7 in $C_{35,6}$ are stabilized by a non-maximal subgroup of S_8 isomorphic to $2^3 : L_3(2)$, while the 105 codewords of minimum weight 8 in $C_{35,5}$ are stabilized by a maximal subgroup of S_8 isomorphic to $2^4 : S_4$.

Remark 8.10. Taking the point set $\mathcal{P}$ to be the 2-subsets of $V_4(2)$, Dempwolff in [50] constructed a design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ where $\mathcal{B} = \{b(\mathcal{L}) \,|\, \mathcal{L} \in \mathcal{P}\}$, with blocks of the form $b(\mathcal{L}) = \{\mathcal{L}\} \cup \{\mathcal{Q} \in \mathcal{P} \,|\, \mathcal{L} \cap \mathcal{Q} = \varnothing\}$. This design has the group S_8 as its full automorphism group, and it is in fact isomorphic to the symmetric 2-$(35, 17, 8)$ design formed by orbiting the image of the union of the orbit of length 1 and 16, i.e., the set $\{\mathfrak{L}\} \cup \Psi$ under S_8. This is also the complementary design of the 2-$(35, 18, 9)$ design described earlier in this section. The design $\mathcal{D}$ is a Hadamard design, and it uniquely extends to a 3-$(36, 18, 8)$ design. The 3-ranks of these designs are 13 and 14 respectively, and their ternary codes were examined in [104].

The rows of the incidence matrix of the 2-$(15, 3, 1)$ design can be used as orthogonal parity checks that allow majority decoding of the code $C_{35,4}$ up to its

full error-correcting capacity. We prove the following

Proposition 8.11. *The code $C_{35,4}$ can correct up to 3 errors by majority decoding.*

Proof: By applying the Rudolph's decoding algorithm [107] to the design 2-$(15, 3, 1)$ we obtain that $\lfloor \frac{r+\lambda-1}{2\lambda} \rfloor = \lfloor \frac{7+1-1}{2\times 1} \rfloor = 3$, and so the result. ■

8.10 The 56-dimensional representation

As for the earlier representations, here we consider n to be a positive integer and Ω a set of size n, and $\Omega^{\{3\}}$ to be the set of all 3-element subsets of Ω. Adopting the terminology of the $\mathbb{ATLAS}$ [34] we call these sets triads, although they are also called triples in [81]. The alternating group A_n where $n \geq 7$ acts primitively as a rank-4 group of degree $\binom{n}{3}$ on the points of $\Omega^{\{3\}}$. The stabilizer of a point $\mathcal{P} = \{a, b, c\}$ is a group isomorphic to $(A_{n-3} \times 3){:}2$, with orbits of lengths 1, $\binom{n-3}{3}$, $3\binom{n-3}{2}$ and $3(n-3)$ respectively. In particular for $n = 8$, we see that A_8 has a unique primitive permutation representation of degree 56 on the cosets of $(A_5 \times 3) : 2$. The orbits of this action have lengths 1, 10, 15 and 30 respectively (see Table 1 and [34]). The elements being permuted in this action are the 56 triads. The permutation module splits into five absolutely irreducible constituents of dimensions 1, 4, 4, 6 and 14 with multiplicities of 2, 1, 1, 3 and 2, and there are only two irreducible submodules, namely of dimensions 1 and 14. Working similarly as in the representations of degrees 15, 28 and 35 above, we get that the permutation module has two maximal submodules of dimensions 42 and 55. From the 42-dimensional submodule we get two non-isomorphic maximal submodules of dimensions 41 and 36 respectively. The 55-dimensional submodule has two maximal submodules, one of dimension 49 and the other of dimension 41, with the latter being isomorphic to the 41-dimensional submodule of the module of dimension 42 found above. Continuing recursively in this manner we get 31 non-isomorphic submodules of dimensions 55, 49, 48, 42, 41, 36, 35, 35, 35, 34, 32, 32, 31, 31, 29, 28, 28, 27, 25, 25, 24, 24, 22, 21, 21, 21, 20, 15, 14, 8 and 7, with the lattice of submodules as depicted in Figure 8.5.

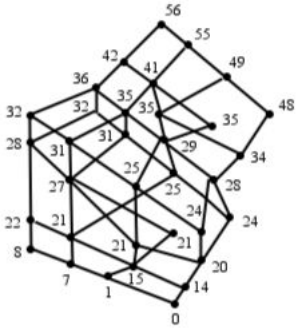


Figure 8.5: Submodule lattice for the 56-dimensional representation

The 32-dimensional submodules give two isomorphic codes, and so do the submodules of dimensions 31, 25, and 24. Thus, in total we obtain twenty-six non-trivial and non-isomorphic codes. In Tables 8.11, 8.12 and 8.13 we give the weight distribution for the codes that contain the all-one vector. In the tables the codes are denoted $C_{56,i}$ and their corresponding duals $C_{56,i}^{\perp}$, with $i = 1, 2, \ldots, 13$. In Tables 8.14, 8.15 and 8.16 we present the codes without the all-one vector.

name	dim	0	4	5	6	7	8	9	10	11	12	13
		56	52		50	49	48	47	46	45	44	43
$C_{56,1}$	7	1										
$C_{56,2}$	8	1										
$C_{56,4}$	15	1										
$C_{56,6}$	21	1					35				280	
$C_{56,7}$	21	1			28				168		490	
$C_{56,8}$	21	1									210	
$C_{56,9}$	22	1								56	210	560
$C_{56,11}$	25	1					35				1120	
$C_{56,12}$	27	1			28		35		588		2240	
$C_{56,13}{}^{\perp}$	28	1			28		35	280	588	1624	2240	7000
$C_{56,12}{}^{\perp}$	29	1					455				15400	
$C_{56,11}{}^{\perp}$	31	1			28		35		3108		37520	
$C_{56,10}{}^{\perp}$	32	1			28	120	35	280	3108	4144	37520	117040
$C_{56,8}{}^{\perp}$	35	1					4235		16800		564480	
$C_{56,7}{}^{\perp}$	35	1	70		560		7315		76272		735980	
$C_{56,6}{}^{\perp}$	35	1			448		1715		49728		538160	
$C_{56,5}{}^{\perp}$	36	1			448	240	1715	2800	49728	109984	538160	1808800
$C_{56,4}{}^{\perp}$	41	1	70		2688		77035		2208640		34062140	
$C_{56,3}{}^{\perp}$	42	1	70	560	2688	12560	77035	457520	2208640	9146256	34062140	115171280
$C_{56,1}{}^{\perp}$	49	1	6020		505232		22206275		556315760		8724879800	

Table 8.11: Codes from the 56-dimensional representation containing the all-ones vector.

name	14	15	16	17	18	19	20	21
	42	41	40	39	38	37	36	35
$C_{56,1}$								
$C_{56,2}$								8
$C_{56,4}$			266				672	
$C_{56,6}$			5201				83104	
$C_{56,7}$	840		5306		12460		46872	
$C_{56,8}$	840		266		7000		64792	
$C_{56,9}$	840	728	266	840	7000	27720	64792	95960
$C_{56,11}$			79121				1450624	
$C_{56,12}$	21980		159761		668780		3381504	
${C_{56,13}}^{\perp}$	21980	51352	159761	357280	668780	1616160	3381504	5051680
${C_{56,12}}^{\perp}$	84480		649061		2956800		12347104	
${C_{56,11}}^{\perp}$	300020		2780561		11067980		52753344	
${C_{56,10}}^{\perp}$	300020	995512	2780561	5819800	11067980	25247040	52753344	80315200
${C_{56,8}}^{\perp}$	6061360		39938241		198847600		744783578	
${C_{56,7}}^{\perp}$	5540000		39662553		202366080		750029056	
${C_{56,6}}^{\perp}$	5476160		39789281		200742080		756458304	
${C_{56,5}}^{\perp}$	5476160	15745072	39789281	93578800	200742080	404154240	756458304	1283739520
${C_{56,4}}^{\perp}$	354062720		2542912057		12957463680		47955156634	
${C_{56,3}}^{\perp}$	354062720	992213488	2542912057	5981538640	12957463680	25917985520	47955156634	82200927200
${C_{56,1}}^{\perp}$	90698577200		650765629745		3317623509200		12275213890940	

Table 8.12: Table 8.11 continued.

Remark 8.12. (i) The code $C_{56,7}$ is part of the family of codes with parameters $[\binom{n}{3}, n, \binom{n-1}{2}]_2$ studied in [81, Theorem 1], and obtained from non-trivial undirected graphs with vertex set $\Omega^{\{3\}}$. The edges of the graphs are defined by the rules that two vertices are adjacent in a graph if and only if they have exactly zero, one or two elements of Ω in common. With the exception of $C_{56,7}$ and its dual all the remaining codes found in this representation are new.

(ii) In this representation we found the following decomposable codes: $C_{56,2} \oplus {C_{56,2}}^{\perp} = \mathbb{F}_2^{56}$, $C_{56,4} = C_{56,3} \oplus \langle \mathbf{1} \rangle$, $C_{56,6} = C_{56,5} \oplus \langle \mathbf{1} \rangle$, $C_{56,7} \oplus {C_{56,7}}^{\perp} = \mathbb{F}_2^{56}$, $C_{56,11} = C_{56,10} \oplus \langle \mathbf{1} \rangle$, ${C_{56,12}}^{\perp} = {C_{56,13}}^{\perp} \oplus \langle \mathbf{1} \rangle$, ${C_{56,8}}^{\perp} = {C_{56,9}}^{\perp} \oplus \langle \mathbf{1} \rangle$ and ${C_{56,1}}^{\perp} = {C_{56,2}}^{\perp} \oplus \langle \mathbf{1} \rangle$.

(iii) The properties of the codes whose weight distributions are listed in Tables 8.11, 8.12, 8.13, 8.14, 8.15, and 8.16 are summarized in Table 8.17. In Table 8.17, the first column gives the parameters of the code, the second, third and fourth columns are true ("yes") if the code is self-orthogonal (s.o.), singly-even (s.e.) or doubly even (d.e.), and false ("no") otherwise. The fifth column gives the structure of the automorphism group. The sixth, seventh and eighth

name	22	23	24	25	26	27	28
	34	33	32	31	30	29	
$C_{56,1}$					28		70
$C_{56,2}$				56	28		70
$C_{56,4}$			9205				12480
$C_{56,6}$			532875				854160
$C_{56,7}$	98840		272965		346416		528380
$C_{56,8}$	117320		251125		333592		546860
$C_{56,9}$	117320	170520	251125	293832	333592	458360	546860
$C_{56,11}$			8146635				14199360
$C_{56,12}$	7030520		18029515		21638232		32351360
${C_{56,13}}^{\perp}$	7030520	11727520	18029515	20693008	21638232	27602960	32351360
${C_{56,12}}^{\perp}$	29944320		69292755		92843520		120603120
${C_{56,11}}^{\perp}$	111765080		291842635		346625832		513131360
${C_{56,10}}^{\perp}$	111765080	188861680	291842635	332235568	346625832	440145440	513131360
${C_{56,8}}^{\perp}$	2048051040		4172993195		6328509152		7279729640
${C_{56,7}}^{\perp}$	2041226880		4157300000		6332396224		73011493760
${C_{56,6}}^{\perp}$	2027795840		4182322795		6288761472		7355866400
${C_{56,5}}^{\perp}$	2027795840	3022186720	4182322795	5317674208	6288761472	7040868800	7355866400
${C_{56,4}}^{\perp}$	130758826240		265841299675		405616141056		466898830280
${C_{56,3}}^{\perp}$	82200927200	193317079200	265841299675	340234799072	405616141056	450742296480	466898830280
${C_{56,1}}^{\perp}$	33477848112800		68047373268875		103850752946528		119510793724560

Table 8.13: Table 8.12 continued.

name	dim	0	4	6	8	10	12	14	16	18
$C_{56,3}$	14	1							210	
$C_{56,5}$	20	1					280		2065	
$C_{56,10}$	24	1					1120		36505	
$C_{56,13}$	28	1			420		6580	41280	327145	1485120
${C_{56,9}}^{\perp}$	34	1			3570		296800	2775200	19785031	101230080
${C_{56,2}}^{\perp}$	48	1	2940	253400	11097730	278187784	4362301300	45349812360	325381240751	1658815478040

Table 8.14: Codes from the 56-dimensional representation without the all-ones vector.

columns are true ("yes") if the code contains the all-ones vector, is optimal or is generated by minimum weight vectors, and false ("no"), otherwise. If the code is generated by minimum weight vectors, or other codewords, then the ninth column gives the 1-$(56, m, \lambda)$ design held by the support of those codewords, and last column gives the number of blocks of the design.

name	20	22	24	26	28	30	32
$C_{56,3}$			5040		6240		4165
$C_{56,5}$	42616		265440		427080		267435
$C_{56,10}$	732256		4066440		7099680		4080195
$C_{56,13}$	6170416	14952000	34648320	46455360	60301560	46388160	34644435
${C_{56,9}}^{\perp}$	375024832	1020557440	2078710620	3166170112	3650746680	3166226112	2078605375
${C_{56,2}}^{\perp}$	6137600058464	16738933866480	34023676352540	51925383202000	59755396862280	51925369744528	34023696916335

Table 8.15: Table 8.14 continued.

name	34	36	38	40	42	44	46	48	50	52
$C_{56,3}$		672		56						
$C_{56,5}$		40488		3136				35		
$C_{56,10}$		718368		42616				35		
$C_{56,13}$	14992320	6176688	1471680	321916	43200	8820		35		
${C_{56,9}}^{\perp}$	1020669440	375004224	101136000	19877522	2764800	267680	16800	665		
${C_{56,2}}^{\perp}$	325384388994	45348764840	4362578500	278127976	11108545	251832	3080	16738914246320	6137613832476	165880

Table 8.16: Table 8.15 continued.

code	s.o.	s.e.	d.e.	aut	**1**	optimal	min words	design	no. of blocks
[56, 7, 26]	no	yes	no	S_8	yes	yes	yes	1-(56, 26, 13)	28
[56, 8, 21]	yes	no	no	S_8	yes	no	yes	1-(56, 21, 3)	8
[56, 14, 16]	yes	yes	yes	S_8	no	no	yes	1-(56, 16, 60)	280
[56, 15, 16]	yes	yes	yes	S_8	yes	no	yes	1-(56, 16, 76)	266
[56, 20, 12]	no	yes	yes	S_8	no	no	yes	1-(56, 12, 60)	280
[56, 21, 8]	no	yes	no	S_8	yes	no	yes	1-(56, 8, 5)	35
[56, 21, 6]	no	yes	no	S_8	yes	no	yes	1-(56, 6, 3)	28
[56, 21, 12]	yes	yes	yes	S_8	yes	no	yes	1-(56, 12, 45)	210
[56, 22, 11]	no	no	no	S_8	yes	no	yes	1-(56, 11, 11)	56
[56, 24, 12]	yes	yes	yes	A_8	no	yes	yes	1-(56, 12, 240)	1120
[56, 25, 8]	yes	yes	yes	A_8	yes	no	no	1-(56, 16, 22606)	79121
[56, 27, 6]	no	yes	no	S_8	yes	no	no	1-(56, 10, 105)	588
[56, 28, 6]	no	no	no	S_8	yes	no	no	1-(56, 9, 45)	280
[56, 28, 8]	no	yes	no	S_8	no	no	yes	1-(56, 8, 60)	420
[56, 29, 8]	no	yes	no	S_8	yes	no	yes	1-(56, 8, 65)	455
[56, 31, 6]	no	yes	no	A_8	yes	no	no	no	
[56, 32, 6]	no	yes	no	A_8	yes	no	no	no	
[56, 34, 8]	no	yes	no	S_8	no	yes	yes	1-(56, 8, 510)	3570
[56, 35, 8]	no	yes	no	S_8	yes	no	yes	1-(56, 8, 605)	4235
[56, 35, 4]	no	yes	no	S_8	yes	no	yes	1-(56, 4, 5)	70
[56, 35, 6]	no	yes	no	S_8	yes	yes	yes	1-(56, 6, 48)	448
[56, 36, 6]	no	no	no	S_8	yes	no	no	no	
[56, 41, 4]	no	yes	no	S_8	yes	no	no	no	
[56, 42, 4]	no	no	no	S_8	yes	no	no	no	
[56, 48, 4]	no	yes	no	S_8	no	yes	yes	1-(56, 4, 210)	2940
[56, 49, 4]	no	yes	no	S_8	yes	yes	yes	1-(56, 4, 430)	6020

Table 8.17: Summary of the properties of the codes

By determining all G-invariant submodules, the number of distinct codes of lengths 28 and 56, obtainable from the 2-modular primitive representations of G is determined. Consequently, the number of self-dual G-invariant codes is also determined. Hence, a combination of the results of Proposition 8.4 and Table 8.17 give a result concerning non-existence of A_8 and S_8-invariant self-dual codes which follows

Proposition 8.13. *There are no self-dual codes of lengths 28 and 56 obtained from the 2-modular primitive representations of A_8 and S_8. Moreover, there is no self-dual doubly-even code of length 56 invariant under A_8 and S_8.*

Chapter 9

Codes from some 2-$(64, 28, 12)$ designs

9.1 Introduction

It was proved by Jungnickel and Tonchev in [71] that there exist four non-isomorphic symmetric 2-$(64, 28, 12)$ designs characterized by symmetric difference property and minimality of their 2-rank. Moreover, these designs have large full automorphism groups, and also large 2-subgroups. In particular, the orders of the full automorphism groups are divisible by 2^6, and their derived 2-$(28, 12, 11)$ quasi-symmetric designs give rise to four inequivalent $[28, 7, 12]_2$ codes. More recently Crnković and Pavčević in [38], constructed 46 non-isomorphic 2-$(64, 28, 12)$ designs for which 2^6 is not a divisor of the order of their full automorphism groups and have in addition shown that none of the derived designs is quasi-symmetric. Thus proving that the said designs are non-isomorphic to those with the same parameters constructed in [71, 98]. Further, according to [[91], Table 11.1, p.38] there are at least 8784 designs with parameters 2-$(64, 28, 12)$ whose derived 2-$(28, 12, 11)$ designs are not quasi-symmetric. In Chapter 8, using modular representation theoretical methods we examined the structure of a $[28, 7, 12]_2$ code invariant under the symplectic group $S_6(2)$. The supports of the codewords of minimum weight 12 in that code give rise to a 2-$(28, 12, 11)$ quasi-

symmetric design which is a derived design of the unique point-primitive and flag-transitive 2-$(64, 28, 12)$ design with automorphism group isomorphic to $2^6{:}S_6(2)$(this is one of four non-isomorphic designs with these parameters constructed in [71, 98]). That study led us to announce in Remark 8.6(iii) the investigation of the binary codes of the class of 46 non-isomorphic 2-$(64, 28, 12)$ designs described above. Hence in this chapter we examine the binary codes defined by the row span of the incidence matrices of the 46 non-isomorphic designs obtained in [38] and prove the following main result:

Theorem 9.1. *Let* $\mathfrak{D}$ *be any of the* 2-$(64, 28, 12)$ *designs given in [38], and* C *the binary code spanned by the row of the incidence matrix of* $\mathfrak{D}$*. Then*
(i) C *is a self-orthogonal, self-complementary and doubly-even code;*
(ii) *the* 2*-rank of* $\mathfrak{D}$ *is either 26 or 27;*
(iii) *if the* 2*-rank of* $\mathfrak{D}$ *is 26, then the minimum weight of* C *is 12 or 16, and the minimum weight of* $C^{\perp}$ *is 8;*
(iv) *if the* 2*-rank of* $\mathfrak{D}$ *is 27, then the minimum weight of* C *is 8, and the minimum weight of* $C^{\perp}$ *is 4, 6 or 8;*
(v) *the automorphism group of* C *is isomorphic to* $\mathrm{Frob}_{21}, \mathrm{Frob}_{21} \times 2$, $\mathrm{Frob}_{21} \times D_8$, $\mathrm{Frob}_{42} \times 2, (\mathrm{Frob}_{42} \times 2){:}2$ *or* $(\mathrm{Frob}_{21} \times D_8){:}2$.

An active area of research in coding theory is the classification of self-orthogonal codes of given length or dimension, see for example [67, 122, 114]. Several methods and techniques are used for this purpose, among which the method of orbit matrices. See Section 9.3 for a brief discussion on this method. In this thesis, using the method of orbit matrices as presented in [39] we completely enumerate and classify the self-orthogonal codes of length 13 (Theorem 9.10) defined by the action of an automorphism of order 4 on the non-fixed parts of the orbit matrices obtained from the 2-$(64, 28, 12)$ designs in discussion. We establish some properties of the codes and the nature of some classes of codewords and observe that the subcodes of codimension 1 are all single weight optimal codes. The proof of Theorem 9.1 follows from a series of lemmas and propositions given in Section 9.2.

Crnković and Pavčević [38] proved the following:

Result 9.2. *(***Crnković & Pavčević***) There are 46 non-isomorphic symmetric* 2-$(64, 28, 12)$ *designs with the Frobenius group of order 21 as an automorphism group; these are given in [38].*

9.2 The binary codes from the 2-$(64, 28, 12)$ designs

Let $\mathfrak{D}_i$ where $1 \leq i \leq 46$ denote any of the 46 symmetric 2-$(64, 28, 12)$ designs given in Result 9.2 (see also [38]). For each $\mathfrak{D}_i$ using Magma [10, 27] we constructed the corresponding codes (dual codes included). Note that given a design and any prime p, the p-ary code of the design is the code over $\mathbb{F}_p$ generated by the rows of the incidence matrix (which are the characteristic functions of the blocks). If A is an incidence matrix of a 2-(v, k, λ) design and $\text{rank}_p(A) < v - 1$, then it is well known that this code is interesting only when p divides $r - \lambda$, the order of the design (see [114, Theorem 1.86]). Moreover, since the order of each design is 16, only the binary codes will be of interest for characterization purposes. Thus, taking the binary row span of the incidence matrix of each design $\mathfrak{D}_i$ we obtain the code C_i of length 64 and determine the weight distribution for each code as listed in Table 9.1. When the context is clear we may omit the subscript i and denote each design by $\mathfrak{D}$ and its corresponding code C. In what follows, we examine the codes of the given designs and hence prove the following:

Proposition 9.3. *Let C be the binary code of the symmetric* 2-$(64, 28, 12)$ *design $\mathfrak{D}$. Then*

(i) *C is self-orthogonal and doubly-even;*

(ii) *C is self-complementary and the* 2*-rank of $\mathfrak{D}$ is either 26 or 27;*

(iii) *$C^{\perp}$ is a singly-even and self-complementary code;*

Proof: For $i \neq j$ consider B_i and B_j two distinct blocks in each $\mathfrak{D}$. Since $|B_i \cap B_j| = 12 \equiv 0 \pmod 2$ and $k = 28 \equiv 0 \pmod 2$, we have that $\mathfrak{D}$ is a self-orthogonal design. Hence the block-point incidence matrix of $\mathfrak{D}$ spans a self-orthogonal code of length 64, and since the spanning vectors have weight divisible by four it follows that C

is doubly-even. The latter assertion also follows readily from Table 9.1, since all the weights are divisible by 4. Since the blocks of $\mathfrak{D}$ are of even size, we have that $\mathbf{1}$ meets evenly every vector of C, so $\mathbf{1} \in C^{\perp}$. Hence $C^{\perp}$ is self-complementary. Moreover, since $\mathfrak{D}$ satisfies $r \equiv \lambda \pmod 4$ and also $r \not\equiv 0 \pmod 8$, we have from [21, Theorem 3(i)] that $\mathbf{1} \in C$, and consequently C is self-complementary, and all weights in $C^{\perp}$ are even. The 2-rank of each design $\mathfrak{D}$, that is, the dimension of each C as it appears listed in Table 9.1 follows from [38, Theorem 2, Theorem 6], and also from computations with Magma [10, 27]. ■

We now examine the codes according to their dimensions and make some observations about their basic properties, in particular the minimum weight, the nature of the minimum words, and the structure of the automorphism groups.

Proposition 9.4. *If the 2-rank of $\mathfrak{D}$ is 26, then the minimum weight of C is 12, except for $i = 6$ when the minimum weight is 16. Furthermore, the minimum weight of $C^{\perp}$ is 8, in all cases.*

Proof: We start by showing that the minimum weight of $C^{\perp}$ is 8. For that let $d^{\perp}$ denote the minimum weight of $C^{\perp}$. Now, $C^{\perp}$ being singly-even implies that $d^{\perp} \equiv 0 \pmod 2$. Moreover, since $C \neq 0$ and $\mathfrak{D}$ satisfies $r \neq 2\lambda$ it follows from [93, Lemma 5] that $d^{\perp} \geq 4$ which excludes codewords of weight 2 in $C^{\perp}$. So we need to show that the minimum $d^{\perp}$ is neither 4 nor 6. Suppose $d^{\perp} \in \{4, 6\}$, then by Theorem 4.10 (see also [66, Theorem 8.4]) any 3 (resp. 5) columns of a parity check matrix H of $C^{\perp}$ are linearly independent, but some 4 (resp. 6) columns are linearly dependent. In each case we verified that this is not possible. Hence $d^{\perp} \geq 8$. Moreover, direct calculations for each code show that the weights of the rows of a generator matrix equals 8; thus $d^{\perp} \leq 8$, and the result follows. Now, we examine the minimum weight d of C. By Proposition 9.3(i) we have that C is doubly-even, so all codewords of C have weight divisible by four, so that $d \geq 4$. But $C \subseteq C^{\perp}$ excludes the possibility of weight 4 codewords in C and we have that $d \geq 8$. However, and once again the earlier argument of the parity check matrix shows that there are no codewords of weight 8 in C. Thus $d(C) = 12$. For the exceptional case when $i = 6$ we used Magma to ascertain the result. ■

Proposition 9.5. *If the 2-rank of $\mathfrak{D}$ is 27, then the minimum weight of C is 8, and the total number of codewords of minimum weight in C equals 1, except for $i = 23$, when there are 29 codewords of minimum weight. The minimum weight of $C^{\perp}$ is 8, except for $i = 8, 9$, when the minimum weight is 4, or $i = 7, 10, 11$, when the minimum weight is 6.*

Proof: With the notation as in Proposition 9.4 we start by showing that $d^{\perp}$ is as stated. Suppose first that $i \in \{8, 9\}$. Again using [93, Lemma 5] we obtain $d^{\perp} \geq 4$. Now, direct calculations for each case show that the weights of the rows of the generator matrix equals 4; thus $d^{\perp} \leq 4$, and so the result. Next consider $i \in \{7, 10, 11\}$. As above we have that $d^{\perp} \geq 4$. Now, suppose that $d^{\perp} = 4$ and argue as follows to get a contradiction. Let p be a fixed point in the support S of a non-zero codeword $w \in C^{\perp}$ of weight $s = d^{\perp}$ and p_l be the number of blocks of the design $\mathfrak{D}$ passing through p and meeting S in l points. A counting argument gives

$$\sum_{l=1}^{k} p_l = r, \ \sum_{l=2}^{k} (l-1)p_l = (s-1)\lambda. \tag{9.1}$$

From Equation (9.1) we obtain

$$\sum_{l=3}^{k} (l-2)p_l = (s-1)\lambda - r, \tag{9.2}$$

and Equations (9.1) and (9.2) imply that $p_2 = r - \sum_{l=3}^{k} p_l \geq r - \sum_{l=3}^{k}(l-2)p_l = r - [(s-1)\lambda - r] = 2r - (s-1)\lambda$. Hence we have $p_2 \geq 56 - 36 = 20$ for any point of S. Now, consider the entries of w. Let $S = \{q_l \,|\, 1 \leq l \leq 4\}$. Notice that every block meeting S in two points and passing through q_1 must pass through another point, say q_4, but there are only three points remaining once q_1 is chosen; thus not all 20 blocks which meet S in two points can pass through q_4; thus we have a contradiction. So that $d \geq 6$. Since the weights of the rows of the generator matrix for $C^{\perp}$ equals 6, it follows that $d^{\perp} \leq 6$, and the assertion follows. Finally, for $i \notin \{7, 8, 9, 10, 11\}$ arguing as in Proposition 9.4 we obtain the desired result. ■

Lemma 9.6. *The automorphism group of C is isomorphic to either* Frob_{21}, $\mathrm{Frob}_{21} \times 2$, $\mathrm{Frob}_{21} \times D_8$, $\mathrm{Frob}_{42} \times 2$, $(\mathrm{Frob}_{42} \times 2){:}2$ *or* $(\mathrm{Frob}_{21} \times D_8){:}2$.

Proof: It follows from [38, Theorem 3, Theorem 5] that if $\mathfrak{D}$ is any of the 46 non-isomorphic 2-$(64, 28, 12)$ designs whose codes are presented in Table 9.1, then $\mathrm{Aut}(\mathfrak{D})$ is $\mathrm{Frob}_{21}, \mathrm{Frob}_{21} \times 2$, $\mathrm{Frob}_{42} \times 2$ or $\mathrm{Frob}_{21} \times D_8$. Furthermore, since the rows of each $\mathfrak{D}$ span the code it is evident that $\mathrm{Aut}(\mathfrak{D}) \subseteq \mathrm{Aut}(C)$. In addition, computations with Magma (see Table 9.1 below) give $|\mathrm{Aut}(\mathfrak{D})| = |\mathrm{Aut}(C)|$ in all cases, except for $i \in \{41, 45, 46\}$. So we have that $\mathrm{Aut}(\mathfrak{D}) = \mathrm{Aut}(C)$. Now, consider $i \in \{41, 45, 46\}$. Notice first that in all cases $[\mathrm{Aut}(C) : \mathrm{Aut}(\mathfrak{D})] = 2$ so that $\mathrm{Aut}(C) = \mathrm{Aut}(\mathfrak{D}) \cdot 2$. In each case we use Magma to ascertain the claims of the lemma. For $i = 41$, computations with Magma show that $\mathrm{Aut}(C)$ contains two normal subgroups, say N and H of orders 21 and 2 respectively, such that $N \cong \mathrm{Frob}_{21}$ and $H \cong \mathbb{Z}_2$, and since $N \cap H = \{1_{\mathrm{Aut}(C)}\}$ and $|\mathrm{Aut}(C)| = |N \cdot H| = 42$ we deduce that $\mathrm{Aut}(C) \cong \mathrm{Frob}_{21} \times 2$ and the result follows. Finally, for $i = 45$ we have that $\mathrm{Aut}(C) \cong (\mathrm{Frob}_{42} \times 2){:}2$, and for $i = 46$ we obtain $\mathrm{Aut}(C) \cong (\mathrm{Frob}_{21} \times D_8){:}2$. ■

Since the all-one vector is always in the code (as the sum of the rows of the incidence matrix), the number of codewords of any weight w equals the number of words of weight $64 - w$. Moreover, all weights are $\equiv 0 \pmod 4$. Therefore only weights up to 32 are listed. In Table 9.1 the first column represents the ordering of the code corresponding to a design (the codes are ordered according to their dimensions), the second column represents the dimension of the code, the third and fourth columns are the orders of the automorphism group of the design and of the code respectively, and the remaining columns list the number of codewords of a given weight w in C. In Table 9.1 we present only the representatives of classes of mutually equivalent codes. The sets of mutually equivalent codes that contain more than one code are $\{2, 3\}$, $\{14, 18, 31, 33\}$, $\{15, 34\}$, $\{17, 30\}$, $\{23, 24\}$, $\{25, 35\}$, $\{26, 28, 36, 38\}$, $\{27, 29, 37, 39\}$, $\{40, 43, 44\}$. Since $\mathbf{1} \in C$, it follows that C is also the code of the complementary 2-$(64, 36, 20)$ design. Moreover, since the codes with the same weight distribution were in all instances equivalent, we can thus state the following

Proposition 9.7. *The binary codes of the 46 non-isomorphic* $(64, 28, 12)$ *designs obtained in [38] can be distinguished by their automorphism groups or by the weight distributions. Up to equivalence there are 30 non-isomorphic binary self-orthogonal*

$\mathfrak{D}_i$	dim	$\lvert\mathrm{Aut}(\mathfrak{D}_i)\rvert$	$\lvert\mathrm{Aut}(C_i)\rvert$	0	8	12	16	20	24	28	32
1	26	21	21	1		98	6888	284858	3652880	16266468	26686478
2	26	21	21	1		77	7154	283465	3656968	16258922	26695690
4	26	21	21	1		63	7294	282835	3658648	16255982	26699218
5	26	21	21	1		112	6804	285040	3652768	16266272	26686870
6	26	21	21	1			7588	282688	3656800	16261568	26691574
7	26	21	21	1		7	7434	283675	3653608	16267742	26683930
8	26	21	21	1		7	7294	284795	3649688	16275582	26674130
9	26	21	21	1		77	7126	283689	3656184	16260490	26693730
10	26	42	42	1		7	7434	283675	3653608	16267742	26683930
11	26	42	42	1		98	7224	282170	3662288	16247652	26709998
12	26	84	84	1		21	7070	286097	3645656	16283226	26664722
13	26	168	168	1		105	6678	286293	3648120	16275778	2667491
14	27	21	21	1	1	161	13916	570381	7300951	32544850	53357206
15	27	21	21	1	1	168	14070	568904	7306383	32533776	53371122
16	27	21	21	1	1	168	14238	567560	7311087	32524368	53382882
17	27	21	21	1	1	140	14350	567644	7309743	32527896	53378178
19	27	21	21	1	1	217	13692	570213	7303639	32537794	53366614
20	27	21	21	1	1	210	15218	569002	7280735	32616068	53255258
21	27	21	21	1	1	217	18060	606949	7225239	32450882	53615030
22	27	21	21	1	1	238	18354	603862	7236831	32427068	53645018
23	27	21	21	1	29	658	14714	564970	7289667	32612484	53252682
25	27	21	21	1	1	126	14322	568358	7306719	32534364	53369946
26	27	21	21	1	1	28	14686	568876	7301231	32548280	53351522
27	27	21	21	1	1	35	14392	570983	7294119	32562294	53334078
32	27	21	21	1	1	168	14238	567560	7311087	32524368	53382882
40	27	42	42	1	1	112	14238	569520	7302127	32543968	53357794
41	27	21	42	1	1	14	14994	566902	7307615	32535932	53366810
42	27	21	21	1	1	28	14630	569324	7299663	32551416	53347602
45	27	84	168	1	1	42	14266	571746	7291711	32566900	53328394
46	27	168	336	1	1	210	13482	572138	7296639	32552004	53348778

Table 9.1: Weight distributions of the binary codes from $(64, 28, 12)$ designs

codes of length 64 obtained from these designs.

Remark 9.8. The binary codes of the residual and derived designs are in all cases the even weight codes of dimensions $[36, 25, 2]_2$ and $[28, 25, 2]_2$ respectively.

9.3 Binary codes from orbit matrices of the 2-$(64, 28, 12)$ designs

We remind the reader that in Section 4.5 we described the method used for the construction of self-orthogonal codes from orbit matrices. Taking $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ to be a 2-(v, k, λ) design and $G \leq \mathrm{Aut}(\mathcal{D})$, we denote the G-orbits of points by $\mathcal{P}_1, \ldots, \mathcal{P}_n$, and the G-orbits of blocks by $\mathcal{B}_1, \ldots, \mathcal{B}_m$, and putting $|\mathcal{P}_j| = \omega_j$, $|\mathcal{B}_i| = \Omega_i$, $1 \leq j \leq n$,

$1 \leq i \leq m$ we define the notion of orbit matrices. Such an orbit matrix is denoted $\mathcal{M}$.

9.4 An automorphism of order 4 acting with 12 fixed points on 2-$(64, 28, 12)$ designs

The following result gives bounds for the number of fixed points of an automorphism of a symmetric design (see [84]).

Result 9.9. *Suppose that a nonidentity automorphism α of a nontrivial symmetric (v, k, λ) design fixes $f(\alpha)$ points. Then $f(\alpha) \leq v - 2n$ and $f(\alpha) \leq \frac{\lambda v}{k-\sqrt{n}}$. Moreover, if equality holds in either inequality, α must be an involution and every non-fixed block contains exactly λ fixed points.*

In the sequel, we apply Result 5.9 to classify self-orthogonal codes constructed from orbit matrices of the 2-$(64, 28, 12)$ designs in discussion and admitting $\mathbb{Z}_4$ as an automorphism. Solving Equations (5.1) and (5.2) we get up to isomorphism 368 orbit matrices for $\mathbb{Z}_4$ acting on a symmetric 2-$(64, 28, 12)$ design with twelve fixed points and thirteen orbits of order 4. Below we give a representative matrix as used in our computations to construct the codes. The block matrix in the bottom right part of this matrix constitutes the non-fixed part of the orbit matrix. The reader will have noticed that this forms a 13×13 matrix, hence the length of the codes examined in Theorem 9.10 below.

The non-fixed parts of the orbit matrices span up to equivalence a unique class of binary self-orthogonal doubly-even codes of length 13. A representative of this class is given by a code with parameters $[13, 3, 4]_2$ and weight enumerator $A(x) = 1 + 3x^4 + 3x^8 + x^{12}$. The automorphism group of this code has order 82944 and is of shape $[(D_8 \times D_8){:}2] \times D_8{:}(3^3{:}3)$.

M	1	1	1	1	1	1	1	1	1	1	1	1	4	4	4	4	4	4	4	4	4	4	4	4
1	1	1	1	1	0	0	0	0	0	0	0	0	4	4	4	4	4	4	0	0	0	0	0	0
1	1	1	1	1	0	0	0	0	0	0	0	0	4	4	0	0	0	0	4	4	4	4	0	0
1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	4	4	0	0	4	4	0	0	4	4
1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	4	4	0	0	4	4	4	4
1	0	0	0	0	1	1	1	1	0	0	0	0	4	4	4	0	0	0	0	0	4	0	4	4
1	0	0	0	0	1	1	1	1	0	0	0	0	4	0	0	4	4	0	4	0	0	4	4	0
1	0	0	0	0	1	1	1	1	0	0	0	0	0	4	0	4	0	4	0	4	0	4	0	4
1	0	0	0	0	1	1	1	1	0	0	0	0	0	0	4	0	4	4	4	4	4	0	0	0
1	0	0	0	0	0	0	0	0	1	1	1	1	4	0	4	0	4	0	0	4	0	4	0	4
1	0	0	0	0	0	0	0	0	1	1	1	1	4	0	0	4	0	4	4	0	4	0	0	4
1	0	0	0	0	0	0	0	0	1	1	1	1	0	4	4	0	0	4	4	0	0	4	4	0
1	0	0	0	0	0	0	0	0	1	1	1	1	0	4	0	4	4	0	0	4	4	0	4	0
4	1	1	0	0	1	1	0	0	1	1	0	0	2	2	1	1	2	2	2	2	1	1	2	2
4	1	1	0	0	1	0	1	0	0	0	1	1	2	1	2	2	1	2	1	2	2	2	2	1
4	1	0	1	0	1	0	0	1	1	0	1	0	1	2	2	2	2	1	2	1	2	2	1	2
4	1	0	1	0	0	1	1	0	0	1	0	1	1	2	2	2	1	2	2	1	2	2	1	2
4	1	0	0	1	0	1	0	1	1	0	0	1	2	1	2	1	2	2	1	2	2	2	2	1
4	1	0	0	1	0	0	1	1	0	1	1	0	2	2	1	2	2	1	2	2	1	1	2	2
4	0	1	1	0	0	1	0	1	0	1	1	0	2	1	2	2	1	2	1	2	2	2	2	1
4	0	1	1	0	0	0	1	1	1	0	0	1	2	2	1	1	2	2	2	2	1	1	2	2
4	0	1	0	1	1	0	0	1	0	1	0	1	1	2	2	2	2	1	2	1	2	2	1	2
4	0	1	0	1	0	1	1	0	1	0	1	0	1	2	2	2	2	1	2	1	2	2	1	2
4	0	0	1	1	1	1	0	0	0	0	1	1	2	2	1	1	2	2	2	2	1	1	2	2
4	0	0	1	1	1	0	1	0	1	1	0	0	2	1	2	2	1	2	1	2	2	2	2	1
4	0	0	0	0	0	0	0	0	0	0	0	0	2	2	2	2	2	2	2	2	2	2	2	4

We thus have the following

Theorem 9.10. *Let $\mathcal{M}$ be any of the 368 orbit matrices for symmetric* 2-$(64, 28, 12)$ *designs under an action of an automorphism group of order 4 with twelve fixed points. The non-fixed parts of $\mathcal{M}$ span up to equivalence a single class of binary self-orthogonal doubly-even* $[13, 3, 4]_2$ *codes of length 13. Moreover, the subcodes of codimension 1 spanned by codewords of weight 8 are optimal doubly-even* $[13, 2, 8]_2$ *codes with weight enumerator* $A(x) = 1 + 3x^8$.

Chapter 10

Modular codes invariant under $S_6(2)$

10.1 Introduction

In Chapters 7 and 8 we characterized all binary codes from the 2-modular representations of the linear groups $L_3(4)$ and $L_4(2)$ respectively. This chapter is motivated by questions raised in Chapters 8 and 9 and by the work of Crnković and Mikulić [40] on designs invariant under the simple symplectic group $S_6(2)$. Through the blend of methods described in Section 6.2.2, and those of Chapters 7 and 8 (see also Chapter 6) we determine and hence describe some of the codes invariant under the symplectic group $S_6(2)$. As in the chapters mentioned above, we have constructed all binary linear codes up to length 135 invariant under the action of the symplectic group $S_6(2)$ through a chain of maximal submodules of the permutation modules induced by the action of the group $S_6(2)$ on $O_6^-(2), O_6^+(2)$, points, $G_2(2)$, isotropic planes, isotropic lines, non-isotropic lines and $S_2(8)$. The submodule lattice of the permutation modules and the weight distribution of the codes obtained from the representations of degrees $28, 36, 63, 120$ and 135 are given. A description of the codes has been given and where possible using the geometry on the objects described above we provide a geometric interpretation of the nature of

the codewords. Moreover, we use the Assmus-Mattson Theorem to determine designs which are held by the codewords of given non-trivial weights in the codes. Due to computer time limitations we did not attempt an exhaustive and inclusive study of the other representations, namely those of degrees $315, 336$ and 960. In this chapter we prove the:

Theorem 10.1. *Let C be a linear binary code of length 28, 36, 63, 120 or 135 invariant under the group $S_6(2)$, then $Aut(C)$ is isomorphic to $S_6(2), O_8^+(2), O_8^+(2) : 2$ or $L_6(2)$ respectively. Up to isomorphism there are 214 non-trivial binary codes obtained from the 2-modular representations of $S_6(2)$, of which 15 are optimal.*

The proof of the theorem follows from a series of propositions in Sections 10.4, 10.5, 10.6, 10.7, and 10.8 respectively.

10.2 The group $S_6(2)$

Below we give a brief overview of the simple symplectic group $G = S_6(2)$ (using the $\mathbb{ATLAS}$ notation) and its maximal subgroups, and primitive permutation representations via the coset action on these subgroups. For more information on the symplectic groups we refer the reader to Section 2.7 (see also [34, p. 60], [118, Section 4.5] or [120]). Let V be an n-dimensional vector space over a finite field $\mathbb{F}$ and f a non-degenerate alternating bilinear form $f : V \times V \longrightarrow \mathbb{F}$ on V. If A_f is the matrix associated with the form f, then the group $Sp(n, \mathbb{F})$ is defined as $Sp(n, \mathbb{F}) = \{T \in GL(n, \mathbb{F}) | T^t A_f T = A_f\}$. The factor group of $Sp(n, \mathbb{F})$ by its center is called the projective special symplectic group and denoted $PSp(n, q)$ or $S_n(q)$ when the group is simple. In terms of matrices the group $Sp(n, q)$ is a subgroup of $GL(n, q)$ consisting of the $n \times n$ matrices P satisfying $P^t AP = A$, where A is a fixed invertible skew-symmetric matrix. The group $PSp(n, q)$ is simple group for all $n \geq 3$ except $PSp(4, 2) \cong S_6$ and when $q = 2$ we have that $PSp_(n, q) \cong Sp_(n, q)$ and hence a subgroup of $GL(n, q)$. The group $S_6(2)$ is isomorphic to the orthogonal group $O_7(2)$, i.e., the group of all 7×7 matrices preserving a non-singular quadratic form. $S_6(2)$

has order 1451520, and it is its own automorphism group. G acts naturally on the points of the projective geometry $PG(5,2)$. It is known that $PG(5,2)$ has 63 points and 651 lines and in addition 315 totally isotropic lines, and 135 totally isotropic planes. G has 8 representations of degree $28, 36, 63, 120, 135, 315, 336$ and 960 (see the $\mathbb{ATLAS}$ [34] or [120]). These representations are shown in Table 10.1: The first column gives the ordering of the primitive representations as given by Magma (or the $\mathbb{ATLAS}$) and as used in our computations; the second gives the degree (the number of cosets of the point stabilizer); the third gives the maximal subgroups; the fourth gives the number of orbits, and the remaining column gives the length of the orbits of the point stabilizer.

no.	degree	Max subgroup	# of orbits	orbit length
1	28	$U_4(2):2$	2	$1, 27$
2	36	S_8	2	$1, 35$
3	63	$2^5 : S_6$	3	$1, 30, 32$
4	120	$U_3(3):2$	3	$1, 56, 63$
5	135	$2^6 : L_3(2)$	4	$1, 14, 56, 64$
6	315	$(2^{1+4} \times 2^2) : (S_3 \times S_3)$	5	$1, 18, 24, 128, 144$
7	336	$S_3 \times S_6$	5	$1, 20, 45, 90, 180$
8	960	$L_2(8):3$	6	$1, 56, 63, 84, 252, 504$

Table 10.1: Maximal subgroups of $S_6(2)$.

We summarize the information obtained from the group and find notations for the objects which are permuted in each of its primitive permutation representations. The primitive representations may also be described (often in several ways, see for example the $\mathbb{ATLAS}$ [34]) in terms of the action of G on various sets of geometrical objects: we shall use the notations $g(m)(m = 28, 36, 63, 120, 135, 315, 336$ and 960, respectively) to denote these sets. We will use names for all objects being permuted in terms of their symplectic notation from the $\mathbb{ATLAS}$, namely $O_6^-(2), O_6^+(2)$, point, $G_2(2)$, isotropic planes, isotropic lines, non-isotropic lines and $S_2(8)$.

10.3 Incidence relations

The rows and columns of Table 10.2 represent the intersection of the objects being permuted as named above. If we denote the entries in Table 10.2 by a_{mn}, then the entry a_{33} corresponds to an intransitive action of an $2^5 : S_6$ on itself with three orbits of lengths 1, 30 and 32 respectively. However the entry a_{73} indicates that there are three orbits of an intransitive action of an $S_3 \times S_6$ on an $2^5{:}S_6$, of length 3, 15 and 45 and the entry a_{47} indicates a transitive action of an $2^6{:}L_3(2)$ on an $S_3 \times S_6$.

Table 10.2: $S_6(2)$-orbits of maximal subgroups on maximal subgroups

	28	36	63	120	135	315	336	960
28	1-27	36	27-36	120	135	45-270	120-216	960
36	28	1-35	28-35	120	30-105	105-210	56-280	960
63	12-16	16-20	1-30-32	120	15120	15-60-240	16-80-240	960
120	28	36	63	1-56-63	63-72	63-252	336	288-672
135	28	8-28	7-56	56-64	1-14-56-64	7-84-224	112-224	64-896
315	4-24	12-24	3-12-48	24-96	3-36-96	1-18-24-128-144	16-48-128-144	192-768
336	10-18	6-30	3-15-45	120	45-90	15-45-120-135	1-20-45-90-180	240-720
960	28	36	63	36-84	9-126	63-252	84-252	1-56-63-84-252-504

We have considered the 2-modular representations of degrees $28, 36, 63, 120$ and 135 and omitted those of degrees $315, 336$ and 960 respectively due to computer time limitations. The sections that follow present the results obtained on these modules.

10.4 The 28-dimensional representation

In its representation on a set $\Omega = \{1, 2, \ldots, 28\}$ the group $S_6(2)$ has for point stabilizer $U_4(2){:}2$ which has two orbits of lengths 1 and 27 respectively. Using the $\mathbb{ATLAS}$ [34], we notice that the constituents being permuted by the group are the 28 symbols (copies of $O_6^-(2)$) of the set Ω. The permutation module splits into three absolutely irreducible constituents of dimension 1, 6 and 14 with multiplicities 2, 2 and 1 respectively. There is only one irreducible submodule of dimension 1. Moreover, the permutation module has only one maximal submodule of dimension 27. In fact the permutation module has only one composition series, namely: $\mathbb{F}_2\Omega = 28 \supseteq 27 \supseteq 21 \supseteq 7 \supseteq 1$.

Figure 10.1: Submodule lattice of the 28-dimensional permutation module

Table 10.3: Weight distribution of the codes from the 28-dimensional representation.

Name	*dim*	0	4	6	8	10	12	14	16	18	20	22	24	28
$C_{28,1}$	7	1					63		63					1
${C_{28,1}}^{\perp}$	21	1	315	6048	47817	206976	472059	630720	472059	206976	47817	6048	315	1

Proposition 10.2. *The code $C_{28,1}$ is self orthogonal and doubly-even, with minimum weight 12. It is a $[28, 7, 12]_2$ code, and its dual ${C_{28,1}}^{\perp}$ is a $[28, 21, 4]_2$ singly even code. $\mathbf{1} \in C_{28,1}$ and $\mathbf{1} \in {C_{28,1}}^{\perp}$. Moreover, $C_{28,1}$, ${C_{28,1}}^{\perp}$ are optimal codes that are generated by their minimum weight codewords. Also* $\mathrm{Aut}(C_{28,1}) \cong S_6(2)$

Proof: See Proposition 8.4(ii).■

Remark 10.3. Note that the code $C_{28,1}$ was discussed in Section 8.7 in connection with codes obtained from the 2-modular representation of A_8. It is worth pointing out that $A_8 \cong O_6^-(2) \leq S_6(2)$. From the $\mathbb{ATLAS}$ [34] we see that the words of minimum weight represent the points of the projective space $PG(5, 2)$ or the isotropic points in the orthogonal space of dimension 7; illustrating yet again the isomorphism between $S_6(2)$ and $\Omega_7^+(2)$. The stabilizer of a point in this action is a group isomorphic to the group $U_4(2) : 2$. The image under $S_6(2)$ of the codewords of minimum weight form a 2-$(28, 12, 11)$ design on which $S_6(2)$ acts primitively. However, the codewords of minimum weight in ${C_{28,1}}^{\perp}$ represent the isotropic lines. The stabilizer of an isotropic line is a group isomorphic to $(2^{1+4} \times 2^2) : (S_3 \times S_3)$. Their minimum words represent the blocks of a 2-$(28, 4, 5)$ design called the Hölz design . For more on this code and design see Remark 8.6 and [40].

10.5 The 36-dimensional representation

Observe that $S_6(2)$ acts two-transitively on the cosets of S_8 (see Table 10.1 and Table 10.2) with orbits of lengths 1, and 35 respectively and we get a permutation representation of degree 36. Hence we form a permutation module of dimension 36 invariant under G. From the $\mathbb{ATLAS}$ [34] the elements being permuted by G are copies of S_8. The permutation module splits into 4 absolutely irreducible constituents of dimensions 1, 6, 8 and 14 with multiplicities of 2, 2, 1 and 1 respectively. There is only one irreducible submodule of dimension 1. Moreover the permutation module has only one maximal submodule of dimension 35. Now, from the 35-dimensional module we get one maximal submodule of dimension 29. From the 29-dimensional module we get two maximal submodules of dimensions 15 and 21. Each of these two modules contains one maximal submodule each of dimension 7 which has in turn one irreducible maximal submodule of dimension 1. We thus find that the permutation module has submodules of dimensions $35, 29, 21, 15, 7$ and 1 and hence obtain 4 non trivial codes of dimensions $7, 15, 21$ and 29. The lattice of the submodules is as shown in Figure 10.2 and the weight distribution given in Table 10.4.

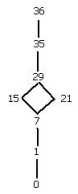


Figure 10.2: Submodule lattice of the 36 dimensional permutation module

Table 10.4: The weight distribution of the codes from a 36-dimensional representation.

Name	dim	0	4	6	8	10	12	14	16	18
		36	32	30	28	26	24	22	20	
$C_{36,1}$	7	1							63	
$C_{36,2}$	15	1			135		945	4320	7623	6720
$C_{36,2}{}^{\perp}$	21	1		336	945	16128	78435	229680	440811	564480
$C_{36,1}{}^{\perp}$	29	1	945	30576	471420	3977568	19541340	59348880	114138486	141852480

Remark: Notice that all the codes are self-complementary and that $C_{36,1}$ is a subcode of all the codes. In addition $C_{36,1}{}^{\perp}$ contains all of them. The containments

amongst the codes is given in Proposition 10.4 and a detailed description of them in Proposition 10.5.

Proposition 10.4. (i) $C_{36,1} \subset C_{36,2} \subset C_{36,1}{}^{\perp}$

(ii) $C_{36,3} \subset C_{36,1}{}^{\perp}$

Proposition 10.5. (i) *The code $C_{36,1}$ is self-orthogonal and doubly-even, with minimum weight 16. It is a $[36, 7, 16]_2$ code, and its dual $C_{36,1}{}^{\perp}$ is a $[36, 29, 4]_2$ singly even code. $\mathbf{1} \in C_{36,1}$ and $\mathbf{1} \in C_{36,1}{}^{\perp}$ with $C_{36,1}$, $C_{36,1}{}^{\perp}$ optimal codes that are generated by their minimum weight codewords. Moreover,* $\mathrm{Aut}(C_{36,1}) \cong S_6(2)$ *and $S_6(2)$ acts irreducibly on $C_{36,1}$.*
(ii) *The code $C_{36,2}$ is singly-even with minimum weight 8. It is a $[36, 15, 8]_2$ code, and its dual $C_{36,2}{}^{\perp}$ is a $[36, 21, 6]_2$ code. Moreover* $\mathrm{Aut}(C_{36,2}) \cong S_6(2)$. *$C_{36,2}$ is a distance 2 from optimal while $C_{36,2}{}^{\perp}$ is near-optimal. Both codes are generated by their minimum weight codewords.*

Proof: (i) $S_6(2)$ acts 2-transitively on the set of co-ordinates of $C_{36,i}$ for $1 \leq i \leq 2$, and so we have that the support of a codeword of any fixed non-zero weight in $C_{36,i}$ yields a 2-design. In particular we can show that the support of the minimum weight codewords yield a 2-$(36, 16, 12)$ design with 63 blocks. We denote this design $\mathcal{D}_{w_{16}}$ and can show that the blocks of $\mathcal{D}_{w_{16}}$ meet in 6 or 8 points. Thus $\mathcal{D}_{w_{16}}$ is a quasi-symmetric design. Now, since in $\mathcal{D}_{w_{16}}$ we have that $|B_i \cap B_j| = \{6, 8\} \equiv 0 \pmod 2$, with B_i and B_j two distinct blocks and $|k| = 16 \equiv 0 \pmod 2$, we have a self-orthogonal design. Thus, the point block incidence matrix of $\mathcal{D}_{w_{16}}$ spans a self-orthogonal code of length 36, which we denote $C_{36,1}$. Since the block size of $\mathcal{D}_{w_{16}}$ is even we have that $\mathbf{1} \in C_{36,1}{}^{\perp}$. Since the code is spanned by its minimum-weight codewords which are divisible by four, it is doubly-even. Notice from Table 10.4 that the weight distribution of $C_{36,1}$ is $A_0 = A_{36} = 1$ and $A_{16} = A_{20} = 63$ and the minimum-weight codewords are the incidence vectors of the blocks of the design and those of weight 20 are the incidence vectors of the blocks of the complementary design. Now, from [98, Theorem 1] or [40, Table 4] we have that $\mathrm{Aut}(\mathcal{D}_{w_{16}}) \cong S_6(2)$. But $\mathrm{Aut}(\mathcal{D}_{w_{16}}) \subseteq \mathrm{Aut}(C_{36,1})$ and $|\mathrm{Aut}(C_{36,1})| = |S_6(2)|$, and

so the result follows. Furthermore, since $r = 28 \neq 2\lambda = 24$ and ${C_{36,1}}^{\perp} \neq 0$ we have that the minimum-weight of ${C_{36,1}}^{\perp}$ is at least 4. From the 2-modular character table of $S_6(2)$ (see[70]) we have that 7 is the smallest dimension for any non-trivial irreducible $\mathbb{F}(2)$-module invariant under $S_6(2)$. Irreducibility now follows easily by using the weight enumerator of the code. The optimality of the codes was found using Magma and verified in the online tables of optimal codes, see [59]. This also follows if we regard $\mathcal{D}_{w_{16}}$ as the residual design of an SDP design. In this way, we obtain a code meeting the Grey-Rankin bound with parameters $(36, 128, 16)$ and of minimum possible 2-rank 7, which is optimal. Finally, since $\mathbf{1} \in C_{36,1}$ it follows that the code of the complementary 2-$(36, 20, 19)$ design is $C_{36,1}$.

(ii) Similarly the support of the codewords of weight 8 in $C_{36,2}$ holds a 2-$(36, 8, 6)$ design D_{w_6} with 135 blocks. The row vectors of the point block incidence matrix of this design generate the code of length 36 denoted $C_{36,2}$ with $\mathrm{Aut}(C_{36,2}) \cong S_6(2)$. Form the online tables of optimal codes we can easily verify that $C_{36,2}$ is a distance 2 from optimal, while ${C_{36,2}}^{\perp}$ is near-optimal. ■

Remark 10.6. (i) The attentive reader will notice that Sections 10.4 and 10.5 uncover the interplay between the designs and codes obtained from the permutation module of dimension 28 and invariant under A_8 examined in Section 8.7 and these of the permutation modules of dimensions 28 and 36 respectively and invariant under $S_6(2)$. It should also become evident to the reader since $A_8 \leq S_6(2)$ this connection is natural. In what follows we attempt to outline an interplay between the codes and designs in a more detailed fashion.

(ii) The designs 2-$(28, 12, 11)$ given in Section 10.4 and $\mathcal{D}_{w_{16}}$ are respectively the derived and the residual designs of a 2-$(64, 28, 12)$ design and they are part of a infinite family of quasi-symmetric designs constructed from the symplectic group $S_{2m}(2)$ and quadratic forms, see Section 8.7 or [40, 98]. These designs are on $v = 2^{2m-1} \pm 2^{m-1}$ points depending on whether we consider hyperbolic or elliptic quadratic forms. Note that the codes $C_{28,1}$ and $C_{36,1}$ are isomorphic as $\mathbb{F}_2$-modules. In Proposition 10.5 we saw that all codes have $S_6(2)$ as their full automorphism group. After a careful examination of Table 10.4 we deduce that the non-zero

weight codewords of the codes $C_{36,i}$ $1 \leq i \leq 3$ are single orbits and are stabilized by maximal subgroups of the automorphism groups. We consider the action of $\mathrm{Aut}(C) = S_6(2)$ on the codewords of minimum weight to describe the nature of the stabilizers and form 2-designs which are invariant under $S_6(2)$. Using this information we then describe the nature of the codewords of minimum weight. So let w_m denote a codeword of a nonzero weight m in $C = C_{36,i}$. If we take $m \in \{16, 8, 6\}$ for $C_{36,i}, 1 \leq i \leq 3$, respectively then from Table 10.4 we see that ${w_m}^{S_6(2)}$ forms a single orbit and so $S_6(2)$ is transitive on code coordinates. From Table 10.4 and the orbit stabilizer theorem we have $[S_6(2):(S_6(2)_{w_m})] \in \{63, 135, 336\}$. This implies that the $(S_6(2))_{w_m} \in \{2^5{:}S_6, 2^6{:}L_3(2), S_3 \times S_6\}$ respectively. Since $S_6(2)$ is transitive on code coordinates, the support of the codewords of the given weights yield the designs $\mathcal{D}_{w_m}$. These are in fact 2-$(36, 16, 12)$, 2-$(36, 8, 6)$, and 2-$(36, 6, 8)$ designs. The number of blocks in the designs equal the indices of $(S_6(2))_{w_m}$ in $(S_6(2)$. We therefore deduce that $S_6(2)$ acts primitively on $\mathcal{D}_{w_m}$.

(iii) Using the above information we can give the geometric interpretation of codewords of minimum weight. From [34], note that codewords of weight 16 in $C_{28,1}$ represent the points of the projective space $PG(5, 2)$ and the stabilizer of a point is a group isomorphic to $2^5{:}S_6$. They are also the blocks of a design $D_{w_{16}}$ with parameters 2-$(36, 16, 12)$. The codewords of weight 8 in $C_{28,2}$ represent the isotropic planes with the stabilizer of an isotropic plane isomorphic to a group $2^6{:}L_3(2)$. Moreover, the image of their support under the action of the group form the blocks of a 2-$(36, 8, 6)$ design. Similarly the codewords of weight 6 in $C_{28,3}$ represent non-isotropic lines with stabilizer a group isomorphic to $S_6 \times S_3$. In addition, the image of the support of the codewords of minimum weight 6 form the blocks of a 2-$(36, 6, 8)$ design. $C_{28,4}$ is the dual of $C_{28,1}$ and so the words of minimum weight can be explained in terms of this relation.

(iv) The designs with parameters 2-$(28, 10, 40)$, 2-$(36, 12, 33)$, and 2-$36, 6, 8)$ where first obtained in [40] using the construction method described in Section 6.2.2. The authors queried in that paper whether or not such designs were known to exist. The 2-$(36, 6, 8)$ design is formed by the ovals of the 2-$(36, 8, 6)$ design, see [40]. Here, we used the codes and the supports of codewords of given non-zero weight

to show yet another way of constructing such designs, and also provide geometric interconnections which uncover the interplay between coding theory and design theory via modular representation theory.

10.6 The 63-dimensional representation

It follows from Theorem 2.32 and it can be also deduced from Tables 10.1 and 10.2 that $S_6(2)$ acts primitively as rank-3 group of degree 63 on the points of the projective geometry $PG(5,2)$. The stabilizer of a point is a group isomorphic to $2^5{:}A_6{:}2 = 2^5{:}S_6$ with orbits of lengths 1, 30 and 32 respectively. It is well known that such an action defines a strongly regular $(63, 30, 13, 15)$ graph. We denote this graph Γ and remark that its complement is a strongly regular $(63, 32, 16, 16)$ graph. The reader should notice that the graph Γ is the symplectic graph $\mathcal{S}_6^+(2)$ given in the proof of Proposition 8.7. We refer the reader to the proof of Proposition 8.7 where the definition of the symplectic graph has first emerged and also connections are established with what is know as the triangle and co-triangle properties, see also [62]. Using this action a permutation module of dimension 63 is formed. Moreover from the ATLAS [34] we can identify the elements being permuted by the group as being the points of the projective geometry. The permutation module splits into four absolutely irreducible constituents of dimension 1, 6, 8 and 14 with multiplicities of 3, 4, 1 and 2 respectively. We found that there are two irreducible submodules of dimension 1 and 6 both absolutely irreducible in this module. Moreover, the 63-dimensional permutation module has two maximal submodules of dimension 57 and 62. Now, from the 57-dimensional module we get four non-isomorphic maximal submodules of dimension $43, 56, 56, 56$, and from the 62-dimensional module we get one maximal submodule of dimension 56 which is isomorphic to the third of the 56-dimensional submodules. From the 43-dimensional submodule we get three non-isomorphic maximal submodules each of dimension 42. From each of the 56-dimensional submodules we get two maximal submodules, one of dimension 42 and the other of dimension 55. The three 55-dimensional submodules

are all isomorphic. We find that the three 42-dimensional submodules are all non-isomorphic, although being each isomorphic to a 42-dimensional submodule obtained from the 43-dimensional submodule. We now have four maximal submodules each of dimension $42, 42, 42$ and 55. From each of these, we get one maximal submodule of dimension 41 and in addition we get another maximal submodule of dimension 36 from the third 42-dimensional submodule. Analogous to the representations of degrees 28 and 36, using Meat-Axe we worked recursively through the chain of submodules of the permutation module and filtered out isomorphic copies of maximal submodules. In doing so, we determined a total of 27 submodules of dimensions 1, 6, 7, 7, 7, 8, 20, 21, 21, 21, 22, 27, 28, 35, 36, 41, 42, 42, 42, 43, 55, 56, 56, 56, 57, 62 and 63 respectively. The lattice of submodules is as shown in Figure 10.3. We obtain a total of 24 non-trivial binary codes of dimensions $6, 7, 7, 7, 8, 20, 21, 21, 21, 22, 27, 28, 35, 36, 41, 42, 42, 42, 43, 55, 56, 56, 56$ and 57 respectively. These codes and their duals will be denoted $C_{63,i}$ and $C_{63,i}{}^{\perp}$, with $1 \leq i \leq 12$ in an increasing order of their dimension. The weight distributions of the codes and those of their duals are given in Tables 10.5 and 10.7 respectively. We note that in Table 10.7 we give only a partial listing of the weight distribution of the duals, since the weights are too large.

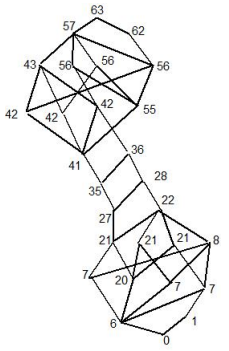


Figure 10.3: Submodule lattice of the 63-dimensional permutation module

Table 10.5: The weight distribution of the codes from a 63-dimensional representation.

Name	dim	0	11	12	15	16	19	20	23	24	27	28	31
$C_{63,1}$	6	1											
$C_{63,2}$	7	1										36	
$C_{63,3}$	7	1									28		
$C_{63,4}$	7	1											63
$C_{63,5}$	8	1									28	36	63
$C_{63,6}$	20	1				945				91560		248832	
$C_{63,7}$	21	1				1953				182280		499968	
$C_{63,8}$	21	1			336	945			54432	91560	195328	248832	455616
$C_{63,9}$	21	1			315	945			54936	91560	193536	248832	458451
$C_{63,10}$	22	1			651	1953			109368	182280	388864	499968	914067
$C_{63,11}$	27	1		1638		20097		749826		9274440		36318492	
$C_{63,12}$	28	1	378	1638	6699	20097	340830	749826	5564664	9274440	28247716	36318492	53692947

Table 10.6: Table 10.5 continued.

dim	32	35	36	39	40	43	44	47	48	51	52	63
6	63											
7	63		28									
7	63	36										
7	63											1
8	63	36	28									1
20	458451		193536		54936				315			
21	914067		388864		109368				651			
21	458451	251136	193536	90720	54936			1008	315			
21	458451	248832	193536	91560	54936			945	315			1
22	914067	499968	388864	182280	109368			1953	651			1
27	53692947		28247716		5564664		340830		6699		378	
28	53692947	36318492	28247716	9274440	5564664	749826	340830	20097	6699	1638	378	1

Table 10.7: Partial listing of the weight distribution of the dual of codes of length 63

Name	dim	0	3	4	5	6	7	8	9	10	11	12
$C_{63,12}{}^{\perp}$	35	1						945				26208
$C_{63,11}{}^{\perp}$	36	1					135	945			6048	26208
$C_{63,10}{}^{\perp}$	41	1						9765				1421784
$C_{63,9}{}^{\perp}$	42	1						11781		60480		2697240
$C_{63,8}{}^{\perp}$	42	1					288	9765	11200		294336	1421784
$C_{63,7}{}^{\perp}$	42	1					1395	9765			328104	1421784
$C_{63,6}{}^{\perp}$	43	1					1683	11781	11200	60480	622440	2697240
$C_{63,5}{}^{\perp}$	55	1		4725		531048		30252537		998505144	20847008637	
$C_{63,4}{}^{\perp}$	56	1		9765		1057224		60544953		1996794072		41694856749
$C_{63,3}{}^{\perp}$	56	1	336	4725	54432	531048	4327488	30252537	184868320	998505144	4811041872	20847008637
$C_{63,2}{}^{\perp}$	56	1	315	4725	54936	531048	4321791	30252537	184908360	998505144	4810848147	20847008637
$C_{63,1}{}^{\perp}$	57	1	651	9765	109368	1057224	8649279	60544953	369776680	1996794072	9621890019	41694856749

Table 10.8: Table 10.7 continued

Dim	14	...	52	53	54	55	56	57	58	59	60	63
35	216000	...	6048				135					
36	216000	...	6048			945	135					1
41	17856000	...	328104				1395					
42	35668800	...	622440		11200		1683					
42	17856000	...	328104	60480		2016	1395					
42	17856000	...	328104			9765	1395					1
43	35668800	...	622440	60480	11200	11781						1
55	292087911600	...	4810848147		184908360		4321791		54936		315	
56	584173436400	...	9621890019		369776680		8649279		109368		651	
56	292087911600	...	4810848147	998288928	184908360	30292416	4321791	526176	54936	5040	315	
56	292087911600	...	4810848147	998505144	184908360	30252537	4321791	531048	54936	4725	315	1
57	584173436400	...	9621890019	1996794072	369776680	60544953	8649279	1057224	109368	9765	651	1

Remark 10.7. Using Theorem 3.27 (see Jordan-Hölder Theorem) we deduce that the codes above are related as shown in the following proposition. We note that $C_{63,1}$ is a subcode of all these codes while ${C_{63,1}}^{\perp}$ contains all of them. Some obvious and interesting properties of these codes can be deduced from their weight distributions. In Proposition 10.8 we show the containment of the codes and in Proposition 10.9, we collect their properties.

Proposition 10.8. (i) $C_{63,6} \subset C_{63,7}$;

(ii) $C_{63,6} \subset C_{63,8}$;

(iii) ${C_{63,7}}^{\perp} \subset {C_{63,6}}^{\perp}$;

(iv) $C_{63,1} \subset C_{63,2} \subset C_{63,5}$;

(v) $C_{63,1} \subset C_{63,6} \subset C_{63,9} \subset C_{63,10}$;

(vi) $C_{63,2} \subset {C_{63,5}}^{\perp} \subset {C_{63,3}}^{\perp} \subset {C_{63,1}}^{\perp}$;

(vii) $C_{63,2} \subset {C_{63,10}}^{\perp} \subset {C_{63,7}}^{\perp} \subset {C_{63,4}}^{\perp} \subset {C_{63,1}}^{\perp}$;

(viii) $C_{63,1} \subset C_{63,3} \subset C_{63,5} \subset C_{63,10} \subset C_{63,12} \subset {C_{63,11}}^{\perp} \subset {C_{63,9}}^{\perp} \subset {C_{63,1}}^{\perp}$.

Proposition 10.9. (i) *The code $C_{63,1}$ is self orthogonal and optimal $[63, 6, 32]_2$ code and its dual ${C_{63,1}}^{\perp}$ is a $[63, 57, 3]_2$ optimal code. Moreover,* $\mathrm{Aut}(C_{63,1}) \cong S_6(2)$ *and $S_6(2)$ acts irreducibly on $C_{63,1}$ as an $\mathbb{F}_2$-module;*

(ii) *The codes* $C_{63,i}$ *for* $i \in \{4,5,9,10,11,12\}$ *and* ${C_{63,i}}^{\perp}$ *for* $i \in \{1,2,6,7,11\}$ *are self-complementary;*

(iii) *The codes* $C_{63,i}$ *for* $i \in \{1,2,6,7,11\}$ *are doubly-even and self-orthogonal. The codes* $C_{63,i}$ *for* $i \in \{1,2,6,7,11\}$ *and* ${C_{63,i}}^{\perp}$ *for* $i \in \{5,6,12\}$ *are singly even;*

(iv) *The codes* $C_{63,i}$ *where* $i \in \{1,4\}$ *and* ${C_{63,i}}^{\perp}$ *for* $i \in \{1,4,5,9,10\}$ *are optimal. Furthermore the codes* $C_{63,5}$ *and* ${C_{63,i}}^{\perp}$ *for* $i \in \{2,3,6,7\}$ *are near-optimal;*

(v) $C_{63,i}$ *for* $i \in \{4,9,10,12\}$ *are decomposable* $\mathbb{F}_2$*-modules;*

(vi) *The automorphism group of* $C_{63,i}$ *for* $i \in \{1,4,7,10\}$ *is* $L_6(2)$ *and the automorphism group of* $C_{63,i}$ *for* $i \in \{2,3,5,6,8,9,11,12\}$ *is* $S_6(2)$*. Moreover,* $L(6,2)$ *acts irreducibly on* $C_{63,1}$ *as an* $\mathbb{F}_2$*-module.*

Proof: (i) Notice from Table 10.5 that $C_{63,1} = [63,6,32]$ is a one weight code with all codewords of weight 32 and so, doubly even. Moreover, the support of the codewords of minimum weight in $C_{63,1}$ yield a symmetric 2-$(63,32,16)$ design which we denote $\mathfrak{D}$. Now $\mathrm{Aut}(\mathfrak{D}) \subseteq \mathrm{Aut}(C_{63,1})$. The complement ($\bar{\mathfrak{D}}$) of this design is a 2-$(63,31,15)$ symmetric designs of points and hyperplanes of the projective geometry $PG(5,2)$, and so by Theorem 4.26 we have that the automorphism group of these designs is $P\Gamma L_6(2)$. In addition a straightforward calculation gives that the order $|\mathrm{Aut}(\mathfrak{D})| = 20158709760 = |\mathrm{Aut}(C_{63,1})|$, so we have $\mathrm{Aut}(C_{63,1}) \cong P\Gamma L_6(2)$. Irreducibility and invariance of the code follows analogously the arguments used in the earlier instances. Optimality is easily verifiable through Magma or by consulting the online table of optimal codes [59].

(ii) That the codes are are self-complementary follows readily from Tables 10.5 and 10.6.

(iii) Arguing similarly as in the proof of Proposition 10.5(ii) we have that in all but $C_{63,5}$, the codes are spanned by their minimum weight codewords. The blocks sizes of the designs supported by minimum-weight codewords in the codes $C_{63,i}$, where $i \in \{2,6,7,11\}$ have sizes $28, 16, 16$ and 12 respectively. Since these are all $\equiv 0 \pmod 4$ we deduce that the corresponding codes are doubly even and hence

self-orthogonal. In fact, for $i = 1$ or 2 we have that $\dim(C_{63,i}) = \dim \mathrm{Hull}(C_{63,i})$ which shows yet again that the two codes are self-orthogonal and doubly-even. Consequently we have that $\mathbf{1} \in C^{\perp}{}_{63,i}$ for $i \in \{1, 2, 6, 7, 11\}$.

(iv) For the automorphism groups, we use the facts established in Proposition 10.8 as well as the following inclusions: The codewords of weight 4 in $C_{63,12}$ form a subcode equivalent to $C_{63,11}$. Similarly codewords of weight 4 in $C_{63,10}$ form a subcode isomorphic to $C_{63,7}$ and finally $C_{63,6}$ is the code formed by weight 4 codewords of $C_{63,9}$. Furthermore, we have that $C_{63,9} = C_{63,6} \oplus \langle \mathbf{1} \rangle$, $C_{63,10} = C_{63,7} \oplus \langle \mathbf{1} \rangle$ and $C_{63,12} = C_{63,11} \oplus \langle \mathbf{1} \rangle$. Also $C_{63,5} = C_{63,3} \oplus \langle \mathbf{1} \rangle$, $C_{63,5} = C_{63,2} \oplus \langle \mathbf{1} \rangle$, $C_{63,4} = c_{63,1} \oplus \langle \mathbf{1} \rangle$, and $C_{63,10} = C_{63,8} \oplus \langle \mathbf{1} \rangle$. From this we deduce that the codes $C_{63,4}, C_{63,5}, C_{63,9}, C_{63,10}$ and $C_{63,12}$ are all decomposable $\mathbb{F}_2$-modules. Now, if $\alpha \in \mathrm{Aut}(C_{63,6})$ then since $\alpha(\mathbf{1}) = \mathbf{1}$ and $C_{63,9} = C_{63,6} \oplus \langle \mathbf{1} \rangle$ then $\alpha \in \mathrm{Aut}(C_{63,9})$ and so $\mathrm{Aut}C_(63, 6) \subseteq \mathrm{Aut}(C_{63,9})$. Similarly $\mathrm{Aut}(C_{63,1}) \subseteq \mathrm{Aut}(C_{63,4})$, $\mathrm{Aut}(C_{63,2}) \subseteq \mathrm{Aut}(C_{63,5})$, $\mathrm{Aut}(C_{63,11}) \subseteq \mathrm{Aut}(C_{63,12})$, $\mathrm{Aut}(C_{63,7}) \subseteq \mathrm{Aut}(C_{63,10})$ and $\mathrm{Aut}(C_{63,3}) \subseteq \mathrm{Aut}(C_{63,5})$. Finally, computation with Magma show that $|\mathrm{Aut}(C_{63,3})| = 1451520 = |\mathrm{Aut}(C_{63,5})| = |\mathrm{Aut}(C_{63,2})|$ and hence their automorphism groups are isomorphic. In view of the above information we have that the codes $(C_{63,i})$ for i in each of the sets $\{1, 4\}, \{2, 3, 5\}, \{6, 9\}, \{7, 10\}, \{11, 12\}$ and $\{8\}$ have the same automorphism group. We need simply prove that the automorphism groups for $(C_{63,i})$, where $i \in \{2, 6, 7, 8, 11\}$ are as claimed. From part (i) we have $\mathrm{Aut}(C_{63,4}) = L_6(2)$. That $\mathrm{Aut}(C_{63,7}) = L_6(2)$ follows from the fact that the automorphism group of the code is equal to the automorphism group of its dual and by using Proposition 10.8 and the orders of the groups. Further, by construction $S_6(2) \subseteq \mathrm{Aut}(C_{63,i})$ and from computations with Magma we have for $i \in \{2, 6, 8, 11\}$ that $|\mathrm{Aut}(C_{63,i})| = 1451520 = |S_6(2)|$. We thus conclude that $\mathrm{Aut}(C_{63,i}) = S_6(2)$ for $i = 2, 6, 8$, and 11. ■

10.6.1 Stabilizer in $\mathrm{Aut}(C)$ of a word w_i in a code C

We examine the action of $\mathrm{Aut}(C) = S_6(2)$ or $\mathrm{Aut}(C) = L_6(2)$ on the set W_m of non-trivial codewords of C and describe their nature. In addition, we look at the structure of the stabilizers $(\mathrm{Aut}(C))_{w_m}$ where $m \in M$ where M is defined as follows: Consider

$M = \{27, 28, 31, 32, 35, 36\}$ for codes $C = C_{63,i}$, $1 \leq i \leq 5$ and $M = \{15, 48\}$ for the codes $C = C_{63,i}$, $6 \leq i \leq 10$. For $m \in M$ we define $W_m = \{w_m \in C_{63,i} | \mathrm{wt}(w_m) = m\}$. In Lemma 10.10 we show that for all $m \in M$, the stabilizer $(\mathrm{Aut}(C))_{w_m} = H$ where $H < \mathrm{Aut}(C)$ is a maximal subgroup of $\mathrm{Aut}(C)$: In addition, for $w_m \in W_m$ we take image of the support of w_m under the action of $G = S_6(2)$ or $G = L_6(2)$ to form the blocks of a t-$(63, m, k_m)$ ($t \in \{1, 2\}$) designs $\mathcal{D} = \mathcal{D}_{w_m}$, where $k_m = |(w_m)^G| \times \frac{m}{63}$ and show that $\mathrm{Aut}(C)$ acts primitively on $\mathcal{D}_{w_m}$. Information on these designs is given in Table 10.10.

Lemma 10.10. *Let $C = C_{63,i}$, $1 \leq i \leq 5$ be a code as in Proposition 10.9 and $0 \neq w \in C$. Then $\mathrm{Aut}(C)_{w_m}$ is a maximal subgroup of $\mathrm{Aut}(C)$. Moreover, the design $\mathcal{D}$ obtained by orbiting the images of the support of any non-trivial codeword in C is primitive.*

Proof: Follows similar arguments to those used in the proof of Lemma 8.5. ■

If we consider the action of $\mathrm{Aut}(C) = L_6(2)$ on the codewords of the codes $C = C_{63,i}$, $i \in \{6, 7, 8\}$ of weight $m \in M$ with $M = \{27, 28, 31, 32, 35, 36\}$, it is found that $\mathrm{Aut}(C)$ splits W_m into several orbits of different length where each may have a different subgroup as stabilizers. In some cases the stabilizer is maximal and in others it is not. For example $\mathrm{Aut}(\mathrm{C}_{63,6})$ acting on codewords of weight 32 splits these words into 9 orbits of length $181440, 90720(2), 60840, 15120, 3780, 6048, 10080$ and 23040 and only acts primitively on the 9-th orbit. This fact is indicated by writing $(32_6)_9$ in the Table 10.9 and Table 10.10. In Table 10.9 the first column gives the codes $C_{63,i}$, the second column represents the codewords of weight m (the sub-indices of m represent the code from where the codeword is drawn), the third column gives the structure of the stabilizers in $\mathrm{Aut}(C)$ of a codeword w_m and the last column, tests the maximality $(\mathrm{Aut}(C))_{w_m}$. In Table 10.10 the first column represents the codewords of weight m and the second column gives the parameters of the t-designs $\mathcal{D}_{w_m}$ as defined in Section 10.6.1. In the third column we list the number of blocks of $\mathcal{D}_{w_m}$. The final column shows whether or not a design $\mathcal{D}_{w_m}$ is primitive under the action of $\mathrm{Aut}(C)$.

Table 10.9: Stabilizer in Aut(C) of a codeword w_m

C	m	$(\mathrm{Aut})_{w_m}$	Maximal	C	m	$(\mathrm{Aut})_{w_m}$	Maximal
$C_{63,8}$	15_8	$(S_3 \times S_3) : 2^7$	Yes	$C_{63,5}$	32_5	$2^5 : S_6$	Yes
$C_{63,9}$	15_9	$(S_3 \times S_3) : 2^7$	Yes	$C_{63,6}$	$(32_6)_9$	$2^5 : S_6$	Yes
$C_{63,10}$	15_{10}	$(S_3 \times S_3) : 2^7$	Yes	$C_{63,7}$	$(32_7)_3$	$2^5 : L_5(2)$	Yes
$C_{63,3}$	27_3	$2 : S_4(3)$	Yes	$C_{63,8}$	$(32_8)_9$	$2^5 : S_6$	Yes
$C_{63,5}$	27_5	$2 : S_4(3)$	Yes	$C_{63,9}$	$(32_9)_9$	$2^5 : S_6$	Yes
$C_{63,8}$	$(27_8)_6$	$2 : S_4(3)$	Yes	$C_{63,10}$	$(32_{10})_3$	$2^5 : L_5(2)$	Yes
$C_{63,2}$	28_2	S_8	Yes	$C_{63,3}$	35_3	S_8	Yes
$C_{63,5}$	28_5	S_8	Yes	$C_{63,5}$	35_5	S_8	Yes
$C_{63,4}$	31_4	$2^5 : L_5(2)$	Yes	$C_{63,8}$	$(35_8)_6$	S_8	Yes
$C_{63,5}$	31_5	$2^5 : S_6$	Yes	$C_{63,3}$	36_2	$2 : S_4(3)$	Yes
$C_{63,9}$	$(31_9)_9$	$2^5 : S_6$	Yes	$C_{63,5}$	36_5	$2 : S_4(3)$	Yes
$C_{63,10}$	$(31_{10})_3$	$2^5 : L_5(2)$	Yes	$C_{63,6}$	48_6	$(S_3 \times S_3) : 2^7$	Yes
$C_{63,1}$	32_1	$2^5 : L_5(2)$	Yes	$C_{63,7}$	48_7	$(S_3 \times S_3) : 2^7$	Yes
$C_{63,2}$	32_2	$2^5 : S_6$	Yes	$C_{63,8}$	48_8	$(S_3 \times S_3) : 2^7$	Yes
$C_{63,3}$	32_3	$2^5 : S_6$	Yes	$C_{63,9}$	48_9	$(S_3 \times S_3) : 2^7$	Yes
$C_{63,4}$	32_4	$2^5 : L_5(2)$	Yes	$C_{63,10}$	48_{10}	$(S_3 \times S_3) : 2^7$	Yes

Table 10.10: Primitive t-designs $\mathcal{D}_{w_m}$ invariant under Aut(C)

m	$\mathcal{D}_{w_{(m)}}$	No of blocks	$Prim$	m	$\mathcal{D}_{w_{(m)}}$	No of blocks	$Prim$
15_8	1-(63, 15, 80)	336	Yes	32_5	1-(63, 32, 32)	63	Yes
15_9	1-(63, 15, 75)	315	Yes	32_6	1-(63, 32, 32)	63	Yes
15_{10}	2-(63, 15, 35)	651	Yes	32_7	1-(63, 32, 32)	63	Yes
27_3	1-(63, 27, 12)	28	Yes	32_8	1-(63, 32, 32)	63	Yes
27_5	1-(63, 27, 12)	28	Yes	32_9	1-(63, 32, 32)	63	Yes
27_8	1-(63, 27, 12)	28	Yes	32_{10}	1-(63, 32, 32)	63	Yes
28_2	1-(63, 28, 16)	36	Yes	35_3	1-(63, 35, 20)	36	Yes
28_5	1-(63, 28, 16)	36	Yes	35_5	1-(63, 35, 20)	36	Yes
31_4	2-(63, 31, 31)	63	Yes	35_8	1-(63, 35, 20)	36	Yes
31_5	1-(63, 31, 31)	63	Yes	36_2	1-(63, 36, 16)	28	Yes
31_9	1-(63, 31, 31)	63	Yes	36_5	1-(63, 36, 16)	28	Yes
31_{10}	1-(63, 31, 31)	63	Yes	48_6	1-(63, 48, 240)	315	Yes
32_1	2-(63, 32, 32)	63	Yes	48_7	1-(63, 48, 96)	651	Yes
32_2	1-(63, 32, 32)	63	Yes	48_8	1-(63, 48, 240)	315	Yes
32_3	1-(63, 32, 32)	63	Yes	48_9	1-(63, 48, 240)	315	Yes
32_4	2-(63, 32, 32)	63	Yes	48_{10}	2-(63, 48, 376)	651	Yes

Remark 10.11. (i) Γ is a strongly regular $(63, 32, 16, 16)$ graph, that is equivalent to a symmetric 2-$(63, 32, 16)$ design which we denote $\mathcal{D}$. The code $C_{63,1}$ of this design is a constant weight code, i.e., a code in which all non-zero codewords have same weight. The complement $\bar{\Gamma}$ is a strongly regular $(63, 30, 13, 15)$ graph isomorphic to the symplectic graph $\mathcal{S}_6^+(2)$. Γ satisfies the triangle property and is uniquely determined by the minimality of its 2-rank which is 6. Notice though that $C_{63,1}$ code is the simplex code of dimension 6 and its dual $C_{63,1}^{\perp}$ is the Hamming code H_6, see [66, 4]. The complement of $\mathcal{D}$ is the symmetric 2-$(63, 31, 15)$ design $\bar{D}$ of points and hyperplanes of the projective geometry $PG(5, 2)$. $\mathcal{D}$ is also a Hadamard design and so extendible to a 3-$(64, 32, 15)$ design [26]. The code of $\mathcal{D}$ is $C_{63,4} = C_{63,1} \oplus \langle \mathbf{1} \rangle$. These designs and codes are well known and their automorphism group is $PGL(6, 2) \cong L_6(2)$ by the fundamental theorem of projective geometry.
(ii) The words of minimum weight in $C_{63,1}^{\perp}$ can also be explained geometrically: The image under $\mathrm{Aut}(C_{63,4})$ of the support of the codewords of minimum weight define a Steiner 2-$(63, 3, 1)$ triple system which we denote $STS(63)$. The 651 vectors of minimum weight generate $C_{63,1}^{\perp}$. Notice that $STS(63)$ is the design of points and lines in the $PG(5, 2)$. It is a quasi-symmetric design with block intersecting in 0 and 1 points. It follows from [110] that the block graph of $STS(63)$ is a strongly regular $(651, 90, 33, 9)$ graph complemented by a strongly regular $(651, 560, 478, 504)$ graph.
(iii) Lemma 10.10 can be of use to help provide a geometric interpretation to the words of minimum weight in the codes examined. The words of the weight 27 in $C_{63,3}$ and $C_{63,5}$ represent copies of $O_6^-(2)$ or the minus hyperplane in the orthogonal space. The stabilizer is a group isomorphic to $U_4(2) : 2$ and the primitivity of the action has been illustrated. Words of weight 28 in $C_{63,2}$ and $C_{63,5}$ represent copies of an $O_6^+(2)$ or a plus hyperplane in the orthogonal space. Codewords of weight 31 in $C_{63,4}$ and $C_{63,5}$ and weight 32 for $C_{63,i}, i \in \{1, 2, 3, 4, 5\}$ represent the points of $PG(5, 2)$ or the isotropic points of the orthogonal space. They also represent the rows of the adjacency matrix of Γ or equivalently the incidence vectors of the blocks of a 2-$(63, 31, 15)$ symmetric design of points and hyperplanes of $PG(5, 2)$. The set of codewords of weight 15 in $C_{63,8}$ represent non-isotropic lines, of weight 15 in $C_{63,9}$ represent isotropic lines and of weight 15 in $C_{63,10}$ the lines of $PG(5, 2)$.

10.7 The 120-dimensional representation

Notice that $S_6(2)$ acts primitively as a rank-3 group of degree 120 on the cosets of $U_3(3) : 2$ with orbits of lengths 1, 56 and 63. The action defines a strongly regular $(120, 56, 28, 24)$ graph, complemented by a strongly regular $(120, 63, 30, 37)$ graph. These graphs are in the class of the graphs partitioned by the symplectic graph and denoted N_{2n}^- where $n = 4$, see [62]. The points permuted in this action are copies of $G_2(2)$, see $\mathbb{ATLAS}$ [34]. The permutation module splits into five absolutely irreducible constituents of dimension 1 6, 8 14 and 48 with multiplicities of 4, 4, 2, 2 and 1 respectively. There are 2 irreducible submodules of dimension 1 and 8 both absolutely irreducible. Working through the chain of submodules of the permutation module we obtain in total 14 submodules of dimensions $119, 112, 111, 105, 91, 85, 84, 36, 35, 29, 15, 9, 8$ and 1, and hence binary codes of same dimensions. The lattice diagram is given in figure 10.4 and their weight distributions are given in the Table 10.11 and Table 10.11.

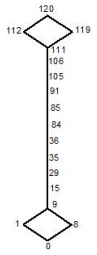


Figure 10.4: Submodule lattice of the 120-dimensional representation

Table 10.11: The weight distribution of the codes from a 120-dimensional representation.

Name	Dim	0	56	64
$C_{120,1}$	8	1	120	135

Table 10.12: Table 10.11 continued.

Name	Dim	0	24	28	32	36	40	44	48	52	56	60
		120	96	92	88	84	80	76	72	68	64	
$C_{120,2}$	9	1									255	
$C_{120,3}$	15	1					378		630		15375	
$C_{120,4}$	29	1	315		945	20160	119448	2459520	12133800	62233920	102040275	178854144
$C_{120,5}$	35	1	5355		16065	1370880	8096760	145313280	884003400	3566142720	7413648915	10322543616
$C_{120,6}$	36	1	5355	16320	16065	3089920	14676984	289255680	1794267720	7041968640	14999707155	20433469056

Proposition 10.12. (i) *The code $C_{120,1}$ is a $[120, 8, 56]_2$ self-orthogonal, doubly-even and projective code. Its dual ${C_{120,1}}^{\perp}$ is a $[120, 112, 3]_2$ singly even and uniformly packed. ${C_{120,1}}^{\perp}$ is a near-optimal code. Moreover,* $\mathrm{Aut}(C_{120,1}) \cong O_8^+(2) : 2$ *and acts irreducibly on $C_{120,1}$.*

(ii) *$C_{120,2}$ is a self-orthogonal and doubly-even. It is a $[120, 9, 56]_2$ code, and its dual ${C_{120,2}}^{\perp}$ is a $[120, 111, 4]_2$ singly even code. Moreover $C_{120,2}$ and ${C_{120,2}}^{\perp}$ are optimal codes and* $\mathrm{Aut}(C_{120,2}) \cong S_8(2)$

(iii) *$C_{120,3}$ is a $[120, 15, 40]_2$ self-orthogonal, doubly-even and decomposable code. Its dual ${C_{120,3}}^{\perp}$ is a $[120, 105, 4]_2$ singly even code and* $\mathrm{Aut}(C_{120,3}) \cong S_6(2)$

(iv) *$C_{120,4}$ is a self-orthogonal and doubly-even $[120, 29, 24]_2$ code. Its dual ${C_{120,4}}^{\perp}$ is a $[120, 91, 8]_2$ singly even code.* $\mathbf{1} \in {C_{120,4}}^{\perp}$ *and* $\mathrm{Aut}(C_{120,4}) \cong S_6(2)$.

(v) *$C_{120,5}$ is a self-orthogonal, doubly-even code. It is a $[120, 35, 24]_2$ code, and its dual ${C_{120,5}}^{\perp}$ is a $[120, 85, 8]_2$ singly even code. Also,* $\mathbf{1} \in C_{120,5}$ *and* $\mathbf{1} \in {C_{120,5}}^{\perp}$ *and* $\mathrm{Aut}(C_{120,5}) \cong S_8(2)$

(vi) *$C_{120,6} = [120, 36, 24]_2$ is a self-orthogonal and doubly-even code. Its dual ${C_{120,6}}^{\perp}$ is a $[120, 84, 8]_2$ singly even code.* $\mathbf{1} \in C_{120,6}$ *and* $\mathbf{1} \in {C_{120,6}}^{\perp}$ *and* $\mathrm{Aut}(C_{120,6}) \cong S_8(2)$

Proof: The proof follows the same arguments as those used in the previous propositions, so we omit the details. ■

Remark 10.13. (i) The words of weight 56 in $C_{120,1}$ have a geometrical meaning. They represent the rows of the adjacency matrix of the graph $\Gamma = (120, 56, 28, 24)$ or equivalently the incidence vectors of the blocks of the symmetric 2-$(120, 56, 56)$

design. The code $C_{120,1} = [120, 8, 56]$ is part of a family of known codes of type $2^{2m-1} - 2^{m-1}, 2m + 1, 2^{2m-2} - 2^{m-1}$.

(ii) Notice that $C_{120,1}$ is a two-weight code. It follows from [23] that this code defines a strongly regular $(256, 120, 56, 56)$ graph Λ complemented by a strongly regular $(256, 135, 70, 72)$ graph $\bar{\Lambda}$. Since $\lambda = \mu$ we have that Λ is in fact a symmetric 2-$(256, 56, 56)$ design.

(iii) The words of weight 56 in $C_{120,1}$ represent copies of $G_2(2)$. These are stabilized by a group isomorphic to $U_3(3)$. The set of codewords of weight 24 in $C_{120,4}$ represent the isotropic lines and the stabilizer of an isotropic line is a group isomorphic to $(2^{1+4} \times 2^2) : (S_3 \times S_3)$. Notice that the latter group is maximal in $S_6(2)$. Since $\mathrm{Aut}(C_{120,1}) = O_8^+(2)$:2 and $\mathrm{Aut}(C_{120,4}) = S_6(2)$, we deduce that $O_8^+(2)$:2 acts primitively on isomorphic copies of $G_2(2)$, and $S_6(2)$ acts primitively on the set of isotropic lines. The set of codewords of weight 64 in $C_{120,1}$ represent isotropic planes. The stabilizer of an isotropic plane is isomorphic to 2^6:$L_3(2)$. Hence $O_8^+(2) : 2$ acts primitively on the isotropic planes. The remaining stabilizers are not maximal subgroups of the corresponding automorphism groups.

10.8 The 135-dimensional representation

$S_6(2)$ acts as rank-4 group primitive permutation group of degree 135 on the cosets of 2^6:$L_3(2)$ with orbits of lengths 1, 14, 56 and 64. Using this action we form a permutation module of dimension 135 invariant under G. The elements being permuted in this action are isotropic planes. The permutation module splits into 5 absolutely irreducible constituents of dimension 1 6, 8 14 and 48 with multiplicities of 5, 5, 3, 2 and 1 respectively. There are two irreducible submodules of dimensions 1 and 8, both absolutely irreducible. Working as in the earlier permutation representations we obtain submodules of dimensions $1, 8, 9, 14, 15(3), 16, 28, 29(2), 34, 35(10), 36(13), 37(3), 41, 42(7), 43(15), 44(8), 45, 49,$ $50(6), 51(7), 52$ and their duals. The digits in brackets represent the number of modules of the given length. Due to computer time limitations we are unable to

determine all submodules and hence codes of length 135 invariant under $S_6(2)$. As a result, in Figure 10.5 we give a partial lattice diagram. We were able to enumerate a total of 172 non-trivial binary codes of length 135. A summary of the properties of the codes found is given in Table 10.13.

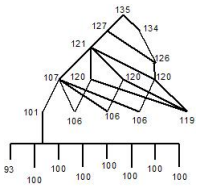


Figure 10.5: Partial submodule lattice of the 135-dimensional representation

In Table 10.13, the first column gives a label for the code, the second gives the parameters of the code, the third gives the number of codewords of a given weight where possible, the fourth column gives the structure of the automorphism group. From the fifth to the ninth columns we have true ("t") indicating if the code is self-orthogonal (s.o.), singly-even (s.e.), doubly even (d.e.), presence of the all-one vector (**1**) in the code or optimality, and false ("f") otherwise. The last column deals with the properties of the dual code.

Table 10.13: Properties of codes from the 135-dimensional representation.

Name	code	wds	Aut	s.o.	s.e.	d.e.	**1**	opt	dual	wds	s.e	d.e	**1**
$C_{135,1}$	$[135, 8, 64]$	135	$O_8^+(2):2$	t	t	t	f	f	$[135, 127, 3]$	1575	f	f	t
$C_{135,2}$	$[135, 9, 63]$	120	$O_8^+(2):2$	f	f	f	t	f	$[135, 126, 4]$	5195	t	f	f
$C_{135,3}$	$[135, 14, 48]$	630	$S_6(2)$	t	t	t	t	f	$[135, 121, 3]$	315	f	f	t
$C_{135,4}$	$[135, 15, 48]$	630	$S_6(2)$	f	f	f	t	f	$[135, 120, 4]$	2835	f	f	t
$C_{135,5}$	$[135, 15, 30]$	36	$S_6(2)$	t	t	f	f	f	$[135, 120, 3]$	315	f	f	t
$C_{135,6}$	$[135, 15, 48]$	630	$S_6(2)$	f	f	f	t	f	$[135, 120, 4]$	2835	t	f	f
$C_{135,7}$	$[135, 16, 30]$	360	$S_6(2)$	f	f	f	t	f	$[135, 119, 4]$	2835	t	f	f
$C_{135,8}$	$[135, 28, 32]$	95	$S_6(2)$	t	t	t	f	f	$[135, 107, 5]$	378	f	f	t
$C_{135,9}$	$[135, 29, 30]$	36	$S_6(2)$	t	t	f	f	f	$[135, 106, 5]$	378	f	f	t
$C_{135,10}$	$[135, 29, 32]$	945	$S_6(2)$	f	f	f	t	f	$[135, 106, 6]$	630	f	f	t
$C_{135,11}$	$[135, 30, 30]$	36	$S_6(2)$	f	f	f	t	f	$[135, 105, 6]$	630	t	f	f
$C_{135,12}$	$[135, 34, 32]$	12285	$O_8^+(2):2$	t	t	t	f	f	$[135, 101, 7]$	12285	f	f	t
$C_{135,13}$	$[135, 35, 31]$	3780	$O_8^+(2):2$	f	f	f	t	f	$[135, 100, 8]$	32400	t	f	f
$C_{135,14}$	$[135, 35, 30]$	36	$S_6(2)$	t	t	f	f	f	$[135, 100, 7]$	945	f	f	t
$C_{135,15}$	$[135, 35, 24]$	945	$S_6(2)$	f	t	f	f	f	$[135, 100, 6]$	630	f	f	t
$C_{135,16}$	$[135, 35, 24]$	1260	$S_6(2)$	f	t	f	f	f	$[135, 100, 5]$	378	f	f	t
$C_{135,17}$	$[135, 35, 32]$	12285	$S_6(2)$	f	f	f	f	f	$[135, 100, 7]$	1080	f	f	f
$C_{135,18}$	$[135, 35, 31]$	3780	$O_8^+(2):2$	f	f	f	f	f	$[135, 100, 8]$	32400	t	f	f
$C_{135,19}$	$[135, 35, 32]$	12285	$S_6(2)$	f	f	f	f	f	$[135, 100, 7]$	1080	f	f	f
$C_{135,20}$	$[135, 35, 30]$	36	$S_6(2)$	t	t	f	f	f	$[135, 100, 7]$	945	f	f	t
$C_{135,21}$	$[135, 35, 32]$	12285	$S_6(2)$	t	t	f	f	f	$[135, 100, 7]$	945	f	f	t
$C_{135,22}$	$[135, 35, 28]$	4320	$O_8^+(2):2$	t	t	t	f	f	$[135, 100, 7]$	2025	f	f	t
$C_{135,23}$	$[135, 36, 30]$	36	$S_6(2)$	f	f	f	t	f	$[135, 99, 8]$	16200	t	f	f
$C_{135,24}$	$[135, 36, 24]$	1260	$S_6(2)$	f	f	f	t	f	$[135, 99, 8]$	13365	t	f	f

Table 10.13 – continued from previous page

Name	code	wds	Aut	s.o	s.e	d.e	**1**	opt	dual	wds	s.e	d.e	**1**
$C_{135,25}$	[135, 36, 15]	63	$S_6(2)$	*f*	*f*	*f*	*t*	*f*	[135, 99, 6]	630	*t*	*f*	*f*
$C_{135,26}$	[135, 36, 27]	1120	$O_8^+(2):2$	*f*	*f*	*f*	*t*	*f*	[135, 99, 8]	32400	*t*	*f*	*f*
$C_{135,27}$	[135, 36, 27]	1120	$S_6(2)$	*f*	*f*	*f*	*f*	*f*	[135, 99, 8]	16200	*f*	*f*	*f*
$C_{135,28}$	[135, 36, 27]	1120	$S_6(2)$	*f*	*f*	*f*	*f*	*f*	[135, 99, 8]	16200	*f*	*f*	*f*
$C_{135,29}$	[135, 36, 28]	4320	$S_6(2)$	*t*	*t*	*f*	*f*	*f*	[135, 99, 7]	945	*f*	*f*	*t*
$C_{135,30}$	[135, 36, 24]	945	$S_6(2)$	*f*	*f*	*f*	*f*	*f*	[135, 99, 8]	13365	*f*	*f*	*f*
$C_{135,31}$	[135, 36, 24]	945	$S_6(2)$	*f*	*t*	*f*	*f*	*f*	[135, 99, 8]	13365	*f*	*f*	*t*
$C_{135,32}$	[135, 36, 24]	1260	$S_6(2)$	*f*	*t*	*f*	*f*	*f*	[135, 99, 8]	13365	*t*	*f*	*t*
$C_{135,33}$	[135, 36, 24]	1260	$S_6(2)$	*f*	*f*	*f*	*t*	*f*	[135, 99, 8]	13365	*f*	*f*	*f*
$C_{135,34}$	[135, 36, 15]	72	$S_6(2)$	*f*	*f*	*f*	*f*	*f*	[135, 99, 5]	378	*f*	*f*	*f*
$C_{135,35}$	[135, 36, 28]	4320	$S_6(2)$	*f*	*f*	*f*	*f*	*f*	[135, 99, 7]	1080	*t*	*f*	*f*
$C_{135,36}$	[135, 37, 15]	63	$S_6(2)$	*f*	*f*	*f*	*t*	*f*	[135, 98, 8]	13365	*t*	*f*	*f*
$C_{135,37}$	[135, 37, 15]	72	$S_6(2)$	*f*	*f*	*f*	*t*	*f*	[135, 98, 8]	13365	*t*	*f*	*f*
$C_{135,38}$	[135, 37, 27]	1120	$S_6(2)$	*f*	*f*	*f*	*t*	*f*	[135, 98, 8]	16200	*t*	*f*	*f*
$C_{135,39}$	[135, 41, 24]	2205	$S_6(2)$	*f*	*t*	*f*	*f*	*f*	[135, 94, 8]	2025	*f*	*f*	*t*
$C_{135,40}$	[135, 42, 24]	4725	$O_8^+(2)$	*f*	*t*	*f*	*t*	*f*	[135, 93, 8]	2025	*f*	*f*	*t*
$C_{135,41}$	[135, 42, 15]	63	$S_6(2)$	*f*	*f*	*f*	*t*	*f*	[135, 93, 8]	2025	*t*	*f*	*f*
$C_{135,42}$	[135, 42, 24]	2025	$S_6(2)$	*f*	*f*	*f*	*f*	*f*	[135, 93, 8]	2025	*f*	*f*	*f*
$C_{135,43}$	[135, 42, 24]	2025	$S_6(2)$	*f*	*t*	*f*	*f*	*f*	[135, 93, 8]	2025	*f*	*f*	*t*
$C_{135,44}$	[135, 42, 24]	2025	$S_6(2)$	*f*	*t*	*f*	*f*	*f*	[135, 93, 8]	2025	*f*	*f*	*t*
$C_{135,45}$	[135, 42, 15]	72	$S_6(2)$	*f*	*f*	*f*	*t*	*f*	[135, 91, 8]	2025	*f*	*f*	*f*
$C_{135,46}$	[135, 42, 24]	4725	$O_8^+(2)$	*f*	*t*	*f*	*f*	*f*	[135, 93, 8]	945	*f*	*f*	*t*
$C_{135,47}$	[135, 43, 24]	4725	$O_8^+(2)$	*t*	*f*	*f*	*f*	*f*	[135, 92, 8]	2025	*f*	*f*	*t*
$C_{135,48}$	[135, 43, 24]	4725	$S_6(2)$	*f*	*f*	*f*	*f*	*f*	[135, 92, 8]	945	*f*	*f*	*f*
$C_{135,49}$	[135, 43, 15]	135	$O_8^+(2)$	*f*	*f*	*f*	*t*	*f*	[135, 92, 8]	2025	*t*	*f*	*f*
$C_{135,50}$	[135, 43, 24]	4725	$S_6(2)$	*t*	*f*	*f*	*f*	*f*	[135, 92, 8]	945	*f*	*f*	*t*
$C_{135,51}$	[135, 43, 24]	4725	$O_8^+(2)$	*f*	*f*	*f*	*f*	*f*	[135, 92, 8]	2025	*f*	*f*	*f*
$C_{135,52}$	[135, 43, 24]	4725	$S_6(2)$	*f*	*f*	*f*	*t*	*f*	[135, 92, 8]	945	*f*	*f*	*t*
$C_{135,53}$	[135, 43, 24]		$S_6(2)$	*t*	*f*	*f*	*f*	*f*	[135, 92, 8]		*f*	*f*	*t*
$C_{135,54}$	[135, 43, 24]		$S_6(2)$	*t*	*f*	*f*	*f*	*f*	[135, 92, 8]		*f*	*f*	*t*
$C_{135,55}$	[135, 43, 15]		$O_8^+(2)$	*f*	*f*	*f*	*t*	*f*	[135, 92, 8]		*f*	*f*	*f*
$C_{135,56}$	[135, 43, 15]		$S_6(2)$	*f*	*f*	*f*	*t*	*f*	[135, 92, 8]		*t*	*f*	*f*
$C_{135,57}$	[135, 43, 24]		$O_8^+(2)$	*f*	*f*	*f*	*f*	*f*	[135, 92, 8]		*t*	*f*	*f*
$C_{135,58}$	[135, 43, 15]		$S_6(2)$	*f*	*f*	*f*	*f*	*f*	[135, 92, 8]		*f*	*f*	*f*
$C_{135,59}$	[135, 43, 24]		$O_8^+(2)$	*t*	*f*	*f*	*f*	*f*	[135, 92, 8]		*f*	*f*	*t*
$C_{135,60}$	[135, 43, 24]		$O_8^+(2)$	*t*	*f*	*f*	*f*	*f*	[135, 92, 8]		*f*	*f*	*t*
$C_{135,61}$	[135, 43, 24]		$S_6(2)$	*f*	*f*		*f*	*f*	[135, 92, 8]		*f*	*f*	*t*
$C_{135,62}$	[135, 44, 15]		$S_6(2)$	*f*	*f*	*f*	*t*	*f*	[135, 91, 8]		*t*	*f*	*f*
$C_{135,63}$	[135, 44, 24]		$S_6(2)$	*f*	*f*	*f*	*f*	*f*	[135, 91, 8]		*f*	*f*	*f*
$C_{135,64}$	[135, 51, 24]			*f*	*f*	*f*	*t*	*f*	[135, 91, 8]		*t*	*f*	*f*
$C_{135,65}$	[135, 44, 24]		$S_6(2)$	*f*	*t*	*f*	*f*	*f*	[135, 91, 8]		*f*	*f*	*f*
$C_{135,66}$	[135, 44, 24]		$S_6(2)$	*f*	*f*	*f*	*f*	*f*	[135, 91, 8]		*f*	*f*	*t*
$C_{135,67}$	[135, 44, 15]		$S_6(2)$	*f*	*f*	*f*	*f*	*f*	[135, 91, 8]		*f*	*f*	*f*
$C_{135,68}$	[135, 44, 15]		$S_6(2)$	*f*	*f*	*f*	*t*	*f*	[135, 91, 8]		*t*	*f*	*f*
$C_{135,69}$	[135, 44, 15]		$O_8^+(2)$	*f*	*f*	*f*	*t*	*f*	[135, 91, 8]		*t*	*f*	*f*
$C_{135,70}$	[135, 45, 15]		$S_6(2)$	*f*	*f*	*f*	*t*	*f*	[135, 90, 8]		*t*	*f*	*f*
$C_{135,71}$	[135, 49, 16]		$S_6(2)$	*f*	*t*	*f*	*f*	*f*	[135, 86, 9]		*f*	*f*	*t*
$C_{135,72}$	[135, 50, 15]		$S_6(2)$	*f*	*f*	*f*	*t*	*f*	[135, 85,]		*t*	*f*	*f*
$C_{135,73}$	[135, 50, 16]		$S_6(2)$	*f*	*f*	*f*	*f*	*f*	[135, 85,]		*f*	*f*	*f*
$C_{135,74}$	[135, 43, 16]		$O_8^+(2)$	*f*	*t*	*f*	*f*	*f*	[135, 85,]		*f*	*f*	*t*
$C_{135,76}$	[135, 50, 15]		$S_6(2)$	*f*	*f*	*f*	*f*	*f*	[135, 85,]		*f*	*f*	*f*
$C_{135,77}$	[135, 50, 16]			*f*	*f*	*f*	*f*	*f*	[135, 85,]		*f*	*f*	*f*
$C_{135,78}$	[135, 50, 16]			*f*	*t*	*f*	*f*	*f*	[135, 85,]		*f*	*f*	*t*
$C_{135,79}$	[135, 51, 15]			*f*	*f*	*f*	*t*	*f*	[135, 84,]		*t*	*f*	*f*
$C_{135,80}$	[135, 51, 15]			*f*	*f*	*f*	*t*	*f*	[135, 84,]		*t*	*f*	*f*
$C_{135,81}$	[135, 51, 15]			*f*	*f*	*f*	*t*	*f*	[135, 84,]		*t*	*f*	*f*
$C_{135,82}$	[135, 51, 16]			*f*	*t*	*f*	*f*	*f*	[135, 84,]		*f*	*f*	*f*
$C_{135,83}$	[135, 51, 15]			*f*	*f*	*f*	*f*	*f*	[135, 84,]		*f*	*f*	*f*
$C_{135,84}$	[135, 51, 15]			*f*	*f*	*f*	*f*	*f*	[135, 84,]		*f*	*f*	*f*
$C_{135,85}$	[135, 51, 15]			*f*	*f*	*f*	*f*	*f*	[135, 84,]		*f*	*f*	*t*
$C_{135,86}$	[135, 52, 15]			*f*	*f*	*f*	*t*	*f*	[135, 83,]		*t*	*f*	*f*

Remark 10.14. We have computed the weight distributions up to dimension 44. Currently Magma is unable to give the computations for higher dimensions. Consequently the relations between the codes could not be fully established. A summary of the codes found and their properties is given in Tables 10.14 and 10.15.

Table 10.14: Weight distribution of codes of length 135.

dim	0	15	24	27	28	29	30	31	32	33	34	35	36	37
8	1													
9	1													
14	1													
15	1													
15	1						36							
15	1													
16	1						36							
28	1								945				3360	
29	1						36		945				3360	
29	1								945				3360	
35	1							3780	12285			12096	33600	
35	1						36		12285				33600	
35	1		945				1044		945				43680	
35	1		1260				1296		4725				33600	
35	1								12285	1260			33600	
35	1							3780	12285			12096	33600	
35	1								12285				33600	4320
35	1						36		12285				33600	
35	1								12285				33600	
35	1				4320				12285				45600	
36	1						36	3780	12285	1260		12096	33600	
36	1		1260				1296		4725				33600	
36	1	63	945				1044	3780	945	16380			43680	
36	1			1120	4320			3780	12285			16416	45600	
36	1			1120			36		12285			4320	33600	4320
36	1			1120					12285	1260		4320	33600	
36	1				4320		36		12285				45600	
36	1		945				1044		945			8640	43680	
36	1		945				1044		945				52320	
36	1		1260				1296		4725				33600	
36	1	72	1260				1296	7560	4725	20160			33600	
36	1				4320				12285	1260			45600	4320
36	1							3780	12285			12096	33600	4320
42	1		4725				4320		68985				638400	
42	1	63	2205				2304	30240	38745	80640		12096	315840	
42	1		2205	1120			2304		38745			276480	315840	276480
42	1		2205		4320		2304		38745				882240	
42	1		2205				2304		38745				949440	
42	1		4725				4320		68985				638400	
42	1	72	2205				2304	30240	38745	70560			315840	
44	1	135	4725		4320	1080	8136	60480	68985	194040	128520	163296	977760	430920

Table 10.15: Table 10.14 continued

dim	...	101	102	103	104	105	106	107	108	111	120	135
8	...											
9	...											1
14	...											
15	...					36						
15	...											
15	...											1
16	...					36						1
28	...											
29	...											
29	...					36						
35	...			12285	3780							1
35	...		1260		3780							
35	...		16380		3780						63	
35	...											
35	...				3780	36						
35	...				3780							
35	...				3780							
35	...				3780				1120			
36	...		1260	12285	3780	36						1
36	...			4725		1296				1260		1
36	...		16380	945	3780	1044				945	63	1
36	...			12285	3780			4320	1120			1
36	...		1260		3780			4320				
36	...				3780	36		4320				
36	...		1260		3780				1120			
36	...		16380		3780						63	
36	...		16380		3780						63	
36	...		20160		7560						72	
36	...											
36	...				3780	36			1120			
36	...			12285	3780							1
42	...		151200		60480						135	
42	...		80640	38745	30240	2304				2205	63	1
42	...		80640		30240			4320			63	
42	...		80640		30240				1120		63	
42	...		80640		30240						63	
42	...		151200		60480						135	
42	...		80640	30240	30240	2016				2520	63	
44	...	128520	194040	68985	60480	8136	1080	4320		4725	135	1

Bibliography

[1] J. L. Alperin and R. B. Bell, *Groups and Representations*, Springer-Verlag, New York, Inc., 1995.

[2] E. Artin, *Geometric Algebra*, Wiley Interscience, New York, 1957.

[3] M. Aschbacher, *Finite group theory*, Cambridge University Press, 2000.

[4] E. F. Assmus, Jr. and J. D. Key, *Designs and their Codes*, Cambridge University Press, 1992, Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).

[5] E. F. Assmus, Jr. and J. D. Key, *Designs and their codes: an update*, Des. Codes Cryptogr. **9** (1996), 7–27.

[6] M. K. Bennett, *Affine and Projective Geometry*, Wiley-Interscience, New York, 1995.

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

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

[9] C. C. Blackburn, *An Application of the Computer Algebra System GAP: The Construction of the Simple Modules of a Finite Group*, Master's thesis, The University of Arizona, 2009.

[10] W. Bosma, J. Cannon, and C. Playoust, *The Magma Algebra System I: The User Language*, J. Symbolic Comput. **24** (1997), 235–265.

[11] S. Braić, A. Golemac, J. Mandić, and T. Vučičić, *Primitive symmetric designs with prime power number of points*, J. Combin. Designs **18** (2010), 141–154.

[12] R. Brauer and C. Nesbitt, *On modular characters of groups*, Annals of Mathematics **42** (1941), no. 2, 556–590.

[13] P. L H. Brooke, *On matrix representations and codes associated with the simple group of order* 25920, J. Algebra **91** (1984), no. 2, 536–566.

[14] P. L. H. Brooke, *On the Steiner system* $S(2, 4, 28)$ *and codes associated with the simple group of order* 6048, J. Algebra **97** (1985), no. 2, 376–406.

[15] A. E. Brouwer, *A slowly growing collection of graph descriptions*, http://www.win.tue.nl/ aeb/graphs/index.html.

[16] A. E. Brouwer, *The Gewirtz graph: an exercise in the theory of graph spectra*, European J. Combin. **14** (1993), no. 5, 397–407.

[17] A. E. Brouwer, *Bounds on linear codes*, Handbook of Coding Theory (V. S. Pless and W. C. Huffman, eds.), vol. 1, Elsevier Science B.V., Amsterdam: North Holland, 1998, pp. 295–461.

[18] A. E. Brouwer and C. J. van Eijl, *On the p-rank of the adjacency matrices of strongly regular graphs*, J. Algebraic Combin. **1** (1992), 329–346.

[19] R. A. Brualdi, W. C. Huffman, and V. S. Pless, *An introduction to algebraic codes*, Handbook of Coding Theory (V. S. Pless and W. C. Huffman, eds.), vol. 1, Elsevier Science B.V., Amsterdam: North Holland, 1998, pp. 3–139.

[20] E. Byrn, M. Greerath, and Honold T., *Ring geometries, two weight codes and strongly regular graphs*, Designs Codes and Cryptology **48** (2008), 1–16.

[21] A. R. Calderbank and P. Frankl, *Binary codes and quasi-symmetric designs*, Discrete Math **83** (1990), 201–204.

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

[23] R. Calderbank and W. M. Kantor, *The geometry of two-weight codes*, Bull. London Math. Soc. **18** (1986), 97–122.

[24] P. J. Cameron, *Permutation Groups*, Cambridge University Press, Cambridge, 1999, London Math. Soc. Students Text, 45.

[25] P. J. Cameron and J. H. van Lint, *Graphs, Codes and Designs*, Cambridge University Press, Cambridge, 1980, London Math. Soc. Lecture Notes in Mathematics.

[26] P. J. Cameron and J. H. van Lint, *Designs, Graphs, Codes and their Links*, Cambridge University Press, Cambridge, 1991, London Math. Soc. Student Texts, 22.

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

[28] Y. Cheng and N. J. Sloane, *Codes from symmetry groups and* $[32, 17, 8]$ *code*, SIAM J. Disc. Math. **2** (1989), no. 1, 28–37.

[29] L. Chikamai, J. Moori, and B. G. Rodrigues, 2*-modular codes admitting the simple group* $L_3(4)$ *as an automorphism group*, To appear in Utilitus Mathematica.

[30] L. Chikamai, J. Moori, and B. G. Rodrigues, *Binary codes from some* 2-$(64, 28, 12)$ *designs and their orbit matrices*, Submitted.

[31] L. Chikamai, J. Moori, and B. G. Rodrigues, *Some irreducible* 2*-modular codes invariant under the symplectic group* $S_6(2)$, In preparation.

[32] L. Chikamai, J. Moori, and B. G. Rodrigues, 2-*modular representations of the alternating group* A_8 *as binary codes*, Glasnik Mathematicki **47** (2012), no. 67, 225–252.

[33] K. L. Clark, *Bounds for the minimum weight of the dual codes of some class of designs*, Ph.D. thesis, Clemson University, S. C., 2000.

[34] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, and R.A. Wilson, *Atlas of Finite Groups*, Oxford University Press, Oxford, 1985.

[35] J.H. Conway and N. J. Sloane, *Sphere Packings, Lattices and Groups*, Springer Verlag, New York, 1988.

[36] G. M. Conwell, *The 3-space* $PG(3,2)$ *and its group*, Ann. of Math. **11** (1910), no. 2, 60–76.

[37] K. Coolsaet, *The uniqueness of the strongly regular graph* $\mathrm{srg}(105,32,4,12)$, Bull. Belg. Math. Soc. Simon Stevin **12** (2005), no. 5, 707–718.

[38] D. Crnković and M. O. Pavčević, *Some new designs with parameters* $(64,28,12)$, Discrete Math. **237** (2001), 109–118.

[39] D. Crnković, B. G. Rodrigues, S. Rukavina, and L. Simčić, *Ternary codes from the strongly regular* $(45,12,3,3)$ *graphs and orbit matrices of* 2-$(45,12,3)$ *designs*, Discrete Math. **312** (2012), 3000–3010.

[40] D. Crnković and V. M. Crnković, *On some combinatorial structures constructed from the groups* $L(3,5), U(5,2)$ *and* $S(6,2)$, Int. J. Combin. (2011), Art. ID 137356, 12 pp.

[41] D. Crnković and V. Mikulić, *Unitals, projective planes and other combinatorial structures constructed from the unitary groups* $U_3(q)$, $q = 3,4,5,7$, Ars Combin. **110** (2013), 3–13.

[42] D. Crnković, V. Mikulić, and B. G. Rodrigues, *Designs, strongly regular graphs and codes constructed from some primitive groups*, NATO Science for Peace and

Security Series - D: Information and Communication Security, vol. 29 (2011), pp. 231–252., IOS Press (ISSN 1874–6268).

[43] J. Degraer and K. Coolsaet, *Classification of some strongly regular subgraphs of the McLaughlin graph*, Discrete Math. **308** (2008), no. 2-3, 395–400.

[44] P. Delsarte, *A geometric approach to a class of cyclic codes*, J. Combin. Theory **6** (1969), 340–358.

[45] P. Delsarte, *Majority logic decodable codes derived from finite inversive planes*, Inform. and Control **18** (1971), 319–325.

[46] P. Delsarte, *Weight of linear codes and strongly regular normed spaces*, Discrete Math. **3** (1972), 47–64.

[47] P. Delsarte and J. M. Goethals, *On a class of majority-logic decodable cyclic codes*, IEEE Trans. Information Theory **14** (1968), 182–188.

[48] P. Delsarte, J. M. Goethals, and F. J. MacWilliams, *On the generalized Reed-Muller codes and their relatives*, Inform. and Control **16** (1970), 403–442.

[49] P. Dembowski, *Finite Geometries*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44, Berlin, Heidelberg, New York: Springer-Verlag, 1968.

[50] U. Dempwolff, *Primitive rank-3 groups on symmetric designs*, Des. Codes and Cryptogr. **22** (2001), 191–207.

[51] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Dover Publications, New York, 1958, With an introduction by Wilhelm Magnus.

[52] J. D. Dixon and B. Mortimer, *Permutation Groups*, Springer Verlag, New York, 1996.

[53] S. M. Dodunekov, S. B. Encheva, and S. N. Kapralov, *On the* $[28, 7, 12]$ *binary self-complementary codes and their residuals*, Des. Codes Cryptogr. **4** (1994), 57–67.

[54] R. Foote and D. S. Dummit, *Abstract algebra*, John Wiley and Sons, Inc.

[55] H. Gottschalk, *Rank three geometries associated with* PSL(3, 4), Bull. Belg. Math. Soc. Simon Stevin **3** (1996), no. 2, 147–160.

[56] H. Gottschalk, *A connection between six distinguished diagrams*, Atti Sem. Mat. Fis. Univ. Modena **47** (1999), 1–12.

[57] R. Gow, *Some characters of affine subgroups of classical groups*, J. London Math. Soc **2** (1976), 231–236.

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

[59] M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes*, Online available at http://www.codetables.de, 2007, Accessed on 15–09–2012.

[60] W. H. Haemers, *Matrices for Graphs, Designs and Codes*, Lecture notes.

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

[62] W. H. Haemers, R. Peeters, and J. M. van Rijckevorsel, *Binary codes of strongly regular graphs*, Des. Codes Cryptogr. **17** (1999), 187–209.

[63] N. Hamada, *On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its application to error correcting codes*, Hiroshima Math. J. **3** (1973), 153–226.

[64] M. Harada and V. D. Tonchev, *Self-orthogonal codes from symmetric designs with fixed-point-free automorphisms*, Discrete Math. **264** (2003), no. 1-3, 81–90.

[65] D. G. Higman, *Finite permutation groups of rank 3*, Math. Z. **86** (1964), 145–156.

[66] R. Hill, *A First Course in Coding Theory*, Oxford Applied Mathematics and Computing Science Series, Oxford University Press, Oxford, 1986.

[67] W. C. Huffman, *Codes and Groups*, Handbook of Coding Theory (In V. S. Pless and W. C. Huffman, eds.), Elsevier, 1998, Volume 2, Part 2, Chapter 17, pp. 1345–1440.

[68] B. Huppert, *Endliche Gruppen I*, Springer Verlag, Berlin, Heidelberg, 1967.

[69] I.M. Isaacs, *Character Theory of Finite Groups*, Academic Press, Inc., 1976.

[70] C. Jansen, K. Lux, R. Parker, and R. Wilson, *An Atlas of Brauer Characters*, London Mathematical Society Monographs. New Series, vol. 11, The Clarendon Press Oxford University Press, New York, 1995, Appendix 2 by T. Breuer and S. Norton, Oxford Science Publications.

[71] D. Jungnickel and V. D. Tonchev, *On symmetric and quasi-symmetric designs with the symmetric difference property and their codes*, J. Combin. Theory Ser. A **59** (1992), no. 1, 40–50.

[72] S. Kalayaycioglu, *Algorithmic Methods in Modular Representation Theory*, 2006, Lecture notes.

[73] W. M. Kantor, *Symplectic groups, symmetric designs, and line ovals*, J. Algebra **33** (1975), 43–58.

[74] W. M. Kantor, *Classification of 2-transitive symmetric designs*, Graphs and Combin. **1** (1985), 165–166.

[75] W. M. Kantor and R. A. Liebler, *The rank-3 permutation representations of the finite classical groups*, Trans. American Math. Soc. **271** (1982), 1–71.

[76] G. T. Kennedy and V. Pless, *A coding theoretic approach to extending designs*, Discrete Math. **142** (1995), 155–168.

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

[78] J. D. Key and J. Moori, *Designs, codes and graphs from the Janko groups J_1 and J_2*, J. Combin. Math. and Combin. Comput. **40** (2002), 143–159.

[79] J. D. Key and J. Moori, *Correction to: "Codes, designs and graphs from the Janko groups J_1 and J_2" [J. Combin. Math. Combin. Comput.* **40** *(2002), 143–159]*, J. Combin. Math. Combin. Comput. **64** (2008), 153.

[80] J. D. Key and J. Moori, *Some irreducible codes invariant under the janko group, J_1 or J_2.*, J. Combin. Math. and Combin. Comput., **81** (2012), 165–189.

[81] J. D. Key, J. Moori, and B. G. Rodrigues, *Binary codes from graphs on triples*, Discrete Maths **282** (2004), 171–182.

[82] J. D. Key, J. Moori, and B. G. Rodrigues, *Permutation decoding for the binary codes from triangular graphs*, European J. Combin. **25** (2004), 113–123.

[83] W. Knapp and P. Schmid, *Codes with prescribed permutation group*, J. Algebra **67** (1980), 415–435.

[84] E. Lander, *Symmetric Designs: An Algebraic Approach*, Cambridge University Press, Cambridge, 1983.

[85] D. Leemans and B. G. Rodrigues, *Binary codes of some strongly regular subgraphs of the Mclaughlin graph*, To appear in Des. Codes and Cryptogr.

[86] M. W. Liebeck, *The affine permutation groups of rank three*, Proc. London Math. Soc. **54** (1987), no. 3, 477–516.

[87] M. W. Liebeck and J. Saxl, *The finite permutation groups of rank three*, Bull. London Math. Soc. **18** (1986), 165–172.

[88] K. Lux and H. Pahlings, *Representation of Groups: A Computational Approach*, Cambridge University Press, Cambridge, 2010.

[89] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1983.

[90] S. Martini, *Representation Theory*, 2009, Lecture notes.

[91] R. Mathon and A. Rosa, *Designs of small order*, Handbook of Combinatorial Designs (Chapman and Hall/CRC, Boca Raton) (C. J. Colbourn and J. H. Dinitz, eds.), 2nd ed., 2007, pp. 25–58.

[92] G. McGuire, V. D. Tonchev, and H. N. Ward, *Characterizing the Hermitian and Ree unitals on 28 points*, Des. Codes Cryptogr. **13** (1998), no. 1, 57–61.

[93] G. McGuire and H. N. Ward, *Characterization of certain minimal rank designs*, J. Combin. Theory Ser. A **83** (1998), 42–56.

[94] J. Moori, *Group Theory and Representation Theory*, University of Natal, Pietermaritzburg, 2000, Lecture notes.

[95] J. Moori and B. G. Rodrigues, *A self-orthogonal doubly even code invariant under* $\mathrm{M^cL}:2$, J. Combin. Theory Ser. A **110** (2005), no. 1, 53–69.

[96] J. Moori and B. G. Rodrigues, *Some designs and codes invariant under the simple group* Co_2, J. Algebra **316** (2007), 649–661.

[97] A. Neumaier, *Some sporadic geometries related to* $PG(3, 2)$, Arch. Math. **42** (1984), no. 1, 89–96.

[98] C. Parker, E. Spence, and V. D. Tonchev, *Designs with the symmetric difference property on* 64 *points and their groups*, J. Combin. Theory Ser. A **67** (1994), no. 1, 23–43.

[99] R. Peeters, *Uniqueness of strongly regular graphs having minimal p-rank*, Linear Algebra Appl. **226–228** (1995), 9–31.

[100] R. Prag, *Brief Summary of Modular Representation Theory*, Lecture notes.

[101] B. G. Rodrigues, *On the Theory and Examples of Group Extensions*, Master's thesis, University of Natal, Pietermaritzburg, 1999.

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

[103] B. G. Rodrigues, *On the stabilizers of the minimum-weight codewords of the binary codes from triangular graphs*, Ars Combin. **82** (2007), 353–364.

[104] B. G. Rodrigues, *Some optimal codes from graphs invariant under the alternating group A_8.*, Adv. Math. Comm. **5** (2011), no. 2, 339–350.

[105] C. M. Roney-Dougal and W. R. Unger, *The affine primitive permutation groups of degree less than 1000*, J. Symbolic Comput. **35** (2003), no. 4, 421–439.

[106] J. J. Rotman, *An Introduction to the Theory of Groups*, Fourth ed., Springer-Verlag, New York, Inc., 1995.

[107] L. D. Rudolph, *A class of majority logic decodable codes*, IEEE Trans. Information Theory **13** (1967), 305–307.

[108] D. Seiple, *Investigation of Binary Self-dual Codes invariant under Simple Groups*, Master's thesis, The University of Arizona, 2009.

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

[110] M. S. Shrikhande and S. S. Sane, *Quasi-symmetric Designs*, London Mathematical Society Lecture Note Series, vol. 164, Cambridge University Press, Cambridge, 1991.

[111] D. E. Taylor, *The Geometry of the Classical Groups*, Sigma Series in Pure Mathematics, vol. 9, Heldermann Verlag, Berlin, 1992.

[112] V. D. Tonchev, *A characterization of designs related to the Witt system* $S(5, 8, 24)$, Math. Z. **191** (1986), 225–230.

[113] V. D. Tonchev, *The uniformly packed binary* $[27, 21, 3]$ *and* $[35, 29, 3]$ *codes*, Discrete Math. **149** (1996), 283–288.

[114] V. D. Tonchev, *Codes*, Handbook of Combinatorial Designs (Chapman and Hall/CRC, Boca Raton) (C. J. Colbourn and J. H. Dinitz, eds.), 2^{nd} ed., 2007, pp. 667–702.

[115] J. Ueberberg, *A class of partial linear spaces related to* $PGL_3(q^2)$., European J. Combin. **18** (1997), 103–115.

[116] J. H. van Lint, *On ovals in* $PG(2, 4)$ *and the Mclaughlin graph*, Report-wsk, Eindhoven Technical University, 1984, 1345–1440.

[117] H. Whitney, *Congruent graphs and the connectivity of graphs*, Amer. J. Math. **54** (1932), 154–168.

[118] R. A. Wilson, *The Finite Simple Groups*, London: Springer-Verlag London Ltd., 2009, Graduate Texts in Mathematics, Vol. 251.

[119] R. A. Wilson, R. A. Parker, and J. N. Bray, *Atlas of Finite Group Representations*, http://brauer.maths.qmul.ac.uk/Atlas/alt/A8/.

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

[121] A. De Wispelaere and H. Van Maldeghem, *Unitals in the Hölz-design on 28 points*, J. Combin. Theory Ser. A **114** (2007), no. 2, 265–277.

[122] V. Y. Yorgov, *A method for constructing inequivalent self-dual codes with applications to length 56*, IEEE Trans. Inform. Theory **33** (1987), no. 3, 77–82.

Index