On the existence of self-dual codes invariant under permutation groups

by
Tendai. M. Mudziiri Shumba

Dissertation submitted in fulfilment of the requirements for the degree of Master of Science

in the

School of Mathematics, Statistics and Computer Science
University of KwaZulu-Natal
June 2014

On the existence of self-dual codes invariant under permutation groups

by
Tendai. M. Mudziiri Shumba

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

Professor B.G. Rodrigues

.....

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

Professor S. Mukwembi

.....

Dedication

To A. G. R. Stewart who first taught me Algebra, And to my mother who was my first teacher.

Abstract

Let G be a prescribed permutation group. We study the question of existence of self-dual codes over a field $F = F_q, q = p^l$, p a prime, admitting G, that is, are G-invariant. This depends on the structure of G and its representations as well as the base field F_q. We investigate what conditions are necessary and sufficient for the existence of such codes. Representation theoretic as well as group theoretic methods are used. For the binary case we look at the existence of self-dual binary codes of length n which are invariant under the symmetric groups S_n and the alternating groups $A_n, n \geq 4$. We find that such codes do not exist. Further, for the sporadic simple and almost simple groups of degree ≤ 2000, $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, J_1, J_2, HS, HS{:}2, Co_3, M_{12}{:}2, M_{22}{:}2$ and $J_2{:}2$ we search for G-invariant self-dual codes of various lengths and attempted a classification where computations were possible, or theoretical methods permitted.

Acknowledgements

The author wishes to thank Professor B. G. Rodrigues and Professor S. Mukwembi without whom the present work would not have been possible. Their support and guidance has been invaluable and has extended beyond the academic to the mundane. Their financial support is gratefully acknowledged.

A debt of gratitude is owed to Professor D. Baboolal for availing a grant through the NRF. His support is greatly appreciated. The School of Mathematics, Statistics and Computer Science provided an environment that was amenable and provided fantastic computational resources. Colleagues and friends in the department have made the author's stay pleasant and bearable. Much gratitude for their camaraderie. Family, especially siblings have been a stay, offering support in various ways. Many thanks are due to them. Above all, the Infinite One of ages for granting the author peace and courage to continue.

The thesis examiners made very useful comments. The author is indebted to them for helping improve the final version of this work.

Contents

List of Tables

List of symbols

$a \mid b, a \nmid b$	a divides b, a does not divide b
$A \setminus B$	Set difference
$A \times B$	The Cartesian product of A and B
$\mathrm{Aut}(\mathcal{C})$	The automorphism group of $\mathcal{C}$
$A \dot{\cup} B$	Disjoint union of A and B
$A \wr B$	The wreath product of A and B
$\mathrm{char}(F)$	The characteristic of F
$\mathcal{C}^{\perp}$	The dual of $\mathcal{C}$
$F^{\times}$	$F \setminus \{0_F\}$
$\mathrm{Fix}(\sigma)$	The set $\{\omega \in \Omega \mid \omega^{\sigma} = \omega\}$, of fixed points of σ
FG	Group algebra of G over F
$\gcd(a, b)$	The greatest common divisor of integers a and b
$\mathrm{Gal}(K/L)$	The Galois group of the field extension
$\lvert G : H \rvert$	The index of H in G
$G \times H$	The direct product of G and H
$G^{\times}$	$G \setminus \{1_G\}$
G/H	Coset space or factor group if H is normal
$G_{p'}$	The set of all p-regular elements of G
$\lvert G \rvert_p$	Highest power of p dividing $\lvert G \rvert$
G_x	The stabilizer of x in G
$H \leq G$	H is a subgroup of G
$H \trianglelefteq G$	H is a normal subgroup of G
$\mathrm{Hom}_R(U, V)$	The set of homomorphisms from U to V
$\mathrm{I}(G)$	The set of involutions of G
L/F	Field extension L of a field F.
$\mathrm{Mat}_n(\Delta_i)$	The ring of all $n \times n$ matrices over Δ_i
$M \uparrow^G, \mathrm{Ind}_H^G$	The induced module
$\mathrm{o}(g)$	The order of an element g of a group
$\mathrm{Orb}_G(x)$	The orbit of x under G
${}_R R$	Left regular module
S_n	The symmetric group on n symbols
$\mathrm{tr}(A)$	Trace of A
V^*	The dual module of V

$V \oplus W$	The direct sum of V and W
$V \otimes_R W$	The tensor product of R-modules V and W
$V \downarrow_H$	FG-module V restricted to $H \leq G$
δ_{ij}	The Kronecker symbol
Δ_i	Division ring
χ_ρ	Character afforded by ρ
χ_V	Character afforded by a representation on a vector space V
ω^σ	The image $\sigma(\omega)$ of ω under σ
ρ	Representation of G
$[\rho]$	Matrix representation of ρ w.r.t some basis
ζ	Primitive root of unity
Ω	A set
$\lvert\Omega\rvert$	The cardinality of Ω
$\mathfrak{p}$	An ideal in R
$\mathcal{O}_K$	The field of fractions of K
$\mathbb{P}(\Omega)$	The power set of Ω
$\mathbb{F}_p$	The finite residue field $\mathbb{Z}/p\mathbb{Z}$

Declaration

This dissertation, in its entirety or in part, has not been submitted to this or any other institution in support of an application for the award of a degree. It represents the author's own work and where the work of others has been used in the text, proper reference has been made.

Tendai Makope Mudziiri Shumba

. . . . . .

Chapter 1

Introduction

Given a permutation group G acting on a set Ω of n points, we construct a binary code $C(G,\Omega) = \langle \mathrm{Fix}(\sigma) | \sigma \in I(G) \rangle^{\perp}$, where $I(G)$ is the set of involutions of G and $\mathrm{Fix}(\sigma) = \{\omega \in \Omega | \omega^{\sigma} = \omega\}$ is the set of fixed points of the permutation σ, i.e., $C(G,\Omega)$ is the code generated by the sets of fixed points of involutions of the group. We use representation theoretic methods to obtain the permutation representation of G on the cosets of a subgroup H of G. Since this action is transitive, we can treat Ω as the set G/H where H is chosen such that $|G : H| = n$.

The code obtained in the construction above is very useful in the search for self-dual codes which are invariant under the action of the group G in that every self-orthogonal code of length n which is invariant under G is contained in $C(G,\Omega)$. Further, every self-dual code $\mathcal{C}$ is such that $C(G,\Omega)^{\perp} \subset \mathcal{C} \subset C(G,\Omega)$. This provides a good starting point for the search of G-invariant self-dual codes.

Using libraries of groups in the computer algebra packages GAP [19] and MAGMA [9] , we construct codes invariant under some sporadic simple and almost simple groups of degree ≤ 2000. We also apply the method to the symmetric groups on $n = 2m$ points for $2 \leq m \leq 50$, and in this case we found that there are no self-dual codes of length $n = 2m$ invariant under the action of the symmetric groups. Modular representation theoretic considerations come in as we regard all the G-invariant codes as $\mathbb{F}_2 G$ modules. A theorem of Günther and Nebe shows that for a code to be self dual, all the constituents of the code regarded as an $\mathbb{F}_2 G$ module occur with even multiplicities. We use

this theorem to further refine our search. Although our treatment is general and applicable to any prime field, particular attention has been given to binary codes.

In Chapter 2 we lay down the basics of the theory of linear codes and designs. In Chapter 3 we show how G-invariant linear codes can be viewed as FG-modules. We discuss the rudiments of modules and representation theory. A method of constructing codes spanned by the sets of fixed points of involutions of some permutation groups due to Chigira et al in [35] is presented in Chapter 4. This is of interest to us because every self-dual code is necessarily self-orthogonal. Further, some necessary conditions for the existence of self-dual codes are embedded within the construction. Given a permutation group G and a set Ω of n points, we construct the code $C(G, \Omega)$, which is the dual of the code spanned by the sets of fixed points of involutions of the group G. Chapter 5 surveys existence criteria for self-dual permutation codes over arbitrary fields of positive characteristic not necessarily 2. Many of the results in this chapter are due to Fan Yun and Yuan Yuan [49]. We conclude by giving a catalogue of our results in Chapter 6.

For general representation theory, both ordinary and modular, we used [13],[14],[15],[32],[18] and [26] as sources. Benson's notes [7] were found to be excellent. For the theory of groups, we found [41],[48],[4] and [3] as very good sources. We refer the reader to [1],[42], [43] and [8] for general ring theory. For the theory of error-correcting codes and designs, we found [5],[23],[38] and [33] readable. As general reference books we used [16] and [31].

Chapter 2

Basics of Coding Theory

In this chapter we lay down the basics of the theory of linear codes and designs.

2.1 Basic definitions

We use F to denote a finite field, which for the most part will be $\mathbb{F}_2$ as we study binary codes more extensively compared to the other codes. We however give general definitions because non-binary codes are also considered. Thus throughout this chapter we assume $F = F_q$, the field of q elements, $q = p^l$ for some prime p and a natural number l.

Definition 2.1.1. If F is a finite field, then F^n, the set of all n-tuples of F is a vector space over F for some $n \in \mathbb{N}$. A **linear code** $\mathcal{C}$ of *length* n is a subspace of F^n.

The elements of the code $\mathcal{C}$ are called *codewords*. The field F is called the *alphabet*. To introduce all the parameters of a code, we need to define a distance function d called Hamming distance.

Definition 2.1.2. For vectors $x = (x_1, \ldots, x_n)$ and
$y = (y_1, \ldots, y_n) \in F^n$ the **Hamming distance** is defined by $d(x, y) = |\{i | 1 \leq i \leq n;\ x_i \neq y_i\}|$. The set $\{i | 1 \leq i \leq n;\ x_i \neq 0\}$ is called the **support** of x.

In other words, the Hamming distance $d(x, y)$ between x and y is the number of coordinate places where they differ.

Definition 2.1.3. For $x \in F^n$, the **weight** $w(x)$, of x is defined as

$$w(x) := d(x, \mathbf{0}).$$

In other words, the weight of a word is the number of non-zero coordinates the word has. With this set up, we see that $d(x, y) = w(x - y)$. We now give another important definition.

Definition 2.1.4. The minimum distance d, of a code $\mathcal{C}$ is the minimum of all the distances between words of the code, that is

$$d := \min\{w(x - y) | x, y \in \mathcal{C}; x \neq y\}.$$

It is not difficult to see that for linear codes, the minimum weight is the minimum distance. We are now in a position to give the definition of a linear code with all the parameters.

Definition 2.1.5. A k-dimensional linear subspace $\mathcal{C}$ of F^n is called an $[n, k]$ code over F. Further, if the minimum weight d, of $\mathcal{C}$ is known, then $\mathcal{C}$ is known as an $[n, k, d]$ code. The numbers n, k, d are called the parameters of the code.

Definition 2.1.6. A code whose codewords have weight divisible by 2 is called an even code. If a code has weight divisible by 4 then it is called doubly even. A code is singly even if it is not doubly even.

Definition 2.1.7. Let $\mathcal{C}$ be an $[n, k]$ code. Then a $k \times n$ matrix E whose rows are made up of any k linearly independent vectors of $\mathcal{C}$ is called the **generator matrix** of $\mathcal{C}$.

2.2 Inner products and the dual code.

A concept that pervades the whole of algebra is the formation of new structures from given old ones. Our definition of linear codes makes it clear that codes are nothing but subspaces of the vector space F^n. Suppose $\mathcal{C}$ is a given $[n, k]$ code. Further, suppose that $\mathcal{C}$ as a vector space is endowed with the standard inner product $<, >$, where for $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_n) \in \mathcal{C}$, we have $< u, v >= u_1v_1 + u_2v_2 + \cdots + u_nv_n$. Then we have a natural way of obtaining a new code from $\mathcal{C}$.

Definition 2.2.1. Let $\mathcal{C}$ be an $[n, k, d]$ code. The dual of $\mathcal{C}$, $\mathcal{C}^{\perp}$ is defined as :

$$\mathcal{C}^{\perp} := \{u | < u, v >= 0 \text{ for all } v \in \mathcal{C}\}.$$

It is not difficult to prove that $\mathcal{C}^{\perp}$ is a linear code, that is, a subspace of F^n.

Proposition 2.2.1. *Suppose $\mathcal{C}$ is an $[n, k]$ code. Then $\mathcal{C}^{\perp}$ is an $[n, n-k]$ code.*

Proof. Since $< \mathbf{0}, v >= 0$ for all $v \in \mathcal{C}$, we have $\mathcal{C}^{\perp} \neq \emptyset$. Let $c_1, c_2 \in \mathcal{C}^{\perp}, \alpha, \beta \in F$. Then

$$\begin{aligned} < \alpha c_1 + \beta c_2, c > &= \alpha < c_1, c > + \beta < c_2, c > \\ &= \alpha.0 + \beta.0, (c_1, c_2 \in \mathcal{C}^{\perp}.) \\ &= 0, \end{aligned}$$

for all $c \in \mathcal{C}$. It follows that $\alpha c_1 + \beta c_2 \in \mathcal{C}^{\perp}$ and by the Subspace Theorem of elementary linear algebra, $\mathcal{C}^{\perp}$ is a subspace of F^n. The last part is a standard linear algebraic result. □

Definition 2.2.2. Let $\mathcal{C}$ be a linear code. Then the **hull** of $\mathcal{C}$ is defined as the intersection $\mathcal{C} \cap \mathcal{C}^{\perp}$.

Definition 2.2.3. Let $\mathcal{C}$ be an $[n, k]$ code. A generator matrix of $\mathcal{C}^{\perp}$ is called the **parity check matrix** for $\mathcal{C}$.

Having defined the dual of a code, we can now give some important properties of some codes.

Definition 2.2.4. Let $\mathcal{C}$ be an $[n, k]$ code. Then $\mathcal{C}$ is said to be self-orthogonal if $\mathcal{C} \subset \mathcal{C}^{\perp}$. We say $\mathcal{C}$ is **self-dual** if $\mathcal{C} = \mathcal{C}^{\perp}$.

The focus of this work is on self-dual codes. We make a few notes concerning them.

Proposition 2.2.2. *Let $\mathcal{C}$ be an $[n, k]$ code. Then $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$.*

Proof. For all $c \in \mathcal{C}$, we have $< c, c^* >= 0$ for all $c^* \in \mathcal{C}^{\perp}$. It follows that $c \in (\mathcal{C}^{\perp})^{\perp}$ and $\mathcal{C} \subseteq (\mathcal{C}^{\perp})^{\perp}$. But $\dim((\mathcal{C}^{\perp})^{\perp}) = n - (n-k) = k = \dim(\mathcal{C})$, thus we must have $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$. □

For a self-dual code $\mathcal{C}$, we have $\dim(\mathcal{C}^{\perp}) = n - k = \dim(\mathcal{C}) = k$ so we have $n = 2k$ which is even. Therefore $k = \frac{n}{2}$.

2.3 Group action on codes

We recall a few facts about group action from elementary group theory.

Definition 2.3.1. Let G be a group and let X be a set. We say G acts on X (from the left) or X is a (left) G-set if there is a map

$$G \times X \to X,\ (g, x) \mapsto gx$$

satisfying

(1) $(gg')x = g(g'x)$, and

(2) $1_G x = x$

for all $x \in X$ and $g, g' \in G$.

If X is a G-set, then the **kernel** of the action of G on X is the set $K = \{g \in G |\ gx = x \text{ for all } x \in X\}$. We say G acts **faithfully** on X if the kernel K of the action is trivial, that is, the set $\{1_G\}$ containing only the identity element of G. An equivalent concept to the definition of the action of a group G on a set X is the condition that G be realised as a permutation group on X, that is, there is a group homomorphism $\phi : G \to S_X$.

Definition 2.3.2. Let X be a G-set and $x \in X$. The **stabilizer** of x under G, G_x is defined as $G_x := \{g \in G |\ gx = x\}$. The **orbit** of x under the action of G, denoted $\mathrm{Orb}_G(x)$, is the set

$$\mathrm{Orb}_G(x) := \{gx |\ g \in G\}.$$

It is easy to prove that the G-orbits partition X by defining an equivalence relation $\sim$ on $X : x \sim y$ if and only if there exists $g \in G$ such that $y = gx$. Further, G_x is a subgroup of G for every $x \in X$.

Definition 2.3.3. A G-set X is **transitive** if there is an $x \in X$ such that $\mathrm{Orb}_G(x) = X$, that is there is exactly one orbit under the action of G on X.

The following result is useful in the subsequent sections.

Theorem 2.3.1. *Let X be a transitive G-set and $x \in X$. Then the G-action on X is equivalent to the G-action on G/G_x, the set of all left cosets gG_x by multiplication on the left.*

Proof. We note that it is an elementary exercise to prove that G acts on left cosets of any subgroup by multiplication on the left. By transitivity all the elements of X are of the form $gx, g \in G$. Consider the mapping

$$\theta : G/G_x \to X, gG_x \mapsto gx.$$

Then the mapping is clearly surjective by the transitivity of X. Suppose that $\theta(gG_x) = \theta(hG_x)$ with $g, h \in G$. Then by definition, $gx = hx$. By the second axiom of a group action, Definition 2.3.1 (2), we have $x = 1x = g^{-1}gx = g^{-1}hx$ so $g^{-1}h \in G_x$ which forces $gG_x = hG_x$ establishing that θ is injective. Therefore, θ is a bijection. Take an arbitrary $y \in X$ and assume that $y' \in X$ is such that $y' = gy$. Set $y = g_0x, g_0 \in G$. Then y corresponds to the coset $\theta^{-1}(g_0x) = g_0G_x$. Because $y' = gy = g(g_0x) = gg_0x$, y' corresponds to the coset $\theta^{-1}(gg_0x) = gg_0G_x$. Thus when y uniquely maps to g_0G_x and vice versa, we see gy maps uniquely to gg_0H and conversely so G-actions on X and G/G_x correspond to each other by the bijection between them. □

Let $G \leq S_n$ be a permutation group. The natural action of the group G on the set $\Omega = \{1, 2, \ldots, n\}$ induces an action of G on a F^n (hence on any $[n, k]$ code) given by

$$\sigma(v) = v^\sigma := (v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(n)}),$$

where $v = (v_1, v_2, \ldots, v_n), \sigma \in G$. This action is equivalently given by $\sigma(v) = (v_{1^{\sigma^{-1}}}, v_{2^{\sigma^{-1}}}, \ldots, v_{n^{\sigma^{-1}}})$, where $i^{\sigma^{-1}} = \sigma^{-1}(i)$. In this dissertation we shall always use the former notation for the action of a permutation group on a code. With this notation, we see that $(v^\sigma)^\tau = v^{\tau\sigma}$.

Definition 2.3.4. Let $G \leq S_n$ be a permutation group and $\mathcal{C}$ be an $[n, k]$ code. Then

$$\sigma(\mathcal{C}) = \mathcal{C}^\sigma := \{\sigma(c) | c \in \mathcal{C}\}.$$

This brings us to an important concept in coding theory, namely that of code (in)equivalence.

Definition 2.3.5. Two $[n, k]$ codes $\mathcal{C}_1, \mathcal{C}_2$ are **equivalent** if there exists a permutation $\sigma \in S_n$ such that $\mathcal{C}_1 = \mathcal{C}_2^\sigma$.

The notion of equivalence of codes is important because codes which are equivalent have the same parameters and properties so the classification of codes is up to equivalence.

Definition 2.3.6. Let $G \leq S_n$ be a permutation group and $\mathcal{C}$ be an $[n, k]$ code. We define $G(\mathcal{C}) = \mathcal{C}^G := \{c^\sigma | c \in \mathcal{C}, \sigma \in G\}$. The code $\mathcal{C}$ is said to be G-invariant if $\mathcal{C}^G = \mathcal{C}$.

2.3.1 The automorphism group of a code

The concept of automorphisms is very important in algebra. In this section we briefly look at the automorphism groups of codes.

Definition 2.3.7. The set of automorphisms of an $[n, k]$ code $\mathcal{C}$, denoted $\mathrm{Aut}(\mathcal{C})$, is defined as :

$$\mathrm{Aut}(\mathcal{C}) := \{\sigma \in S_n | \mathcal{C}^\sigma = \mathcal{C}\}.$$

This is the set of all permutations which map $\mathcal{C}$ to itself.

It is an elementary group theory exercise to prove that $\mathrm{Aut}(\mathcal{C})$ is a group. The definition above is not general . It can be generalised through the study of isometries, so that field automorphisms are taken into account. Recall from elementary linear algebra that given a metric space V, an isometry is a mapping from V to itself that preserves distance. We give a formal definition below.

Definition 2.3.8. A mapping $\iota : F^n \to F^n$ is called an **isometry** if it respects the Hamming distance, that is $d(v, \mathbf{0}) = d(v^\iota, \mathbf{0})$.

Definition 2.3.9. A mapping $\sigma : F^n \to F^n$ is called **semilinear** if there exists an automorphism α of F such that for all $u, v \in F^n$ and $\kappa \in F$, the following holds:

(i) $\sigma(u + v) = \sigma(u) + \sigma(v)$ and

(ii) $\sigma(\kappa u) = \alpha(\kappa)\sigma(u)$.

This gives the following general setting for code equivalence.

Definition 2.3.10. Two codes $\mathcal{C}$ and $\mathcal{C}'$ are equivalent if there exists a semilinear isometry $\iota : F^n \to F^n$ such that $\mathcal{C}^\iota = \mathcal{C}'$.

Note that in the definition above we implicitly used the fact that linear codes are essentially metric spaces, namely Hamming subspaces, as they are equipped with a distance function, the Hamming distance. We have the following general definition of automorphisms of a linear code and the attendant automorphism group.

Definition 2.3.11. An **automorphism** of a linear code $\mathcal{C}$ is a semilinear isometry which maps $\mathcal{C}$ onto itself. These mappings form a subgroup $\mathrm{Aut}(\mathcal{C})$ of the group of all semilinear isometries. In other words, $\mathrm{Aut}(\mathcal{C})$ is the stabilizer of $\mathcal{C}$ in the isometry group G of Hamming space. Equivalently, this can be viewed as the image of the said subgroup in the group of permutations of $\mathcal{C}$.

Remark 2.3.2. Definitions 2.3.10 and 2.3.11 are generalizations of definitions 2.3.5 and 2.3.7 respectively. However, because we mostly consider binary codes in the cases where we use these concepts, we will subsequently use the later set for equivalence of codes and automorphism groups of codes respectively.

The Hamming space F^n has two natural sources of isometries. One can apply a permutation of F to each coordinate or an arbitrary permutation to the set of n coordinates. This generates a group G of $n!.q!^n$ isometries which is the wreath product, that is a semidirect product of S^n acting on $(S_q)^n$. It can be shown that in fact G is the full isometry group of the Hamming space.

We now give some results concerning the automorphism groups of codes and their duals. First we prove a very straight forward result about the standard inner product.

Lemma 2.3.3. *Let V be a subspace of the vector space F^n where F is a field and let $<,>$ be the standard inner product over V. If $G \leq S_n$ is a permutation group and V is G-invariant then $<,>$ is G-invariant.*

Proof. Let $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in V$ and $\sigma \in G$. Then

$$\begin{aligned} <\sigma(x), \sigma(y)> &= <(x_{1^\sigma}, x_{2^\sigma}, \ldots, x_{n^\sigma}), (y_{1^\sigma}, \\ &\quad y_{2^\sigma}, \ldots, y_{n^\sigma})> \\ &= \sum_{i=1}^{n} x_{i^\sigma} y_{i^\sigma} \\ &= \sum_{i'=1}^{n} x_{i'} y_{i'} \ (\ i^\sigma \in \{1, \ldots, n\}) \\ &= <x, y> \end{aligned}$$

so $<,>$ is G-invariant as required. □

We now state a result which establishes the relationship between $\mathrm{Aut}(\mathcal{C})$ and $\mathrm{Aut}(\mathcal{C}^\perp)$.

Proposition 2.3.4. *Let $\mathcal{C}$ be a code and $\mathcal{C}^\perp$ its dual. Then* $\mathrm{Aut}(\mathcal{C}) = \mathrm{Aut}(\mathcal{C}^\perp)$.

Proof. Let $\sigma \in \mathrm{Aut}(\mathcal{C})$. Then $\mathcal{C}^\sigma = \mathcal{C}$ and $\sigma^{-1} \in \mathrm{Aut}(\mathcal{C})$. Further, let $c \in \mathcal{C}$ and $c^* \in \mathcal{C}^\perp$ be arbitrary. It follows that

$$\begin{aligned} 0 &= < c, c^* > \text{ (By definition of } \mathcal{C}^\perp.) \\ &= < \sigma^{-1}(c), c^* > \ (\mathcal{C}^\sigma = \mathcal{C}.) \\ &= < \sigma^{-1}(c), \sigma^{-1}(\sigma(c^*)) > \\ &= < c, \sigma(c^*) > \text{ (By Lemma 2.3.3).} \end{aligned}$$

Therefore $\sigma(c^*) \in \mathcal{C}^\perp$ for all $\sigma \in \mathrm{Aut}(\mathcal{C}), c^* \in \mathcal{C}^\perp$. This shows that for any arbitrarily chosen $\sigma \in \mathrm{Aut}(\mathcal{C}), \mathcal{C}^\perp = (\mathcal{C}^\perp)^\sigma$ and $\sigma \in \mathrm{Aut}(\mathcal{C}^\perp)$. We then have the inclusion $\mathrm{Aut}(\mathcal{C}) \subseteq \mathrm{Aut}(\mathcal{C}^\perp)$. A reversal of the argument establishes the reverse inclusion from which equality follows. □

A consequence of this result which is of immense importance is that if a code $\mathcal{C}$ is G-invariant for some permutation group G, then $\mathcal{C}^\perp$ is also G-invariant.

2.4 Designs

Designs and codes have many links. Designs turn up in the study of codes and vice versa. In this section we introduce some elementary ideas of design theory.

Definition 2.4.1. A t-(v, k, λ) design is a collection D of k-subsets, called blocks, of a set X of v points such that any t-subset of X is contained in exactly λ blocks of D. The parameters t, v, k, λ are such that $v > k > t > 0$ and $\lambda > 0$.

Definition 2.4.2. Two designs having the same parameters t, v, k, λ are **isomorphic** if there is a bijection between their point sets mapping the blocks of one design to the blocks of the other.

A t-$(v, k, 1)$ design is called a **Steiner system**. These special designs are customarily given by the notation $S(t, k, v)$.

Definition 2.4.3. A projective plane of order n is an $S(2, n+1, n^2+n+1)$ Steiner system.

Definition 2.4.4. The block intersection numbers of a design D are the cardinalities of the intersections of any two distinct blocks.

Definition 2.4.5. A t-(v, k, λ) design is **self-orthogonal** if the block intersection numbers have the same parity as the block size k. Further, a 2-(v, k, λ) design is **symmetric** if all block intersection numbers are λ.

The concept of self-orthogonal designs was introduced by V. D. Tonchev [46].

Remark 2.4.1. In the literature, it is more common to define a symmetric design as a design in which the number of blocks equals the number of points. However, from this definition we can show equivalence with the one given above.

Definition 2.4.6. *(Incidence Matrix)*
Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a t-(v, k, λ) design where $\mathcal{P} = \{p_1, p_2, \ldots, p_v\}$ is the point set of the design, $\mathcal{B} = \{B_1, B_2, \ldots, B_k\}$ is the set of blocks of the design and $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$. Then **the incidence matrix** of $\mathcal{D}$ is defined to be the matrix $A = [a_{ij}]_{k \times v}$, where

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

The concept of a code being a vector space naturally lends to a description of codes as spaces spanned by some q-ary vectors, where $F = F_q$ is the ground field over which the vector space is defined. Often times it is a matter of expediency that one consider codes as subspaces of vector spaces spanned by sets. Such considerations arise in the study of codes obtained from combinatorial designs for example. Because of our construction in Chapter 5, we are interested in such considerations. The following notation follows that of Assmus and Key [5].

Definition 2.4.7. For a field F and a set Ω, denote by F^Ω the vector space of functions from Ω to F with addition and multiplication being point-wise. For a subset Y of Ω, denote the characteristic function on Y by the vector v^Y, that is ,

$$v^Y(\omega) = \begin{cases} 1 & \text{if } \omega \in Y \\ 0 & \text{otherwise.} \end{cases}$$

We can easily show that the standard basis for F^Ω is $\{v^{\{\omega\}} | \omega \in \Omega\}$. The standard basis for F^n, the space of n-tuples, has a natural ordering through

the numbers 1 to n. To avoid ordering, we may take $V = F^X$, where X is a set of cardinality n. Then by the foregoing discussion, a code is a subspace of V whose basis is specified through the coordinate functions v^i, for $i \in X$, that is $v^i(i) = 1$ and $v^i(j) = 0$ for $j \neq i$. Note that for the case where Ω is a singleton we may write v^ω for $v^{\{\omega\}}$ where there is no danger of confusion.

Definition 2.4.8. Let V be a vector space. Then by V^* we denote the dual space of V, the space of all linear transformations from V to the 1-dimensional vector space F. Let C be a subspace of $V = F^n$. Then the functionals, $\varphi_i : C \to F$ for $i \in \{1, 2, \ldots, n\}$ are defined by $c\varphi_i = c_i$ where c_i is the i-th coordinate of c, that is, $c = (c_1, c_2, \ldots, c_n)$. It follows that $\varphi_i \in C^*$, the dual of C. We use this to define codes spanned by sets. This follows from the ideas expressed by Assmus and Mattson in their expository paper [6]. The next result is taken from [5].

Proposition 2.4.2. *Let U be a vector space of dimension k over the field $F = F_q$ and let S be a sequence, $\{f_1, \ldots, f_n\}$ of functionals in U^* such that S spans U^*. Taking $V = F^n$, the set*

$$C = \{(f_1(u), f_2(u), \ldots, f_n(u)) | u \in U\}$$

is a linear code of length n and dimension k over F.

Proof. Let $\theta : U \to F^n, \theta(u) = (f_1(u), f_2(u), \ldots, f_n(u))$. Then

$$\begin{aligned} \theta(u+v) &= (f_1(u+v), f_2(u+v), \ldots, f_n(u+v)) \\ &= (f_1(u) + f_1(v), f_2(u) + f_2(v), \ldots, f_n(u) + f_n(v)) \\ &= (f_1(u), f_2(u), \ldots, f_n(u)) + (f_1(v), f_2(v), \ldots, f_n(v)) \\ &= \theta(u) + \theta(v), \end{aligned}$$

using the fact that the f_i are linear functionals and the definition of function addition. It follows that θ is linear. Because the functionals span U^*, the kernel of θ is $\{0\}$. Thus C has dimension k as required. □

Chapter 3

Background from Group Representation Theory

In this chapter we show how G-invariant linear codes can be viewed as FG-modules. We discuss the rudiments of modules and representation theory. Throughout this chapter G denotes a finite group and R is a commutative unital ring, unless stated otherwise. Further, provided the contrary has been declared, we assume F to be a field, unless stated otherwise.

3.1 Basics

In this section a brief background of the module theory required in this survey up to the level of self-containment is given.

Definition 3.1.1. Let R be a ring. Then A_R, or just A if the context is clear, is a **right R-module** if A is an abelian group, written additively, and there is a map $\theta : A \times R \to A$

$$\theta((a, r)) = ar$$

which satisfies

1) $(a + b)r = ar + br$,

2) $a(r + s) = ar + as$,

3) $a(rs) = (ar)s$,

4) $a1_R = a$.

Thus left modules can be defined analogously with multiplication by the elements of the ring on the left instead of the right. If a module is finitely generated by a subset and has a basis then such a module is referred to as a **free module**.

Definition 3.1.2. The **right regular R-module** R_R (analogously ${}_RR$ for left modules) is defined to be the additive group of R made into a right (respectively left) module by multiplication to the right (respectively left).

Because of convenience, from now on we will assume that every module is a left module.

Definition 3.1.3. Let M be an R-module. Then a subgroup $N \leq M$ is a **submodule** of M if for all $r \in R$ and $n \in N, rn \in N$.

Definition 3.1.4. Let M and N be R-modules. Then a group homomorphism $f : M \to N$ is an **R-module homomorphism** if for all $r \in R$ and $m \in M, f(rm) = rf(m)$.

The concept of modules is a generalisation of the notion of vector spaces over arbitrary rings instead of fields. If F is a given field and G is a finite group, then the study of FG-modules will be of central importance.

Definition 3.1.5. Let F be a field and V be a finite dimensional vector space over F. A **representation** ρ is a homomorphism from G to $GL(V)$, the group of all invertible linear transformations over V. The dimension $n = \dim_F(V)$ of V is called the **degree** of the representation.

If V is of dimension $\dim(V) = n$ and a basis $\mathcal{B}$ is chosen for V, then we can obtain an isomorphism from $GL(V)$ to $GL(n, F)$. Therefore we have the following equivalent concept of group representations.

Definition 3.1.6. Let G be a finite group and let F be a commutative ring of coefficients. A **representation** of G over F is a group homomorphism $G \to GL(n, F)$ for some n.

The later definition is usually called the matrix representation.

Definition 3.1.7. A representation $\rho : G \to GL(V)$ is **faithful** if $\ker(\rho) = \{1_G\}$.

Certain authors sometimes refer to a representation $\rho : G \to GL(V)$ as an F-representation of G on V. As usual the **group algebra** FG consists of linear combinations of elements of G with coefficients in F. Addition and multiplication are defined as follows:

$$\begin{aligned}\left(\sum_{g\in G}\alpha_g g\right)+\left(\sum_{g\in G}\beta_g g\right) &= \sum_{g\in G}(\alpha_g+\beta_g)g,\\ \left(\sum_{g\in G}\alpha_g g\right)\left(\sum_{g\in G}\beta_g\right) &= \sum_{g\in G}\left(\sum_{hh'=g}\alpha_h\beta_{h'}\right)g.\end{aligned}$$

The structure FG is a ring, an F-algebra even.

Remark 3.1.1. An **R-algebra** is a ring A together with a ring homomorphism $\lambda_A : R \to Z(A)$ satisfying $\lambda_A(1_R) = 1_A$, where $Z(A)$ is the centre of A.

Definition 3.1.8. Let $\rho : G \to GL(V)$ be an F-representation. The **centralizer** of ρ is the algebra of all linear transformations $A : V \to V$ for which $A\rho(g) = \rho(g)A$ for all $g \in G$. If $\bar{\rho}$ is a matrix representation, the **centralizer algebra** is the algebra of all $n \times n$ matrices which commute with $\bar{\rho}(g)$ for all $g \in G$.

3.1.1 The link between codes and FG-modules

Here we give the important link between linear codes and FG-modules which will be of importance in the sequel. Given a representation $\varphi : G \to GL(n, F)$, $V = F^n$ is made into a FG-module via

$$(\sum_{g\in G}\alpha_g g).v := \sum_{g\in G}\alpha_g\varphi(g)(v), \quad v \in V.$$

Conversely, provided that an FG-module M, regarded as an F-module via the inclusion $F \hookrightarrow FG$, is finitely generated and free, a representation $\varphi : G \to GL(n, F)$ can be obtained by choosing an F-basis for M and setting $\varphi(g)(v) = g.v, \quad g \in G, v \in V$. It follows from the definition of linear codes as subspaces of F^n for some finite field F that they are simply FG-submodules. Thus, for a permutation group G, the G-invariant codes are precisely the FG-submodules of F^n.

Example 3.1.2. For a field F the representations of G correspond to finite dimensional FG-modules.

Definition 3.1.9. Two representations
$\varphi : G \to GL(n, F)$ and $\psi : G \to GL(m, F)$, are **similar** if $n = m$ and there exists $X \in GL(n, F)$ such that $X\varphi(g)X^{-1} = \psi(g)$ for all $g \in G$. In general an intertwining operator is an $n \times m$ matrix X with the property that

$$\varphi(g)X = X\psi(g), \forall g \in G.$$

This is equivalent to a homomorphism between the corresponding FG-modules.

Example 3.1.3. For $G = \mathbb{Z}/2\mathbb{Z} = \{1, t\}, F = \mathbb{F}_2$, define $\varphi : G \to GL(2, F)$ by

$$\varphi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \varphi(t) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Then the corresponding FG-module is given by

$$\begin{aligned}
(\sum_{g\in G} \mu_g g).v &= \sum_{g\in G} \mu_g \varphi(g)(v) \\
&= (\alpha.1 + \beta.t)v \\
&= (\alpha\varphi(1) + \beta\varphi(t))v \\
&= \left(\alpha \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \beta \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) \begin{pmatrix} x \\ y \end{pmatrix} \\
&= \left(\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} + \begin{pmatrix} \beta & \beta \\ 0 & \beta \end{pmatrix}\right) \begin{pmatrix} x \\ y \end{pmatrix} \\
&= \begin{pmatrix} \alpha + \beta & \beta \\ 0 & \alpha + \beta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\
&= \begin{pmatrix} (\alpha + \beta)x + \beta y \\ (\alpha + \beta)y \end{pmatrix}.
\end{aligned}$$

3.1.2 The dual of a module.

The concept of dual modules will be important in establishing a criterion for the existence of self-dual codes invariant under some permutation group. We give the definition of this notion below.

Definition 3.1.10. Let V be a right FG-module. Then the **dual module**, $V^* = \mathrm{Hom}_F(V, F)$, the set of all homomorphisms from V to F is a right FG-module where if $f \in V^*, g \in G$ and $v \in V$, then $fg(v) := f(vg^{-1})$. The module V^* is called the **contragredient** module to V. If $V \cong V^*$ then we say V is **self-dual**.

3.2 Reducibility and decomposability

Before we discuss the important subject of decomposition and irreducibility, we give a definition of invariant spaces.

Definition 3.2.1. Let ρ be a representation of G on V. Then a subspace W of V is **ρ-invariant** if $\rho(g)W \subseteq W$ for all $g \in G$.

Definition 3.2.2. A representation $\varphi : G \to GL(n, F)$ is **reducible** if it is similar to a representation ψ such that

$$\psi(g) = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \ \forall g \in G.$$

A representation is **irreducible** if it is non-zero and not reducible.

Given an n-dimensional vector space, the subspace spanned by the first $i < n$ basis vectors is an invariant subspace. ($W \leq V$ is invariant if $gw \in W \ \forall g \in G, \forall w \in W$.)

Definition 3.2.3. Let F be a commutative unital ring (not necessarily a filed). An FG-module V is **reducible** if there is a submodule W of V with $0 \neq W \neq V$. Provided that F is a field this concept corresponds to the reducibility of the representation. A FG-module is **irreducible** or **simple** if it is non-zero and not reducible.

Definition 3.2.4. A representation $\varphi : G \to GL(n, F)$ is **decomposable** if it is similar to a representation ψ such that

$$\psi(g) = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}, \forall g \in G.$$

This says that $V = W_1 \oplus W_2, \dim(W_1) = i, \dim(W_2) = j$ with W_1, W_2 invariant subspaces.

Definition 3.2.5. A FG-module V is **decomposable** if $V = W_1 \oplus W_2$ with W_1, W_2 non-zero submodules of V. If V is non-zero and not decomposable, then V is **indecomposable**. We say that V is **completely reducible** or **semisimple** if it can be written as a direct sum of irreducible submodules.

We now define absolutely irreducible representations but we will try to avoid using the technicalities of tensor products in our definition. From elementary algebra we recall that if F is a field and K is another field with $F \subseteq K$, then we say K is an extension of F.

Definition 3.2.6. Let $\rho : G \to GL(V)$ be an F-representation of G. We say the representation ρ is **absolutely irreducible** if it is irreducible for any extension K of F. If K is the smallest field containing F such that all the F representations of G are absolutely irreducible, then any extension field $K \subseteq L$ containing K is called a **splitting** field for G.

It was shown in Section 3.1 that having a representation of G is equivalent to having an FG-module so the definition above can be equivalently stated in terms of FG-modules.

Lemma 3.2.1. (Schur's Lemma) *Suppose ρ and φ are irreducible F-representations of G on vector spaces V and W respectively, and $\psi : V \to W$ is a linear transformation such that*

$$\psi\rho(g) = \varphi(g)\psi$$

for all $g \in G$. Then $\psi = 0$ or else ψ is an isomorphism (hence $\rho \sim \varphi$.)

Proof. Suppose that $\psi \neq 0$. Let $V_1 = \ker(\psi)$ and $W_1 = \mathrm{Im}(\psi)$. If $v \in V_1$, then $0 = \varphi(g)\psi v = \psi\rho(g)v$ for all $g \in G$, so $\rho(g)v \in \ker(\psi)$ and $\rho(g)V_1 \subseteq V_1 = \ker(\psi)$, that is V_1 is ρ-invariant. But $V_1 \neq V$ so $V_1 = 0$ since ρ is irreducible and hence ψ is injective.

If $w \in W_1$, write $w = \psi(u), u \in V$. Then

$$\begin{aligned} \varphi(g)w &= \varphi(g)\psi(u) \\ &= \psi(\rho(g)u) \in \mathrm{Im}(\psi) = W_1 \end{aligned}$$

for all $g \in G$. Therefore W_1 is φ-invariant and non-zero, so $W_1 = W$ by irreducibility. It follows that ψ is surjective. Thus ψ is a bijection so an isomorphism. □

3.3 Homomorphisms, tensors and exact sequences

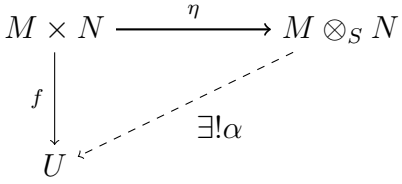
The study of the set of all homomorphisms from one algebraic structure to another gives insight into the properties of the structures themselves. Tensor products, which are defined in terms of homomorphisms, provide a way of constructing new modules from old ones. The study of these is the basis for this section. First the concept of bimodules is introduced.

Definition 3.3.1. Let R, S be rings. A commutative group A, additively written, is an $(\mathbf{R}, \mathbf{S})$**-bimodule** if it is a left R-module and it is also a right R-module.

Definition 3.3.2. Let R, S be rings, M an (R, S)-bimodule and N an S-module. The map $f : M \times N$ to an R-module U is **balanced** if

- $f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n)$, for all m_1, m_2 in M and $n \in N$.
- $f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2)$ for all $m \in M, n_1, n_2 \in N$.
- $f(ms, n) = f(m, sn)$ for all $m \in M, n \in N$ and $s \in S$.
- $f(rm, n) = rf(m, n)$ for all $m \in M, n \in N$ and $r \in R$.

Definition 3.3.3. Let R, S, M and N be as in the previous definition. The **tensor product** of M and N over S is an R-module denoted by $M \otimes_S N$, equipped with a balanced map $\eta : M \times N \to M \otimes_S N$ such that if U is an R-module and $f : M \times N \to U$ is a balanced map there is a unique R-module homomorphism $\alpha : M \otimes_S N \to U$ such that $f = \alpha \circ \eta$, or such that the following diagram commutes:



Tensor products exist and are unique up to isomorphism. We write $m \otimes n = \eta(m, n)$ for some $m \in M$ and $n \in N$. The tensor product $M \otimes_S N$ is the R-module generated by the set $\{m \otimes n | m \in M, n \in N\}$ where $m \otimes n$ satisfies:

(1) $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$ for all $m_1, m_2 \in M$ and $n \in N$,

(2) $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$ for all $m \in M$ and $n_1, n_2 \in N$,

(3) $(ms) \otimes n = m \otimes (sn)$ for all $m \in M, n \in N$ and $s \in S$.

Example 3.3.1. Consider the case where R is a field F and U and V are finite-dimensional F-vector spaces. Then U is an (F, F)-bimodule so that the vector space $U \otimes_F V$ can be constructed. If $\{u_1, \cdots, u_r\}$ and $\{v_1, \cdots, v_s\}$ are bases for U and V respectively, then $U \otimes_F V$ is an rs-dimensional F-vector space having as a basis the set $\{u_i \otimes v_j | \ 1 \leq i \leq r, 1 \leq j \leq s\}$. If $u = \sum_i a_i u_i \in U$ and $v = \sum_j b_j v_j \in V$, then $u \otimes v = \sum_{i,j} a_i b_j (u_i \otimes v_j)$.

Example 3.3.2. If R is a commutative ring then left and right modules are equivalent. Given any two (left) R-modules M and N, $M \otimes_R N$ can be formed and this again is an R-module via

$$r(m \otimes n) = rm \otimes n = m \otimes rn, \ r \in R, m \in N, n \in N.$$

A ring R can be regarded as an (R, R)-bimodule via left and right multiplication. If S is a subring of R, R can similarly be regarded as an (R, S)-bimodule. If H is a subgroup of G, then FH can be regarded as a subring of FG and FG is viewed as a (FG, FH)-bimodule. If M is a FH-module, $FG \otimes_{FH} M$ is a left FG-module called the **induced module** $M \uparrow^G$. In this work we also use the notation Ind_H^G for induced modules. The group $\mathrm{Hom}(N, \mathrm{Hom}(M, A))$ corresponds bijectively to the set of bilinear maps $M \times N \to A$. The right action of R on M gives a left action of R on $\mathrm{Hom}(M, A)$ by $(r\varphi)(m) = \varphi(mr)$ where $\varphi \in \mathrm{Hom}(M, A), m \in M$ and $r \in R$. Thus it makes sense to look at $\mathrm{Hom}(N, \mathrm{Hom}(M, A))$. It corresponds bijectively to the set of R-balanced bilinear maps $M \times N \to A$. Hence the definition of the general tensor product given (also called the universal property of tensor products) gives an isomorphism of abelian groups

$$\mathrm{Hom}_R(N, \mathrm{Hom}(M, A)) \cong \mathrm{Hom}_S(M \otimes_R N, A).$$

If M is an (S, R)-bimodule and A is a left S-module then this isomorphism restricts to

$$\mathrm{Hom}_R(N, \mathrm{Hom}_S(M, A)) \cong \mathrm{Hom}_S(M \otimes_R N, A).$$

In particular we have

$$\mathrm{Hom}_{FH}(U, \mathrm{Hom}_{FG}(FG, V)) \cong \mathrm{Hom}_{FG}(FG \otimes_{FH} U, V).$$

Since FG is viewed as a (FG, FH)-bimodule,we can regard $\mathrm{Hom}_{FG}(FG, V)$ as a left FH-module by restriction, $V\downarrow_H$. Thus the isomorphism theorem of Nakayama or the *Frobenius Reciprocity Theorem*

$$\mathrm{Hom}_{FH}(U, V\downarrow_H) \cong \mathrm{Hom}_{FG}(U\uparrow^G, V)$$

is obtained. If U and V are two FG-modules, then $U \otimes_F V$ becomes an FG-module via

$$g(u \otimes v) = gu \otimes gv,\ g \in G, u \in U, v \in V.$$

Remark 3.3.3. Elements of the group algebra FG act in a way extended linearly from the action of G. From this we deduce that

$$\begin{aligned}(g+h)(u\otimes v) &= gu\otimes gv + hu\otimes hv\\ &\neq (g+h)u\otimes(g+h)v,\end{aligned}$$

where $g, h \in G, u \in U$ and $v \in V$.

Similarly, $\mathrm{Hom}_F(U, V)$ becomes an FG-module: if $f \in \mathrm{Hom}_F(U, V)$ and $g \in G$,

$$(gf)(u) = f(g^{-1}u).$$

With these definitions, if U, V and W are FG-modules, then

$$\mathrm{Hom}_F(U, \mathrm{Hom}_F(V, W)) \cong \mathrm{Hom}_F(U \otimes_F V, W)$$

is an isomorphism of FG-modules. Taking G-fixed points on both sides,

$$\mathrm{Hom}_{FG}(U, \mathrm{Hom}(V, W)) \cong \mathrm{Hom}_{FG}(U \otimes_F V, W)$$

is obtained.

Definition 3.3.4. A **short exact sequence** of FG-modules is a sequence of FG-modules and FG-module homomorphisms of the form

$$0 \to V_1 \to V_2 \to V_3 \to 0$$

such that for each pair of composable arrows the image of the left one is the kernel of the right one. A short exact sequence

$$0 \to V_1 \xrightarrow{\alpha} V_2 \xrightarrow{\beta} V_3 \to 0$$

is **split** if there is a map $V_3 \xrightarrow{\gamma} V_2$ (a *splitting*) such that $\beta \circ \gamma = \mathrm{id}_{V_3}$.

In the case of a split short exact sequence in Definition 3.3.4 $V_2 = \alpha(V_1) \oplus \gamma(V_3) \cong V_1 \oplus V_3$. This is because for a short exact sequence the homomorphisms α, β are necessarily injective and surjective respectively. Further, given $v_2 \in V_2, \beta(v_2) \in V_3$ and $\gamma(\beta(v_2)) \in V_2$. Taking an element $z = v_2 - \gamma(\beta(v_2)) \in V_2$, then

$$\begin{aligned} \beta(z) &= \beta(v_2 - \gamma(\beta(v_2))) \\ &= \beta(v_2) - \beta(\gamma(\beta(v_2))) \\ &= \beta(v_2) - \mathrm{id}_{V_3}(\beta(v_2)) \\ &= \beta(v_2) - \beta(v_2) = 0. \end{aligned}$$

Thus $z \in \ker(\beta) = \mathrm{Im}(\alpha) = \alpha(V_1)$, since the sequence is short exact. Therefore, $v_2 = z + \gamma(\beta(v_2)) \in \alpha(V_1) + \gamma(V_3)$, where $\beta(V_3) = V_3$ by surjectivity of β. Hence $V_2 = \alpha(V_1) + \gamma(V_3)$. It remains to show that the sum is direct. Suppose that $v_2 \in \alpha(V_1) \cap \gamma(V_3)$. Then $v_2 = \alpha(v_1)$ for some $v_1 \in V_1$. But then $\alpha(V_1) = \ker(\beta)$ so $\beta(\alpha(v_1)) = 0$. Since $v_2 = \alpha(v_1) \in \gamma(V_3), \alpha(v_1) = \gamma(v_3)$ for some $v_3 \in V_3$. Thus $0 = \beta(\gamma(v_3)) = \beta \circ \gamma(v_3) = v_3$ from which $v_2 = \alpha(v_1) = \gamma(v_3) = 0$. This establishes the directness of the sum. The map

$$\theta : \alpha(V_1) \oplus \gamma(V_3)$$

such that

$$\alpha(v_1) + \gamma(v_3) \mapsto v_1 + v_3$$

furnishes the required isomorphism.

Remark 3.3.4. Given a short exact sequence

$$0 \to V_1 \to V_2 \to V_3 \to 0,$$

we may represent it as below in matrix notation

$$0 \to (\varphi) \to \begin{pmatrix} (\varphi) & * \\ 0 & (\psi) \end{pmatrix} \to (\psi) \to 0.$$

The notion of short exact sequences is a particular case of the notion of exact sequences which will be defined below.

Definition 3.3.5. Let R be a ring and $M_1, M_2, \cdots, M_n$ be R-modules. A sequence $M_1 \overset{f_1}{\to} M_2 \overset{f_2}{\to} M_3 \overset{f_3}{\to} \cdots \overset{f_{n-2}}{\to} M_{n-1} \overset{f_{n-1}}{\to} M_n$ of R-homomorphisms f_i is **exact** at M_i if $\mathrm{Im} f_{i-1} = \ker f_i$. The sequence is exact if it is exact at each $M_i, i \in \{2, \cdots, n\}$.

If L is a submodule of M, then $0 \to L \stackrel{1_L}{\to} M \stackrel{\text{nat}}{\to} M/L \to 0$ is exact. Conversely, if $0 \to L \stackrel{f}{\to} M \stackrel{g}{\to} M/L \to 0$ is exact, then $L \cong f(L)$, a submodule of M and $N \cong M/f(L)$. The following lemma follows naturally from the definition.

Lemma 3.3.5. *Assume that $0 \to L \stackrel{f}{\to} M \stackrel{g}{\to} N \to 0$ is an exact sequence of R-modules. Then the following are equivalent:*

(1) There is an R-map $i : N \to M$ with $g \circ i = 1_N$ (splitting),

(2) There is an R-map $j : M \to L$ with $j \circ f = 1_L$,

(3) For some submodule M_1 of M, $M = f(L) \oplus M_1$ and $M_1 \cong N$.

Proof. It can easily be proven that (1) and (2) are equivalent to (3). □

At this stage a module-theoretic version of Maschke's Theorem can be stated.

Theorem 3.3.6. (Maschke's Theorem) *If $|G| \in F^\times$ and $0 \to V_1 \stackrel{\alpha}{\to} V_2 \stackrel{\beta}{\to} V_3 \to 0$ is a short exact sequence of k-modules then it splits as a short exact sequence of FG-modules.*

Proof. Given a k-splitting $\varphi : V_3 \to V_2$, set
$\gamma = \frac{1}{|G|} \sum_{g \in G} g^{-1} \varphi g$. If $x \in V_3$,

$$\beta\gamma(x) = \frac{1}{|G|} \sum_{g \in G} \beta g^{-1} \varphi g x = \frac{1}{|G|} \sum_{g \in G} g^{-1} \beta \varphi x g = x,$$

since $\beta \circ \gamma = \mathrm{id}_{V_3}$. Thus γ is an FG-splitting. Further, if $h \in G$, then

$$\begin{aligned} \gamma(hx) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \varphi g h x &= \frac{1}{|G|} \sum_{g \in G} h h^{-1} g^{-1} \varphi g h x \\ &= h \frac{1}{|G|} \sum_{g \in G} (gh)^{-1} \varphi (gh) x \\ &= h\gamma(x). \end{aligned}$$

□

Equivalently, we can say that under the hypothesis of the theorem above, every FG-module is completely reducible.

3.4 Structure theorems

In this section we state without proof two important structure theorems which we need in subsequent sections, namely the Jordan-Hölder Theorem and the Wedderburn Structure Theorem, which is sometimes referred to as the Artin-Wedderburn Theorem.

Definition 3.4.1. A module M has a composition series if there exists a finite series of submodules $M = M_k \supset M_{k-1} \supset \cdots \supset M_1 \supset M_0 = \{0\}$ such that the quotient modules M_i/M_{i-1} are simple for all $1 \leq i \leq k$. The modules M_i/M_{i-1} are called composition factors of the series and k is called the length of the series. Two composition series are equivalent if there is an isomorphism between the composition factors.

Theorem 3.4.1. (Jordan-Hölder) *If a module V has a composition series then any two composition series are equivalent.*

Theorem 3.4.2. (Wedderburn Structure Theorem).
Let R be a finite-dimensional algebra over a finite field F and suppose that R is semisimple. Then

$$R \cong \prod_{i=1}^{m} \mathrm{Mat}_{d_i}(\Delta_i)$$

where Δ_i is a division ring containing F in its centre and finite-dimensional over F and $\mathrm{Mat}_{d_i}(\Delta_i)$ denotes the ring of all $d_i \times d_i$ matrices over the division ring Δ_i.

3.5 Characters

As it may not be easy to deal computationally with FG-modules especially when the degrees of the corresponding representations are large as finding all FG-submodules is a computationally intractable problem. However, there is an equivalent way which is relatively easier to handle, namely character theory. In this section we introduce some basic notions of character theory and use them to show how an existence criterion for self-dual binary codes can be tested computationally.

Definition 3.5.1. Let $T : V \to V$ be a linear transformation. Then we define $\mathrm{tr}(T) = \mathrm{tr}(A)$ for any representing matrix A of T. As usual if $A = [a_{ij}]_{n \times n}$, then $\mathrm{tr}(A) = \sum_{i=1}^{n} a_{ii}$.

It is an exercise in elementary Linear Algebra to show that $\mathrm{tr}(AB) = \mathrm{tr}(BA)$. We will use this simple yet useful result in some work that follows.

Definition 3.5.2. If ρ is an F-representation of G then the **character** $\chi = \chi_\rho$ of ρ (or afforded by ρ) is the function from G to F defined by

$$\chi(g) = \mathrm{tr}(\rho(g))$$

for all $g \in G$.

All the adjectives used to describe representations can be used with characters as well, for example reducible, irreducible, faithful, linear and so on. We now give the following simple but extremely useful result.

Proposition 3.5.1. *Let $\chi = \chi_\rho$ be a character of G. Then χ is a class function, that is it is constant on conjugacy classes of G.*

Proof. If $g, h \in G$ then

$$\begin{aligned}
\chi(g^{-1}hg) &= \mathrm{tr}(\rho(g^{-1}hg)) \\
&= \mathrm{tr}(\rho(g^{-1})\rho(h)\rho(g)) \\
&= \mathrm{tr}(\rho(h)\rho(g^{-1})\rho(g)), \ (\mathrm{tr}(AB) = \mathrm{tr}(BA)) \\
&= \mathrm{tr}(hg^{-1}g) \\
&= \mathrm{tr}(\rho(h)) = \chi(h)
\end{aligned}$$

□

Proposition 3.5.2. *If ρ, φ are equivalent as F-representations of G, then*

$$\chi_\rho = \chi_\varphi.$$

Proof. For suitable chosen bases, $[\rho] = [\varphi]$, where $[\rho], [\varphi]$ are the matrix representations corresponding to ρ, φ respectively. □

Proposition 3.5.3. *If ρ, φ are F-representations, then*

$$\chi_{\rho\oplus\varphi} = \chi_\rho + \chi_\varphi.$$

Proof. Since $[\rho \oplus \varphi]$ is similar to $\begin{pmatrix} [\rho] & 0 \\ 0 & [\varphi] \end{pmatrix}$ the result is clear. □

Corollary 3.5.4. *Suppose* $\mathrm{char}(F) \nmid |G|$ *and that* χ *is an* F*-character of* G*. Then there are irreducible* F*-characters* $\chi_1, \ldots, \chi_k$ *of* G *such that*

$$\chi = \chi_1 + \cdots + \chi_k.$$

Proof. Let $\chi = \chi_\rho$ for some F-representation ρ. Then by Maschke's Theorem, we have

$$\rho \sim \rho_1 \oplus \rho_2 \oplus \cdots \oplus \rho_k.$$

Let χ_i be the character afforded by ρ_i for each i. Applying Proposition 3.5.3 the result follows. □

We define the concept of inner products of functions.

Definition 3.5.3. If φ and θ are functions from G to F define a symmetric bilinear form on the space of all functions $f : G \to F$ by

$$< \varphi, \theta >= \sum_{g \in G} \varphi(g)\theta(g^{-1}).$$

Many results in ordinary representation and character theory require the field to be algebraically closed. As a result the field $\mathbb{C}$ is often used as a ground field, or in some instances its subfields which are splitting fields for a given group G.

Theorem 3.5.5. *If* $F \subseteq \mathbb{C}$ *is a splitting field for* G*, and if* $\chi_1, \ldots, \chi_k$ *are all absolutely irreducible* F*-characters of* G*, then*

$$< \chi_i, \chi_j >= \delta_{ij}$$

for all i, j*.*

Proof. This is a special case of a result proved in the standard texts of the subject which states that the inner product of two distinct irreducible characters of G is zero and that the inner product of an irreducible character with itself is 1. □

Corollary 3.5.6. *If* $\chi_1, \ldots, \chi_r$ *are all absolutely irreducible characters of* G *and* χ *is any* F*-character, then*

$$\chi = \sum_{i=1}^{r} < \chi, \chi_i > \chi_i.$$

Proof. From Corollary 3.5.4, $\chi = \sum_{i=1}^{r} n_i\chi_i$ where $0 \leq n_i \in \mathbb{Z}$ for all i. Thus

$$\begin{aligned} < \chi, \chi_j > &= < \sum_{i=1}^{r} n_i\chi_i, \chi_j > \\ &= \sum_{i=1}^{r} n_i < \chi_i, \chi_j > \\ &= \sum_{i=1}^{r} n_i\delta_{ij} \\ &= n_j \end{aligned}$$

for all j. □

All the irreducible characters χ_i for which $< \chi, \chi_i > \neq 0$ are called the **constituents** of χ and the integers $n_i =< \chi, \chi_i >$ are called the **multiplicities** of the constituents.

3.6 Brauer characters

In the previous sections many of the results relied on the fact that the characteristic of the field does not divide the order of the group. However, in the study of G-invariant codes it is often the case that the characteristic of the field divides the order of the group. Thus a need arises to develop a theory that will work in the event that this important condition is not met. In this section we will briefly discuss modular characters. Let M be a $\mathbb{C}G$-module. Then there is a class function

$$\chi_M : \{\text{conjugacy classes of G}\} \to \mathbb{C}$$

given by $g \mapsto \text{tr}(g, M)$. The following proposition is a characterization of ordinary characters of finite groups. We will state it without proof here.

Proposition 3.6.1. *Let M and M' be $\mathbb{C}G$-modules. Then the following holds for characters χ of G.*

(1) $\chi_{M\oplus M'} = \chi_M + \chi_{M'}$.

(2) $\chi_{M\otimes M'} = \chi_M\chi_{M'}$.

(3) If $\chi_M = \chi_{M'}$, then $M \cong M'$.

The goal of this section is to develop character theory over fields of non-zero characteristics p, p prime, such that (1) and (2) hold and $\chi_M = \chi_{M'}$ if and only if M and M' have the same composition factors with the same multiplicities. However, we soon have a problem. If M is a direct sum of p copies of M', then for all $g \in G, \mathrm{tr}(g, M) = p.\mathrm{tr}(g, M') = 0$. Thus Brauer character theory has to be used in such cases.

Theorem 3.6.2. *Let F be an algebraically closed field of characteristic p, p a prime. Then the following are equivalent.*

(i) For all $g \in G$, $tr(g, M) = tr(g, M')$.

(ii) For each simple FG-module S, the multiplicities of S as a composition factor of M and M' are congruent modulo p.

Proof. For $0 \to M_1 \to M_2 \to M_3 \to 0$, the following situation arises:

$$M_2 = \begin{pmatrix} M_1 & * \\ 0 & M_3 \end{pmatrix}.$$

Thus $\mathrm{tr}(g, M_2) = \mathrm{tr}(g, M_1) + \mathrm{tr}(g, M_3)$, and if M and M' have the same composition factors then for all $g \in G, \mathrm{tr}(g, M) = \mathrm{tr}(g, M')$. Without loss of generality, suppose that M and M' are semisimple. Since $\mathrm{tr}(g, pS) = 0, (ii)$ implies (i). Conversely, if $\mathrm{tr}(g, M) = \mathrm{tr}(g, M')$ for all $g \in G$, we have $\mathrm{tr}(x, M) = \mathrm{tr}(x, M')$ for all $x \in FG$. Using the Wedderburn structure Theorem, there are elements $x_i \in FG$ such that

$$\mathrm{tr}(x_i, S_j) = \begin{cases} 1 & i = j, \\ 0 & i \neq j. \end{cases}$$

Thus $\mathrm{tr}(x_i, M)$ equals the number of copies of S_i as a composition factor of M modulo p. □

3.7 p and p' elements

Definition 3.7.1. We set F to be a field of characteristic p, p a prime. A **p-element** of a finite group G is an element whose order is a p power, that is, the order is p^a for some $a \in \mathbb{N}$. A **p′-element** is an element whose order is relatively prime to p.

Lemma 3.7.1. *Let G be a finite group. Given $g \in G, g$ can be written as $g = xy$ such that*

(i) x is a p-element.

(ii) y is a p'-element.

(iii) Every element of G that commutes with g commutes with x and y.

The elements x and y are known as the p-part (p-regular part) and the p'-part (p'-regular part) of g respectively.

Proof. Let the order of g be $n = p^a m$, with $p \nmid m$. Since $\gcd(p^a, m) = 1$, there exist $s, t \in \mathbb{Z}$ such that $sp^a + tm = 1$. Then $g = g^{tm} g^{sp^a}$. Take x to be g^{tm} and y to be g^{sp^a}. Because x, y are powers of g, they commute with any element that commutes with g. □

In the literature p-elements are sometimes called p-singular elements while p'-elements are called p-regular elements. Suppose F and G are as in Definition 3.7.1. Suppose further that F has all the $|G|_{p'} = |G_{p'}|$-th roots of unity where $G_{p'}$ is the set of all p' elements. These form a cyclic group of order $|G|_{p'}$ under multiplication. All eigenvalues of elements of G belong to this cyclic group. Choose an isomorphism of cyclic groups, namely ψ from the set $\{|G|_{p'}$-th roots of unity in $F^\times\}$ to the set
$\{|G|_{p'}$-th roots of unity in $\mathbb{C}\}$. If g is a p'-element (i.e., an p-regular element) of G and M a finite dimensional FG-module, then $g \sim \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_d \end{pmatrix}$,
and $d = \dim_F M$. Define

$$\varphi_M(g) := \sum_{i=1}^{d} \psi(\lambda_i).$$

Here we note that $\varphi_M(g)$ is a cyclotomic integer which gives a map

$$\varphi_M : \{\text{conjugacy classes of } p'\text{-elements of } G\} \to \mathbb{C}.$$

(Recall from elementary number theory a cyclotomic integer is an integral linear combination of powers of a primitive nth root of unity, that is, if ζ is a primitive nth root of unity, a cyclotomic integer is of the form $a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1}, a_i \in \mathbb{Z}$.)

Theorem 3.7.2. *For finite-dimensional modules M and M' the following are equivalent:*

(1) $\varphi_M = \varphi_{M'}$

(2) The multiplicities of each simple FG-module as composition factors of M and M' are equal.

Proof. Without loss of generality, assume that M and M' are semisimple. The conditional statement (2) $\Rightarrow$ (1) is self-evident. For the converse, a counter example of smallest dimension is looked at. If M and M' have a composition factor in common this can be removed to get a smaller example. Therefore, assume that they do not. If $\varphi_M = \varphi_{M'}$, by reducing back to F we obtain $\mathrm{tr}(g, M) = \mathrm{tr}(g, M')$ for all $g \in G$ so that the multiplicities are congruent modulo p. Thus, all multiplicities are divisible by p. Therefore $M = pM_1$ and $M' = pM_1'$. Further, $\varphi_M = p\varphi_{M_1}$ and $\varphi_{M'} = p\varphi_{M_1}$. Hence M_1 and M_1' give a smallest counter example. □

3.8 Choice of ψ and Brauer character table.

Let G be a finite group with order $|G| = p^a m, p \nmid m$ and let F be a field of characteristic p, p a prime. Suppose that F has all the mth roots of unity. Let $C, \hat{C}$ be the groups of mth roots of unity in F and $\mathbb{C}$ respectively. Let $K := \mathbb{Q}[\hat{C}]$, the field formed by adjoining the complex mth roots of unity to the field of rationals. Then from the theory of field extensions and Galois theory,

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Aut}(\hat{C}) \cong \mathbb{Z}/\varphi(m)$$

where φ is the Euler totient function. Let $\mathcal{O}_K$ be the ring of integers in K. Then $\mathbb{Z}[\hat{C}] = \mathcal{O}_K$. We note that $\mathcal{O}_K$ is a Dedekind domain and in particular, every prime ideal in $\mathcal{O}_K$ is maximal. Choose a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lying over p, that is $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Then the following holds:

Proposition 3.8.1. *The field $\mathcal{O}_K/\mathfrak{p}$ is the smallest field containing mth roots of unity: if p^r is the smallest power of p such that $m \mid p^r - 1$, then*

$$\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^r} \hookrightarrow F,$$

$$\hat{C} + \mathfrak{p} \cong C$$

and Gal$(\mathbb{F}_{p^r}/\mathbb{F}_p) \cong$ Stabilizer of $\mathfrak{p}$ in Gal$(K/\mathbb{Q}) \cong \mathbb{Z}/r\mathbb{Z}$.

Proof. We note that since $\gcd(m,p)=1$, we have $m \mid p^{\varphi(m)}-1$ by Euler's Theorem. Let ζ be a primitive mth root of unity in $\mathbb{C}$. Then $\mathcal{O}_K/\mathfrak{p}$ is the field extension of $\mathbb{F}_p$ generated by the image of $\zeta+\mathfrak{p}$. Since

$$\frac{X^m-1}{X-1} = X^{m-1}+X^{m-2}+\cdots+1 = \prod_{j=1}^{m-1}(X-\zeta^j),$$

setting $X=1$ gives $1-\zeta^j \mid m$ in $\mathcal{O}_K$ for all $j=1,\ldots,m-1$. If $1-\zeta^j \in \mathfrak{p}$, then $m \in \mathfrak{p}\cap\mathbb{Z} = p\mathbb{Z}$, contradicting $\gcd(m,p)=1$. Thus $\zeta+\mathfrak{p}$ is a primitive *mth*-root of unity so $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^r}$ and $\hat{C}+\mathfrak{p} \cong C$. □

Definition 3.8.1. *(Brauer character table)* The **Brauer character table** of a finite group G (modulo p) is a table with rows indexed by simple FG-modules S and columns indexed by conjugacy classes of p' elements of G and whose entries are the values of Brauer characters $\varphi_S(g)$.

Note that once the isomorphism $\psi : C \to \hat{C}$ has been established, all other isomorphisms $C \to \hat{C}$ are obtained by applying elements of $\mathrm{Gal}(K/\mathbb{C})$. Rows of the Brauer table of G are the irreducible Brauer characters φ_S where S is a simple FG-module. The columns of the Brauer character table of G are the ring homomorphisms $\chi_-(g) : \mathcal{R}(G) \to \mathbb{C}$, where g is a p-regular element of G.

Proposition 3.8.2. *(1) If an element of Gal$(K/\mathbb{Q})$ is applied to a column of the Brauer character table, then another column is obtained.*

(2) If an element of the stabilizer of $\mathfrak{p}$ in Gal$(K/\mathbb{Q})$ is applied to a row of the Brauer character table, then another row is obtained.

Proof. (1) Let ζ be a primitive mth root of unity in $\mathbb{C}$. Then $K=\mathbb{Q}(\zeta)$ and an element σ of $\mathrm{Gal}(K/\mathbb{Q})$ sends ζ to ζ^t for some t such that $\gcd(m,t)=1$. Then for each p-regular element g of G, $\chi_-^\sigma(g) = \chi_-(g^t)$.

(2) The element σ of $\mathrm{Gal}(K/\mathbb{Q})$ stabilizes $\mathfrak{p}$ when t is a power of p. Let S be a simple FG-module with corresponding representation $\rho : G \to \mathrm{GL}_n(F)$. Then S^σ is an FG-module with the corresponding representation

$$\rho^\sigma : G \xrightarrow{\rho} \mathrm{GL}_n(F)$$

$$g \mapsto (\lambda_{ij}(g)) \mapsto (\lambda_{ij}(g)^t).$$

□

Thus the Brauer character table is determined by the choice of $\mathfrak{p}$ up to permutations of rows and columns.

Remark 3.8.3. If an element of $\mathrm{Gal}(K/\mathbb{Q})$ which does not stabilize $\mathfrak{p}$ is applied to a row of the Brauer character table, another row is not necessarily obtained.

Example 3.8.4. Let $p = 2$ and $m = 7$. Then the seventh roots of unity in F have two possible minimal polynomials, $X^3 + X^2 + 1$ or $X^3 + X + 1$. Let ζ be a seventh root of unity in $\mathbb{C}$. Then there are two prime ideals in $\mathbb{Z}[\zeta]$, namely $\mathfrak{p}_1 = [2, \zeta^3 + \zeta^2 + 1]$ and $\mathfrak{p}_2 = [2, \zeta^3 + \zeta + 1]$ lying over 2 (that is, $\mathfrak{p}_i \cap \mathbb{Z} = \mathfrak{p}_i\mathbb{Z}, i = 1, 2$) such that $\mathbb{Z}[\zeta]/\mathfrak{p}_1 \cong \mathbb{F}_8 \cong \mathbb{Z}[\zeta] \cong \mathbb{Z}[\zeta]/\mathfrak{p}_2$.

3.9 Condition for the existence of self-dual codes.

We end this chapter by giving a result which gives a necessary and sufficient condition for the existence of self-dual binary codes due to A. Günther and G. Nebe [22].

Theorem 3.9.1. *Let $G \leq S_n$. Then there exits a self dual code $\mathcal{C} \subseteq \mathbb{F}_2^n$ with $G \leq \mathrm{Aut}(\mathcal{C})$ if and only if every simple self-dual $\mathbb{F}_2G$-module S occurs with even multiplicity in the $\mathbb{F}_2G$-module $\mathbb{F}_2^n$.*

As in the original paper, we present the proof as a series of lemmas.

Lemma 3.9.2. *Let V be a simple self-dual $\mathbb{F}_2G$-module and assume that V carries a non-degenerate symmetric G-invariant bilinear form $\varphi : V \times V \to \mathbb{F}_2$. Then φ is unique up to isometry (an isometry is a distance preserving linear map).*

Proof. Consider the map $\alpha_\varphi : V \to V^*$ given by $v \mapsto (v' \mapsto \varphi(v, v'))$. By the non-degeneracy of the bilinear form, we have that $\varphi(v, v') = 0$ for all v' if and only if $v = 0$. Thus $\ker(\alpha_\varphi) = 0$ and the map is injective. The map is clearly homomorphic and surjective so is an isomorphism. Let $\psi : V \times V \to \mathbb{F}_2$ be another non-degenerate symmetric bilinear form on V. Then $\alpha_\psi = \alpha_\varphi \circ \vartheta$ for some ϑ in the field

$$\mathfrak{C} := \mathrm{End}_G(V)$$

of all $\mathbb{F}_2G$-endomorphisms of V. Thus

$$\psi(v,v') = \alpha_\psi(v)(v') = \alpha_\varphi(\vartheta(v))(v') = \varphi(\vartheta(v),v')$$

for all $v, v' \in V$. Consider the involution τ on $\mathfrak{C}$ given by

$$\varphi(v,\alpha(v')) = \varphi(\alpha^\tau(v),v')$$

for v, v' in V. Since both φ and ψ are symmetric,

$$\begin{aligned}\varphi(\vartheta(v),v') = \psi(v,v') &= \psi(v',v)\\ &= \varphi(\vartheta(v'),v)\\ &= \varphi(v,\vartheta(v'))\\ &= \varphi(\vartheta^\tau(v),v')\end{aligned}$$

for all $v, v' \in V$ therefore $\vartheta \in \mathfrak{F} = \{\alpha \in \mathfrak{C} | \alpha^\tau = \alpha\}$. We have that the involution τ is either the identity on $\mathfrak{C}$ or a field automorphism of order 2. In the first instance $\mathfrak{F} = \mathfrak{C} = \{\alpha\alpha^\tau = \alpha^2 | \alpha \in \mathfrak{C}\}$ as squaring is a field automorphism of the finite field $\mathfrak{C}$. In the second case the map $\mathfrak{C} \to \mathfrak{F}, \alpha \mapsto \alpha\alpha^\tau$ is the norm map onto the field $\mathfrak{F}$. In either case there exists $\gamma \in \mathfrak{C}$ with $\gamma\gamma^\tau = \vartheta$. It follows that γ induces an isometry between the spaces (V,φ) and (V,ψ) since $\psi(v,v') = \varphi(\vartheta(v),v') = \varphi(\gamma^\tau(\gamma(v)),v') = \varphi(\gamma(v),\gamma(v'))$ for all $v, v' \in V$. □

Lemma 3.9.3. *Let $G \leq S_n$ and $N \subseteq M \subseteq \mathbb{F}_2^n$ be G-submodules (G-invariant codes). Then $(M/N)^* \cong N^\perp/M^\perp$.*

Proof. Let $M_N^* := \{f \in \mathrm{Hom}_{\mathbb{F}_2}(M,\mathbb{F}_2) | f(n) = 0 \ \forall n \in N\} \subseteq M^*$. Then M_N^* is canonically isomorphic to
$(M/N)^*$. Let

$$\beta : N^\perp \to M_N^*, n' \mapsto (m \mapsto b(m,n')).$$

Then β is well defined and surjective since $\Upsilon : \mathbb{F}_2^n \to F^\times, v \mapsto (m \mapsto b(m,v))$ is surjective and $\Upsilon(v) \in M_N^*$ if and only if $v \in N^\perp$. The kernel of β is $M^\perp$ and hence by The First Isomorphism Theorem of modules

$$\begin{aligned}\mathrm{Im}(\beta) &= M_N^*, \text{ (by surjectivity)}\\ &\cong N^\perp/\ker(\beta) = N^\perp/M^\perp\\ &\cong (M/N)^*.\end{aligned}$$

□

Corollary 3.9.4. *Let $G \leq S_n$. If there exists a self-dual code $\mathcal{C} \subseteq \mathbb{F}_2^n$ with $G \leq \mathrm{Aut}(\mathcal{C})$ then every self-dual simple G-module occurs with even multiplicity in a composition series of the $\mathbb{F}_2 G$-module $\mathbb{F}_2^n$.*

Proof. Let $\mathcal{C} = N_k \supseteq N_{k-1} \supseteq \ldots \supseteq N_1 \supseteq N_0 = \{0\}$ be a composition series of the $\mathbb{F}_2 G$-module $\mathcal{C}$. Then

$$\mathcal{C} = \mathcal{C}^\perp = N_k^\perp \subseteq N_{k-1}^\perp \subseteq \ldots N_1^\perp \subseteq N_0^\perp = \mathbb{F}_2^n$$

is a composition series of $\mathbb{F}_2^n/\mathcal{C}^\perp$ as dualizing gives an automorphism $W \mapsto W^\perp$ of the submodule lattice of $\mathbb{F}_2^n$. The composition factors satisfy

$$N_{i-1}^\perp/N_i^\perp \cong (N_i/N_{i-1})^*$$

by Lemma 3.9.3. The result follows. □

Lemma 3.9.5. *Let V be a simple self-dual $\mathbb{F}_2$-module endowed with a non-degenerate G-invariant symmetric bilinear form φ. The module $(U, \psi) := \perp_{i=1}^k (V, \varphi)$ contains a submodule X with*

$$X = X^{\perp,\psi} := \{u \in U |\ \psi(u, x) = 0 \text{ for all } x \in X\}$$

if and only if k is even.

Proof. If U contains such a module $X = X^{\perp,\psi}$ then k is even by Corollary 3.9.4. Conversely, if k is even, then $X = \{(v_1, v_1, v_2, v_2, \ldots, v_{k/2}, v_{k/2})\} \subseteq V$ satisfies $X = X^{\perp,\psi}$. □

We are now in a position to prove Theorem 3.9.1.

Proof of Theorem 3.9.1. If $\mathcal{C} \subseteq \mathbb{F}_2^n := V$ is a self-dual G-invariant code then every self-dual simple module occurs with even multiplicity in a composition of V by Corollary 3.9.4. Conversely, assume that every self-dual composition factor occurs in V with even multiplicity and $M \subseteq M^\perp \subseteq V$ is a maximally self-orthogonal code (there is no G-invariant self-dual code properly containing M). Then there exists a G-invariant non-degenerate symmetric bilinear form on the G-module $M^\perp/M$, that is,

$$\varphi : M^\perp/M \times M^\perp/M \to \mathbb{F}_2$$

such that

$$(m' + M, m'' + M) \mapsto (m', m'').$$

Now, any proper $\mathbb{F}_2G$-submodule X of $(M^\perp/M, \varphi)$ with $X \subseteq X^{\perp,\varphi}$ would lift to a self-orthogonal G-invariant code in V properly containing M, which is impossible. This implies that every $\mathbb{F}_2G$-submodule $X \subseteq M^\perp/M$ has a G-invariant complement $X^{\perp,\varphi}$, that is $M^\perp/M$ is isomorphic to a direct sum of simple self-dual modules, $(M^\perp/M, \varphi) \cong \perp_{V \cong V^*} (V, \varphi_V)^{n_V}$, where φ_V is a non-degenerate G-invariant bilinear form on V which is unique up to isometry, by Lemma 3.9.2. By hypothesis, every simple self-dual G-module occurs with even multiplicity in $M^\perp/M$, that is all the n_V are even. But by Lemma 3.9.5 this means that the n_V must all be zero, that is, $M = M^\perp$ is a self-dual code in V. □

Testing this condition in practice is not easy. A more computationally convenient way of carrying out the test is to use character theory. From standard character theory texts, we have that if F is the complex number field, V an FG-module and V^* is its dual, then

$$\chi_V = \overline{\chi_{V^*}}.$$

If a G-module V is self-dual then we have

$$\begin{aligned} \chi_V &= \overline{\chi_{V^*}} \\ &= \overline{\chi_V}. \end{aligned}$$

This is equivalent to saying that the character χ_V is real.

Using GAP or MAGMA, we get the Brauer (2-modular) character of the $\mathbb{F}_2G$-module $\mathbb{F}_2^n$ and decompose it into the sum of irreducible Brauer characters, which is equivalent to decomposing the module $\mathbb{F}_2^n$ into irreducible or simple modules. To see which irreducible characters correspond to self-dual modules, we look at the real character constituents. We then check the parity of their multiplicities. Subsequently we use Theorem 3.9.1 to check if a self-dual G-invariant code exists. This serves as a good preliminary check for existence in the binary case.

Chapter 4

A construction of self-orthogonal codes from permutation groups

In this chapter we present a method of constructing codes spanned by the fixed points of involutions of some permutation groups due to Chigira et al [35]. This is of interest to us because every self-dual code is necessarily self-orthogonal. Further, some necessary conditions for the existence of self-dual codes are embedded within the construction. Given a permutation group G and a set Ω of n points, we construct the code $C(G, \Omega)$, which is the dual of the code spanned by the sets of fixed points of involutions of the group G. We first lay down some notation.

4.1 Notation

Definition 4.1.1. Let G be a group. A non-trivial element $g \in G$ is called an **involution** if $g^2 = 1_G$ where 1_G is the identity of the group.

Definition 4.1.2. A group G is almost simple if $G_0 \lhd G \subseteq \mathrm{Aut}(G_0)$ for some non-abelian simple group G_0.

We denote the set of all involutions of G by $I(G)$. Since we are dealing with permutation groups, we can form the sets of fixed points of involution as follows:

$$\mathrm{Fix}(\sigma) = \{i \in \Omega | i^\sigma = i\}$$

where Ω is an n-point set, n the degree of the permutation group G and σ some element of G. By i^σ we mean $\sigma(i)$. We will take Ω to be the set $\{1, 2, \ldots, n\}$. By $\mathbb{P}(\Omega)$ we refer to the power set of Ω, the collection of all subsets of Ω. We will show below that $\mathbb{P}(\Omega)$ can be regarded as a vector space over F_2, the binary field, by defining addition as the symmetric set difference. With this notation in place, we define the code $C(G, \Omega)$.

Definition 4.1.3. The binary code $C(G, \Omega)$ is defined as :

$$C(G, \Omega) := \langle \mathrm{Fix}(\sigma) | \sigma \in I(G) \rangle^\perp,$$

where $\langle \mathrm{Fix}(\sigma) | \sigma \in I(G) \rangle$ is the span of the sets $\mathrm{Fix}(\sigma)$, of fixed points of involutions σ, of the group G.

Chigira et al [35, Theorem A] proved that if $\mathcal{C}$ is any self-orthogonal code of length n, then $\mathcal{C} \subseteq C(G, \Omega)$. They further proved that if $\mathcal{C}$ is a self-dual code of length n, invariant under G, then

$$C(G, \Omega)^\perp \subseteq \mathcal{C} \subseteq C(G, \Omega).$$

For our work to be self contained, we present the details of the proof. We note that the last result gives us a starting point in the search for self-dual codes of a certain length which are invariant under permutation groups.

4.2 The results

With the notation of the last section, we note that we have $C(G, \Omega) \in \mathbb{P}(\Omega)$. The following holds.

Lemma 4.2.1. *The collection $\mathbb{P}(\Omega)$ can be regarded as an n-dimensional vector space over $\mathbb{F}_2$, the field of two elements with addition in $\mathbb{P}(\Omega)$ taken to be the symmetric set difference. Additionally, the vector space can be endowed with an inner product $<,>$ defined by*

$$< X, Y >:= |X \cap Y| \mod 2.$$

Proof. By definition, the symmetric set difference of X and Y is given as :

$$X \triangle Y := \{a \in X \cup Y | a \notin X \cap Y\}.$$

Clearly, if $A, B \in \mathbb{P}(\Omega)$, then $A \triangle B \in \mathbb{P}(\Omega)$. Further, by definition of the symmetric set difference, $A \triangle B = B \triangle A$. For any $X \in \mathbb{P}(\Omega)$ we have $X \triangle \varnothing = X$. Therefore $\varnothing$ is the additive identity. We also have $X \triangle X = \varnothing$ for all $X \in \mathbb{P}(\Omega)$ so each X is self-inverting. Thus, $(\mathbb{P}(\Omega), \triangle)$ is an additive group. Defining scalar multiplication by $1.X = X$ and $0.X = \varnothing$, distributivity follows trivially. Closure of $\mathbb{P}(\Omega)$ under the scalar multiplication is also trivial so $\mathbb{P}(\Omega)$ is a vector space. To prove that the dimension of $\mathbb{P}(\Omega)$ is n, we set $X_i = \{i\}, i \in \Omega$. Then the X_i are disjoint for different $i \in \Omega$. Let $\mathcal{B} = \{X_i\}_{i \in \Omega}$. We claim that $\mathcal{B}$ spans $\mathbb{P}(\Omega)$. Let $X \in \mathbb{P}(\Omega)$. Then

$$\begin{aligned} X &= \triangle_{i=1}^{n} X_i \\ &= \alpha_1 X_1 \triangle \alpha_2 X_2 \cdots \triangle \alpha_n X_n, \end{aligned}$$

where

$$\alpha_i = \begin{cases} 1 & i \in X \\ 0 & \text{otherwise.} \end{cases}$$

Thus our claim is proved. If $\varnothing = \triangle_{i=1}^{n} \alpha_i X_i$, then by definition of α_i and disjointness of the X_i, we have that all the $\alpha_i = 0$ which shows that $\mathcal{B}$ is a linearly independent set and so is a basis for $\mathbb{P}(\Omega)$. Given $X, Y \in \mathbb{P}(\Omega)$ by definition,

$$\begin{aligned} < X, Y > &= |X \cap Y| \\ &= |Y \cap X| \\ &= < Y, X > \end{aligned}$$

so $<,>$ is symmetric. It is not difficult to check that
$< \alpha X, Y >= \alpha < X, Y >$ since there are only two scalars. We check linearity.

To this end, let $X, Y, Z \in \mathbb{P}(\Omega)$. Then working mod 2,

$$\begin{aligned}
< X \vartriangle Y, Z > &= |[(X \setminus Y) \cup (Y \setminus X)] \cap Z| \\
&= |((X \setminus Y) \cap Z) \cup ((Y \setminus X) \cap Z)| \\
&= |(X \setminus Y) \cap Z| + |(Y \setminus X) \cap Z| \\
&- |[(X \setminus Y) \cap Z] \cap [(Y \setminus X) \cap Z]| \\
&= |(X \setminus Y) \cap Z| + |(Y \setminus X) \cap Z| \\
&- |X \cap Y^{\mathrm{c}} \cap Z \cap Y \cap X^{\mathrm{c}} \cap Z| \\
&= |(X \setminus Y) \cap Z| + |(Y \setminus X) \cap Z| \\
&\quad -|\varnothing| \\
&= |(X \setminus Y) \cap Z| + |(Y \setminus X) \cap Z| - 0 \\
&= |[(X \setminus Y) \cup (X \cap Y)] \cap Z| \\
&\quad +|[(Y \setminus X) \cup (Y \cap X)] \cap Z| \\
&= |X \cap Z| + |Y \cap Z|,
\end{aligned}$$

using set-theoretic definitions and in the penultimate line adding $2|X \cap Y| \equiv 0$ mod 2. It follows that $<,>$ is linear and hence an inner product. □

Using this inner product, the weight of X is the integer $|X|$. We now discuss the specifics of the construction. If H is the stabilizer of a point and satisfies $N_G(I(H)) = H$, where as usual $I(H)$ denotes the set of involutions of H, then the codes $C(G, G/H)$ are formed. The condition that $N_G(I(H)) = H$ given above is equivalent to saying that the minimum weight of $C(G, \Omega)$ is greater than 2. The scheme is as follows:

1. Define a group G and a subgroup H, such that $N_G(I(H)) = H$.
2. Determine a permutation representation of G on G/H by calculating the coset table.
3. Calculate the sets of fixed points of involutions of G.
4. Form the code $C(G, G/H)$. We note that here $\Omega = G/H$.

We then use the in-built functions of MAGMA to determine code invariants like the dimensions, weights, minimum distances and so on. For ease of manipulation for every $X \in \mathbb{P}(\Omega)$ we form vectors v_X with all the entries

zero except at the i-th coordinate place if $i \in X$. In fact, the map $\theta : \mathbb{P}(\Omega) \to \mathbb{F}_2^n, X \mapsto v_X = (v_1, \ldots, v_n)$ where

$$v_i = \begin{cases} 1 & \text{if } i \in X \\ 0 & \text{otherwise} \end{cases}$$

is an isomorphism of vector spaces. For example, if $n = 4$, we have $\Omega = \{1, 2, 3, 4\}$. If we let $X = \{2, 3\}$, then $v_X = (0, 1, 1, 0)$. In the subsequent discussions we identify $X \in \mathbb{P}(\Omega)$ with v_X. From the previous chapter, we saw that any G-invariant code can be regarded as a G-submodule over $\mathbb{F}_2$. In general finding G-submodules is not any easy task but GAP and MAGMA calculate these for degrees n which are not too large. Further, MAGMA has a classification of G-submodules which can be used to classify G-invariant self-dual codes. We now give the details of the proofs of the results stated at the start of this chapter. We note that since the action of G on $\Omega = G/H$ is transitive and a permutation representation of degree n is uniquely determined up to equivalence, we write $C(G, \Omega)$ as $C(G, n)$.

Theorem 4.2.2. *Let $\mathcal{C}$ be a G-invariant binary self-orthogonal code of length n. Then $\mathcal{C} \subseteq C(G, \Omega)$.*

Proof. Take a non-zero codeword $X \in \mathcal{C}$, (that is let $\varnothing \neq X$). Further, let $\sigma \in I(G)$. Then the subgroup $\langle \sigma \rangle$ of G acts on $X \cap X^\sigma$. Since $\mathcal{C}$ is self-orthogonal, the weight of $X \cap X^\sigma$, $|X \cap X^\sigma|$ is even. Set $Y = (X \cap X^\sigma) \setminus (\mathrm{Fix}(\sigma) \cap X)$. By definition of Y, $y \in Y$ implies that $y = x^\sigma$ for some $x \in X$ and $x \neq y$. Thus x, x^σ are different elements. Thus Y is a disjoint union of the sets $\{a, a^\sigma\}$ for $a \in Y$ since σ is well-defined, that is, if $a \neq b$, then $a^\sigma \neq b^\sigma$. It follows that

$$\begin{aligned} |Y| &= N|\{a, a^\sigma\}| \\ &= N.2 \end{aligned}$$

for some N. It follows that $|Y|$ is even and therefore

$$|\mathrm{Fix}(\sigma) \cap X| = |X \cap X^\sigma| - |Y|$$

is even being the difference of two even numbers and by the fact that $X \cap X^\sigma = Y \cup (\mathrm{Fix}(\sigma) \cap X)$ is a disjoint union. Thus $< X, \mathrm{Fix}(\sigma) >= |X \cap \mathrm{Fix}(\sigma)| \equiv 0 \mod 2$ and hence $X \in \langle \mathrm{Fix}(\sigma) | \sigma \in I(G) \rangle^\perp$ so the result follows. □

The theorem above allows the characterisation of self-orthogonal or self-dual codes with a fixed automorphism group.

Lemma 4.2.3. *Let K act on Ω and G be a normal subgroup of K. Then $C(G,\Omega)$ is K-invariant.*

Proof. Let $x \in K$ and $\sigma \in I(G)$. For $i \in \mathrm{Fix}(\sigma)$, we have

$$\begin{aligned}(x\sigma x^{-1})(x(i)) &= x\sigma(x^{-1}x(i)) \\ &= x\sigma(i) \\ &= x(i)\ (i^\sigma = i \text{ for } i \in \mathrm{Fix}(\sigma)).\end{aligned}$$

Therefore, $\mathrm{Fix}(x\sigma x^{-1}) = x(\mathrm{Fix}(\sigma))$. We note that
$x\sigma x^{-1}(x(i)) = x(i)$ shows that $x(i) \in \mathrm{Fix}(x\sigma x^{-1})$. But $x(i) \in x(\mathrm{Fix}(i))$ so $x(\mathrm{Fix}(\sigma)) \subseteq \mathrm{Fix}(x\sigma x^{-1})$. Conversely, if $y \in \mathrm{Fix}(x\sigma x^{-1})$, then $y = (x\sigma x^{-1})(y)$ and

$$\begin{aligned}x^{-1}(y) &= x^{-1}(x\sigma x^{-1})(y) \\ &= (x^{-1}x\sigma x^{-1})(y) = \sigma x^{-1}(y) = \sigma(x^{-1}(y)).\end{aligned}$$

It follows that $x^{-1}(y) \in \mathrm{Fix}(\sigma)$. Therefore,

$$\begin{aligned}y &= x(x^{-1}(y)) \\ &= x(\sigma(x^{-1}(y)))\end{aligned}$$

and $y \in x\mathrm{Fix}(\sigma)$ which gives the reverse inclusion and so equality follows. □

Lemma 4.2.4. *Let K act on Ω and G be a normal subgroup of K. If $C(G,\Omega)$ is self-orthogonal, then $C(G,\Omega) = C(K,\Omega)$.*

Proof. Since $I(K) \supseteq I(G)$ we have

$$\mathrm{Fix}(I(K)) \supseteq \mathrm{Fix}(I(G)).$$

Taking duals and using definition, we have

$$C(K,\Omega) \subseteq C(G,\Omega). \tag{i}$$

On the other hand, by Lemma 4.2.3, $C(G,\Omega)$ is K-invariant. By hypothesis, $C(G,\Omega)$ is self-orthogonal and by Theorem 4.2.2,

$$C(K,\Omega) \supseteq C(G,\Omega). \tag{ii}$$

By (i) and (ii), equality follows and the result is established. □

Lemma 4.2.5. *Suppose $G = \mathrm{Aut}(C(G,\Omega))$. If $\mathcal{C}_1, \mathcal{C}_2$ are distinct subcodes of $C(G,\Omega)$ satisfying the condition $G = \mathrm{Aut}(\mathcal{C}_1) = \mathrm{Aut}(\mathcal{C}_2)$, then they are inequivalent.*

Proof. Suppose for a contradiction that there exists $\pi \in S_\Omega$ such that $\mathcal{C}_1^\pi = \mathcal{C}_2$. Then $\pi G \pi^{-1} = \mathrm{Aut}(\mathcal{C}_1^\pi) = \mathrm{Aut}(\mathcal{C}_2) = G$. Thus, π preserves $\langle \mathrm{Fix}(\sigma) | \sigma \in I(G) \rangle$, so $\pi \in \mathrm{Aut}(C(G,\Omega))(= \mathrm{Aut}(\mathcal{C}_1))$. It follows that $\mathcal{C}_1 = \mathcal{C}_1^\pi = \mathcal{C}_2$ contradicting the fact that $\mathcal{C}_1, \mathcal{C}_2$ are distinct. □

Lemma 4.2.6. *Let $\mathcal{D}$ be a self-orthogonal t-(n,k,λ) design with k even. Suppose that $\mathcal{D}$ is invariant under a permutation group G on the set Ω. Then the code generated by the rows of the block incidence matrix of $\mathcal{D}$ is contained in $C(G,\Omega)$.*

Proof. Because k is even and the design is self-orthogonal, the code formed in the hypothesis of the lemma is G-invariant and self-orthogonal and so the result follows by Theorem 4.2.2. □

4.2.1 An example

Many known self-orthogonal codes have sporadic almost simple groups as automorphism groups. The following shows how one such relates to $C(G,\Omega)$.

Example 4.2.7. Let $G = M_{24}$ and $n = 24$. The set of fixed points of $2A$-involutions forms the Witt system W_{24}, the 5-$(24,8,1)$ design or $(5,8,24)$ Steiner system. The $2B$-involutions are fixed point free. Since the extended Golay code $\mathcal{G}_{24}$ is generated by W_{24}, we have $C(G,24)^\perp = \mathcal{G}_{24}$. The code $\mathcal{G}_{24}$ is also obtained as $C(M_{12}{:}2, 24)$. The details of the calculation are below.
Using the table of Marks in GAP we construct the Mathieu group M_{24} as follows:

```
gap> tom:=TableOfMarks("M24");
TableOfMarks( "M24" )
gap> m24:=UnderlyingGroup(tom);
 Group([ (1,2)(3,4)(5,24)(6,12)(7,9)(8,10)
 (11,17)(13,14)(15,16)(18,23)(19,21)(20,22),
 (1,8,17)(2,18,7)(3,13,14)(4,20,19)
      (5,6,15)(21,24,23) ])
```

We then transfer to MAGMA. We do :

```
 > M24:=PermutationGroup<24|[ (1,2)(3,4)
 (5,24)(6,12)(7,9)(8,10)(11,17)(13,14)
 (15,16)(18,23)(19,21)(20,22),(1,8,17)
 (2,18,7)(3,13,14)(4,20,19)(5,6,15)(21,24,23) ]>;
```

We then calculate the conjugacy classes of M_{24}:

```
>X:=ConjugacyClasses(M24);
```

A typical entry in X is

```
 > X[2];
<2,11385,(2, 18)(3, 16)(4, 24)(8, 10)(9, 20)
(11, 23)(12, 15)(13, 17)>
```

which gives the order, size and representative of each conjugacy class respectively. We find the conjugacy classes which contain involutions;

```
> l:=[];
>  for i in [1..#X] do
for>   if X[i,1] eq 2 then
for|if>  l:=Append(l,i);
for|if> end if;
for> end for;
> l;
[ 2, 3 ]
```

which shows that M_{24} has two conjugacy classes, namely class 2 and class 3, which contain involutions. The sets of involutions for each conjugacy class are calculated:

```
>M24c2A:=Conjugates(M24,X[2,3]);
>M24c2B:=Conjugates(M24,X[3,3]);
```

We now calculate the sets of fixed points of involution for each conjugacy class:

```
>FixedPoints2AInvs:=[];
>for i in M24c2A do
for>set:={j:j in [1..24]|j^i eq j};
for|if>if #set ne 0 then
for|if>FixedPoints2AInvs:=Append(FixedPoints2AInvs, set);
for|if>end if;
for>end for;
> #FixedPoints2AInvs;
11385

FixedPoints2BInvs:=[];
for i in M24c2B do
for>set:={j:j in [1..24]|j^i eq j};
for|if> #set ne 0 then
for|if>FixedPoints2AInvs:=
Append(FixedPoints2AInvs,set);
for|if>end if;
for>end for;
>FixedPoints2BInvs;
[]
```

showing that the first set is non-empty and that the $2B$-involutions act fixed-point freely on a set of 24 points. We wish to change all the sets of involutions into vectors, using the isomorphism of the earlier section.

The following lines of code gives what we want:

```
>FixedPointsVecs:=[];
>for i in FixedPoints2AInvs do
for>t:=[];
for>for j in [1..24] do
for|for|if>if j in i then t[j]:=1;
for|for|if>else
for|for|if>t[j]:=0;
for|for|if>end if;
for|for>end for;
for>end for;
```

```
>FixedPointsVecs:=Append(FixedPointsVecs,t);
end for;
```

As an example, choose i to be the set of fixed points of the first involution in the $2A$ class, that is

```
>i:=FixedPoints2AInvs[1];
 > i;
{ 6, 9, 10, 14, 16, 19, 22, 23 }.
```

We then run the loop

```
> t:=[];
> for j in [1..24] do
for> if j in i then t[j]:=1;
for|if> else
for|if> t[j]:=0;
for|if> end if;
for> end for;
> t;
[ 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1,
0, 1, 0, 0, 1, 0, 0, 1, 1, 0 ]
```

which correctly gives a list with 1's in the 6th, 9th, 10th, 14th, 16th, 19th, 22nd and 23rd positions. The next task is to form a vector space spanned by these vectors. We do the following:

```
>V:=sub<VectorSpace(GF(2),24)|
[VectorSpace(GF(2),24)!i:i in FixedPointsVecs]>; .
```

We finally put this in linear code form so that we can use MAGMA intrinsic functions:

```
> code:=LinearCode(V);
> code;
[24, 12, 8] Linear Code over GF(2)
Generator matrix:
[1 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 1 0 1 0 1 1 1 0]
```

```
[0 1 0 0 0 0 0 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 1]
[0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1 1 1 1 1 0 1 0 0]
[0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 1 1 1 0 1 1]
[0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 1 1 1 1 0 1 0 1 0]
[0 0 0 0 0 1 0 0 0 0 0 0 0 1 1 0 1 1 1 0 0 1 0 1]
[0 0 0 0 0 0 1 0 0 1 0 0 0 1 0 1 1 0 0 0 1 1 0 1]
[0 0 0 0 0 0 0 1 0 1 0 0 0 1 1 0 0 1 1 1 0 0 1 0]
[0 0 0 0 0 0 0 0 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1]
[0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 1 0 1 0 1 0 1 1 1]
[0 0 0 0 0 0 0 0 0 0 0 1 0 1 1 0 1 0 0 1 1 0 1 1]
[0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 0 0 1 1 1 1 0 0].
```

We test the self-duality of $C(M_{24}, 24) :=$ code.

```
> dual:=Dual(code);
> dual eq code;
true.
```

Thus the code $C(M_{24}, 24)$ is self-dual. But by [38, Theorem 104], a binary $[24, 12, 8]$ code is unique so $C(M_{24}, 24)$ must be the extended Golay code $\mathcal{G}_{24}$. Further, filtering the sets of fixed points of the $2A$-involutions so that distinct ones only are included, we have

```
> Bl:=[];
> for i in FixedPoints2AInvs do
for>  if not (i in Bl) then
for|if> Bl:=Append(Bl,i);
for|if> end if;
for> end for;
> #Bl;
759
```

showing that there are 759 such distinct sets. It is well known that these fixed points of $2A$-involutions of M_{24} form the Witt system W_{24}.

```
 >D:=Design<5,24|Bl>;
 >D;
 5-(24, 8, 1) Design with 759 blocks.
```

Because W_{24} generates $\mathcal{G}_{24}$, we reach the same conclusion as before, that is,

$$C(M_{24}, 24) = \mathcal{G}_{24}.$$

The calculation:

```
gap> tom2:=TableOfMarks("M12:2");
TableOfMarks( "M12.2" )
gap> M12:=UnderlyingGroup(tom);
Group([ (1,2)(3,4)(5,24)(6,12)(7,9)(8,10)
(11,17)(13,14)(15,16)(18,23)(19,21)(20,22),
(1,8,17)(2,18,7)(3,13,14)
(4,20,19)(5,6,15)(21,24,23) ])


M12ext2:=PermutationGroup<24|(1,2)(3,4)(5,24)
(6,12)(7,9)(8,10)(11,17)(13,14)(15,16)(18,23)
(19,21)(20,22), (1,8,17)(2,18,7)(3,13,14)
(4,20,19)(5,6,15)(21,24,23)>;

> c:=SparseFixPointsCode(M12ext2);
> LinearCode(c);
[24, 12, 8] Linear Code over GF(2)
Generator matrix:
[1 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 1 0 1 0 1 1 1 0]
[0 1 0 0 0 0 0 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 1]
[0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1 1 1 1 1 0 1 0 0]
[0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 1 1 1 0 1 1]
[0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 1 1 1 1 0 1 0 1 0]
[0 0 0 0 0 1 0 0 0 0 0 0 0 1 1 0 1 1 1 0 0 1 0 1]
[0 0 0 0 0 0 1 0 0 1 0 0 0 1 0 1 1 0 0 0 1 1 0 1]
[0 0 0 0 0 0 0 1 0 1 0 0 0 1 1 0 0 1 1 1 0 0 1 0]
[0 0 0 0 0 0 0 0 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1]
[0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 1 0 1 0 1 0 1 1 1]
[0 0 0 0 0 0 0 0 0 0 0 1 0 1 1 0 1 0 0 1 1 0 1 1]
[0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 0 0 1 1 1 1 0 0]
```

shows that $\mathcal{G}_{24} = C(M_{12}{:}2, 12)$.

We now give a result which gives a refinement in the search for self-dual permutation codes invariant under a particular permutation group.

Lemma 4.2.8. *If there is a G-invariant self-dual code $\mathcal{C}$, then $\mathcal{C} \subseteq C(G,\Omega)$ and $C(G,\Omega)^{\perp} \subseteq \mathcal{C} \subseteq C(G,\Omega)$. In particular, the code $\langle Fix(\sigma)|\sigma \in I(G)\rangle$ is self-orthogonal.*

Proof. Since a self-dual code is necessarily self-orthogonal, we have

$$\mathcal{C} \subseteq C(G,\Omega)$$

by Theorem 4.2.2. Therefore $C(G,\Omega)^{\perp} \subseteq \mathcal{C} \subseteq C(G,\Omega)$. Note that

$$\langle \mathrm{Fix}(\sigma)|\sigma \in I(G)\rangle = C(G,\Omega)^{\perp}.$$

□

We use this lemma to find all self-dual codes invariant under a permutation group G of modest degree n. As an example, self-dual codes of length 132 with automorphism groups M_{11} are constructed from $C(M_{11}, 132)$. We note however that there does not always exist a G-invariant self-dual code even if $C(G,\Omega)^{\perp} \subseteq C(G,\Omega)$.

Example 4.2.9. Let $G = S_4(3) \cong PSU_4(2)$ and $H := 3^{1+2}_{+}{:}2A_4$. We get these groups in MAGMA by doing the following:

```
> load simgps;
Loading "/opt/magma/libs/simgps/simgps"
> G:=SimGroup("PSU42");
> Order(G);
25920
> Subs:=Subgroups(G:OrderEqual:=8*81);
> for i in Subs do
for> if (Order(Center(i`subgroup))eq 3) then
for|if> H:=i`subgroup;
for|if> end if;
for> end for;
> Order(H);
648
> 25920/648;
40.
```

The calculations of the orders agree with those given in the $\mathbb{ATLAS}$ [27]. We find the image of the action of G on the right coset space of H as follows:

```
> Gon40:=CosetImage(G,H);
> Gon40;
Permutation group Gon40 acting on a set of
 cardinality 40
    (1, 2)(3, 5)(4, 7)(6, 10)(8, 13)(9, 14)
    (11, 12)(15, 19)(16, 21)(17, 23)(18,24)
    (20, 25)(22, 27)(26, 31)(28, 32)(29, 33)
    (30, 34)(35, 37)(36, 38) (39,40)
     (2, 4, 8, 13)(5, 9, 15, 20)(1, 3, 6, 11)
    (7, 12, 17, 19)(10, 16, 22, 28)(14,18)
    (21, 26)(23, 29, 27, 31)
     (25, 30, 35, 34)(32, 33, 36, 39).
```

We use the MAGMA program

`FixPointsCode`

written to automate the calculations given in Example 4.2.7 to find the code spanned by the fixed point sets of involutions of the action image Gon40.

```
> V:=FixPointsCode(Gon40);
> dualcode:=LinearCode(V);
> dualcode;
[40, 15, 8] Linear Code over GF(2).
```

Note that we remove the generator matrices for all codes in our MAGMA output for spacial reasons. By definition, $C(G, G/H)$ is the dual of the code spanned by the fixed point sets of involutions. Thus

```
> code:=dual_code(V);
> code:=LinearCode(code);
> code;
[40, 25] Linear Code over GF(2)

> MinimumWeight(code);
4
```

which shows that $\mathcal{C} = C(G, G/H)$ is a $[40, 25, 4]$ code and $\mathcal{C}^{\perp}$ is a $[40, 15, 8]$ code. We now determine the G-invariant codes between $\mathcal{C}^{\perp}$ and $\mathcal{C}$ as follows:

```
> module:=GModule(Gon40,GF(2));
> module;
GModule module of dimension 40 over GF(2)
> Submods:=Submodules(module);
>  bases:=[Basis(m):m in Submods];
> codebases:=[];
> for i in bases do
for> theta:=map<i->VectorSpace(GF(2),40)|
x:->x>;
bas:=[theta(v): v in i];
for> codebases:=Append(codebases,bas);
for> end for;
> codes:=[LinearCode(sub<VectorSpace
(GF(2),40)|b>):b in codebases];
> codes:=[c:c in codes|c subset code];
> codes:=[c:c in codes|dualcode subset c];
> #codes;
4

> codes;
[
    [40, 15, 8] Linear Code over GF(2),

    [40, 16, 8] Linear Code over GF(2),

    [40, 24] Linear Code over GF(2),

    [40, 25, 4] Linear Code over GF(2)

]
```

We see that the subcodes above have dimensions $15, 16, 24$ and 24. It follows that there are no G-invariant self-dual codes of length 40 because there is no 20-dimensional subcode. We write a program

`GInvSelfDualCodes`

to automate the procedure above. Using this program gives:

```
> time se:=GInvSelfDualCodes(Gon40);
Time: 0.020
> #se;
0
```

The following shows that $C(G,\Omega)^{\perp} \subset C(G,\Omega)$, where $\Omega = G/H$.

```
> dualcode subset code;
true
```

showing that the condition $C(G,\Omega)^{\perp} \subset C(G,\Omega)$ does not guarantee existence of self-dual codes invariant under G.

If all the involutions of G act fixed point freely on Ω, then $C(G,\Omega)$ is the entire space $\mathbb{P}(\Omega)$. In this case the theorem only yields a trivial result. In the ensuing discussion, we assume, for simplicity that G acts transitively on Ω so we may consider $\Omega = G/H$ for some subgroup H of G.

Lemma 4.2.10. *Let σ be an involution of G. If $\sigma(aH) = aH$ for some $a \in N_G(I(H))$, then $\sigma(bH) = bH$ for all $b \in N_G(I(H))$.*

Proof. If $\sigma(aH) = aH$, then we have

$$\begin{aligned}(a^{-1}\sigma a)^2 &= a^{-1}\sigma^2 a \\ &= a^{-1}.1.a = 1\end{aligned}$$

so σ is an involution of H, that is $\sigma \in I(H)$. Take an arbitrary $b \in N_G(I(H))$. Then $b^{-1}\sigma b \in H$ and $\sigma(bH) = bb^{-1}\sigma(bH) = b(b^{-1}\sigma bH) = bH$. □

Lemma 4.2.11. *For $a \in G \setminus H$, the following conditions are equivalent:*

(1) $a \in N_G(I(H))$;

(2) $\{H, aH\} \in C(G, G/H)$.

In particular, $N_G(I(H)) \neq H$ if and only if the minimum weight of $C(G,G/H)$ is equal to 2.

Proof. Let $a \in N_G(I(H)) \setminus H$ and $\sigma \in I(H)$. By Lemma 4.2.10 if $aH \in \mathrm{Fix}(\sigma)$, then $bH \in \mathrm{Fix}(\sigma)$ for all $N_G(I(H)) \setminus H$. Thus $|\{H, aH\} \cap \mathrm{Fix}(\sigma)| \equiv 0 \mod 2$, that is $\{H, aH\} \in C(G, G/H)$.

Conversely, suppose $\{H, aH\} \in C(G, G/H)$. Let $s \in I(H)$. Then $sH = H$ so s fixes aH as well. Thus $saH = aH$ and $a^{-1}sa \in I(H)$. □

Suppose that $N_G(I(H)) \neq H$. Let $N = N_G(I(H)), r = |G : N|, m = |N : H|$, that is $n = |G : H| = |G : N||N : H| = mr$. Further, suppose that $\Omega' = G/N$. Let $\{g_1N, \ldots, g_rN\}$ and set

$$X_i = g_i(N/H) = \{g_iaH | a \in N\},\ i \in \{1, \ldots, r\}.$$

Then $\Omega = G/H = \dot{\bigcup}_{i=1}^{r} X_i$ and $|X_i| = m$ for each i. For $\sigma \in I(H)$, set

$$F_1(\sigma) = \{g_iN | X_i \subset \mathrm{Fix}(\sigma)\},$$

$$F_2(\sigma) = \{g_iN | X_i^\sigma = X_i\}.$$

By definition of $C(G, \Omega)$, we have $C(G, \Omega') = \langle F_2(\sigma) | \sigma \in I(G)\rangle^\perp \subset \mathbb{P}(\Omega')$. Let

$$C' = \langle F_1(\sigma) | \sigma \in I(G)\rangle^\perp\ (\subset \mathbb{P}(\Omega')).$$

Proposition 4.2.12. *With the notation as above,*

$$C(G, G/H) = \{W \subset \Omega | \{g_iN|\ |W \cap X_i| = odd\} \in C'\}.$$

The group $\mathrm{Aut}(C(G, G/H))$ *is isomorphic to the wreath product* $S_m \wr Aut(C')$.

Proof. Let $W \subseteq \Omega$. Suppose $E(W) = \{g_iN|\ |W \cap X_i| = \mathrm{odd}\}$. Then we have $W \in C(G, G/H)$ if and only if $|W \cap \mathrm{Fix}(\sigma)|$ is even for each $\sigma \in I(G)$. This bi-conditional statement is equivalent to the condition that $|E(W) \cap F_1(\sigma)|$ is even, that is, $E(W) \in C'$ as required. Since $|\tau(W) \cap X_i| = |W \cap X_i|$ for all permutations τ on X_i, by the well defined property of permutations, we have $S_{X_i} \subseteq \mathrm{Aut}(C(G, G/H))$.

Let $\rho \in \mathrm{Aut}(C(G, G/H))$. Denote by $\bar{\rho}$ the permutation on Ω' induced by ρ. Then the image of the map $\rho \overset{\theta}{\mapsto} \bar{\rho}$ is $\mathrm{Aut}(C')$. Furthermore, the kernel of this map is the direct product of the S_{X_i}. Therefore we have

$$\mathrm{Aut}(C(G, G/H)) \cong S_m \wr \mathrm{Aut}(C').$$

□

Proposition 4.2.13. *With the same notation as Proposition 4.2.12, the following statements hold:*

(1) If m *is even, then* $C(G, G/H)^\perp$ *is self-orthogonal ;*

(2) If m is odd, then $C(G, G/H)^{\perp}$ is self-orthogonal if and only if $C'^{\perp}$ is self-orthogonal;

(3) If $N_G(I(H)) \setminus H$ contains no involutions (the assumption holds if m is odd), then $C' = C(G, \Omega)$.

Proof. For (1) and (2) by Lemma 4.2.10, the set $\mathrm{Fix}(\sigma)$, σ in $I(G)$ is a union of some X_i's. Since the condition $X_i \subset \mathrm{Fix}(\sigma)$ is equivalent to $g_i N \in F_1(\sigma)$, we have

$$|\mathrm{Fix}(\sigma) \cap \mathrm{Fix}(\tau)| = m \times |F_1(\sigma) \cap F_1(\tau)|$$

for $\sigma, \tau \in I(H)$.

To prove (3), we have $F_1(\sigma) \subset F_2(\sigma)$. Let $g_i N \in F_2(\sigma)$. Then $\sigma(g_i(N/H)) = g_i(N/H)$, that is, $g_i^{-1}\sigma g_i \in N$. By hypothesis $g_i^{-1}\sigma g_i \in H$ and therefore $g_i H \in \mathrm{Fix}(\sigma)$. Thus $X_i \subset \mathrm{Fix}(\sigma)$ and $g_i N \in F_1(\sigma)$. Hence $F_1(\sigma) = F_2(\sigma)$. The result follows. □

Chapter 5

Survey on existence criteria for self-dual permutation codes

In this chapter we give a survey of existence criteria for self-dual permutation codes over arbitrary fields of positive characteristic not necessarily 2 we have been considering so far. Many of the results in this chapter are due to Fan Yun and Yuan Yuan [49]. In Theorem 3.9.1 we have already given a criterion for the existence of self-dual codes invariant under some permutation group due to Günther and Nebe. We will not refer to it here. We assume F to be a finite Galois field of order $q = p^l$, where p is a prime. We use X to denote a finite set. The F-vector space with basis X is denoted by FX. If X is a group then we have the group algebra discussed in Chapter 2. Any left ideal C of such a group algebra is called a **group code.**

5.1 Permutation codes

As in the introduction to this chapter, let X be a finite set and F be a Galois field of finite order. Let $FX = \{\sum_{x\in X} a_x x |\ a_x \in F\}$ be the F-vector space with basis X. Suppose X is a G-set for some group G. Extending the G-action on X linearly results in FX becoming an FG-module, that is if $X = \{x_1, x_2, \ldots, x_n\}$, for $g \in G$ and $\sum_i c_i x_i \in FX$, then

$$g\left(\sum_i c_i x_i\right) = \sum_i c_i (g x_i).$$

Such a module is called a permutation module.

Definition 5.1.1. We call C a G-**permutation** code of FX, denoted $C \subseteq FX$ if C is an FG-submodule of the FG-module FX.

Example 5.1.1. A finite group G is a G-set by left multiplication. The regular module of the group algebra FG is an FG-permutation module. A permutation module turns out to be just a left ideal of the algebra FG which is the group code defined in the introductory section of the chapter.

Example 5.1.2. Let $G = \{1, g, g^2, \ldots, g^{n-1}\} \cong \mathbb{Z}_n$ be a cyclic group of order n. Further, let $X = \overbrace{G \times \cdots \times G}^{m}$, a G-set by multiplication on the left. Then

$$FX = \overbrace{FG \oplus \cdots \oplus FG}^{m}$$

which is
$\{(a_{0,0} + a_{0,1}g + \cdots + a_{0,n-1}g^{n-1}, \ldots, a_{m-1,0} + a_{m-1,1}g + \cdots + a_{m-1,n-1}g^{n-1})$
$|a_{i,j} \in F\}$. Then a subset C of FX is a permutation code if and only if for arbitrary

$$(c_{0,0}, c_{0,1}, \ldots, c_{0,n-1}, \ldots, c_{m-1,0}, c_{m-1,1}, \ldots, c_{m-1,n-1}) \in C$$

then

$$(c_{0,n-1}, c_{0,0}, \ldots, c_{0,n-2}, \ldots, c_{m-1,n-1}, c_{m-1,0}, \ldots, c_{m-1,n-2})$$

is in C, that is, if and only if C is a cyclic code.

Though group codes can be viewed as permutation codes, permutation codes may not be group codes. The F-vector space FX is endowed with a non-degenerate symmetric bilinear form

$$\left\langle \sum_{x \in X} a_x x, \sum_{x \in X} b_x x \right\rangle = \sum_{x \in X} a_x b_x$$

for all $\mathbf{a} = \sum_{x \in X} a_x x, \mathbf{b} = \sum_{x \in X} b_x x \in FX$. This is called the classical inner product on FX. For $g \in G$,

$$\begin{aligned} < g(\mathbf{a}), g(\mathbf{b}) > &= \left\langle g\left(\sum_{x \in X} a_x x\right), g\left(\sum_{x \in X} b_x x\right) \right\rangle \\ &= \left\langle \sum_{x \in X} a_x gx, \sum_{x \in X} b_x gx \right\rangle = \sum_{x \in X} a_x b_x \\ &= < \mathbf{a}, \mathbf{b} > . \end{aligned}$$

The penultimate line follows because X is a G-set. Thus the classical inner product is G-invariant in the sense $< g(\mathbf{a}), g(\mathbf{b}) >=< \mathbf{a}, \mathbf{b} >$ for all $g \in G$ and $\mathbf{a}, \mathbf{b} \in FX$.

Remark 5.1.3. Let $U \subseteq FX$. We set the dual of U with respect to $<,>$ as usual, that is, $U^{\perp} = \{\mathbf{a} \in FX| \ < \mathbf{u}, \mathbf{a} >= 0 \text{ for all } \mathbf{u} \in U\}$. Recall from Chapter 1 that if C is any FG-submodule of FX then for any $g \in G, c^* \in C^{\perp}$ and $c \in C$, we have $< gc^*, c >=< gc^*, gg^{-1}c >=< c^*, g^{-1}c >= 0$, by the G-invariance of the inner product $<,>$.

Thus $C^{\perp}$ is also an FG-submodule. All the definitions of self-orthogonality, self-duality and other code-related definitions apply to permutation codes. We also recall the fact that self-duality of codes and of modules are different concepts. If $C \subseteq FX$ is a permutation code, that is a submodule of FX, then from Definition 3.1.10 we saw that C^*, the dual module of C, can be made into an FG-module via $gf(\mathbf{c}) = f(g^{-1}c)$ for all $g \in G, f \in C^*$ and $c \in C$. We have the following result.

Lemma 5.1.4. *Let $C \subseteq FX$ be an FG-permutation code. Then the classical inner product induces a homomorphism $\beta : FX \to C^*$ such that the following sequence of FG-modules is exact:*

$$0 \to C^{\perp} \to FX \xrightarrow{\beta} C^* \to 0.$$

Proof. For arbitrary $\mathbf{a} \in FX$ define $\beta_{\mathbf{a}} : C \to F, \mathbf{c} \mapsto < \mathbf{a}, \mathbf{c} >$. Then the map $\beta : FX \to C^*$ given by $\mathbf{a} \mapsto \beta_a$ is clearly surjective. Further, $\mathbf{a} + \mathbf{b} \mapsto \beta_{\mathbf{a}+\mathbf{b}}$ and

$$\begin{aligned} \beta_{\mathbf{a}+\mathbf{b}}(\mathbf{c}) &= < \mathbf{a} + \mathbf{b}, \mathbf{c} > \\ &= < \mathbf{a}, \mathbf{c} > + < \mathbf{b}, \mathbf{c} > \ \text{(linearity)} \\ &= \beta_{\mathbf{a}}(\mathbf{c}) + \beta_{\mathbf{b}}(\mathbf{c}) = (\beta_{\mathbf{a}} + \beta_{\mathbf{b}})(\mathbf{c}) \end{aligned}$$

so β is a linear map. For $g \in G, \mathbf{a} \in FX$ and $c \in C$, by G-invariance of the classical inner product, we have

$$\begin{aligned} \beta_{g\mathbf{a}}(\mathbf{c}) =< g\mathbf{a}, \mathbf{c} > &= < g\mathbf{a}, gg^{-1}\mathbf{c} >=< \mathbf{a}, g^{-1}\mathbf{c} > \\ &= \beta_{\mathbf{a}}(g^{-1}\mathbf{c}) \\ &= g\beta_{\mathbf{a}}(\mathbf{c}), \end{aligned}$$

that is $\beta_{g\mathbf{a}} = g\beta_{\mathbf{a}}$ for all $g \in G$ and $\mathbf{a} \in FX$. Thus β is an FG-homomorphism. The kernel of β is

$$\begin{aligned} \ker(\beta) &= \{\mathbf{a} \in FX |\ \beta_{\mathbf{a}}(\mathbf{c}) =< \mathbf{a}, \mathbf{c} >= 0 \text{ for all } \mathbf{c} \in C\} \\ &= C^{\perp}, \end{aligned}$$

that is $C^{\perp} = \mathrm{Im}(\mathrm{inc}) = \ker(\beta)$, where inc is the inclusion map $C^{\perp} \to FX$, so we have the desired exact sequence. □

The next corollary is just a restatement of a very basic result in coding theory.

Corollary 5.1.5. *If $C \subseteq FX$ is a self-orthogonal permutation code, then C is self-dual if and only if $dim(C) = |X|/2$. In particular, if FX has a self-dual code, then X is even.*

Proof. We note that because of the exact sequence of Lemma 5.1.4, we have $\mathrm{Im}(\beta) \cong FX/\ker(\beta)$ by the First Isomorphism Theorem for modules from which we have $\dim(\mathrm{Im}(\beta)) + \dim(\ker(\beta)) = \dim(FX)$ which is

$$\dim(C^*) + \dim(C^{\perp}) = |X|, \qquad (*)$$

by the exactness of the sequence. But it is well known that as vector spaces $C \cong C^*$ so $\dim(C) = \dim(C^*)$ so (*) becomes $\dim(C) + \dim(C^{\perp}) = |X|$. It follows that $C = C^{\perp}$ if and only if $|X| = 2.\dim(C)$. □

5.2 Transitive permutation codes

In this section we look at transitive permutation codes, that is, X is a transitive G-set. Recall from Theorem 2.3.1, the action of G on X is equivalent to the G-action on G/G_x. In particular, if $G_x \trianglelefteq G$, then the permutation module FX is equivalent to the regular module of the quotient group G/G_x. The stabilizer of G_x in G is $\{g \in G |\ gG_x = G_x\} = G_x$. The following corollary follows immediately from Corollary 5.1.5.

Corollary 5.2.1. *Let X be a transitive G-set and $x \in X$. If there is a self-dual code in FX, then $|G : G_x|$ is even.*

Proof. Suppose $C \subseteq FX$ is a self-dual code. Then considering the transitive action of G on G/G_x, by the Orbit-Stabilizer Theorem

$$\begin{aligned} |G| &= |\mathrm{Orb}_G(G_x)||G_{G_x}| \\ &= |G/G_x||G_x|, \end{aligned}$$

by transitivity and the observation about the stabilizer G_{G_x} of G_x in G given in the introduction. We have $|G : G_x| = |G|/|G_x| = |G/G_x| = 2.\dim(C)$ which is even. □

We recall from representation theory that if V is an FG-module there is a (composition) series of submodules $V = V_0 \supseteq V_1 \supseteq V_2 \supseteq \ldots \supseteq V_r = 0$ such that every quotient module V_{i-1}/V_i is a simple FG-module for $i = 1, \ldots, r$. The series is independent, up to isomorphism, of the choice of the factors, by the Jordan-Hölder Theorem for modules. It makes sense to refer to the multiplicity of a simple FG-module S in V.
If FG is a semisimple algebra, then it is a direct sum

$$FG = \bigoplus_{i=1}^{n} M_{n_i}(\Delta_i)$$

of matrix algebras $M_{n_i}(\Delta_i)$ of degree n_i over Δ_i, corresponding to a simple module S_i where $\Delta_i = \mathrm{End}_F(S_i)$ is the endomorphism algebra of S_i and n_i is the multiplicity of S_i in the regular module FG, by the Wedderburn Structure Theorem. In particular, the trivial FG-module F appears in the regular module FG exactly once.

Lemma 5.2.2. *Let X be a transitive G-set. If the characteristic p of F is prime to the order of G, then the trivial FG-module F appears in FX exactly once.*

Proof. Let $x \in X$. Then FX is the induced module $\mathrm{Ind}_{G_x}^{G}(F)$ of the trivial FG_x-module F. On the other hand, the regular FG_x-module $FG_x = \mathrm{Ind}_1^{G_x}(F)$ is an induced module. Under the conditions of the hypothesis, both FG_x are semisimple, since by Maschke's Theorem, FG is semisimple and very submodule of a semisimple module also has this property. Thus $FG_x = F \oplus \ldots$ and

$$FG = \mathrm{Ind}_{G_x}^{G}(F) \oplus \ldots \cong FX \oplus \ldots$$

in which the trivial module F appears once. The result follows. □

Before we state a non-existence criteria for self-dual permutation codes we state some group-theoretic results we need.

Definition 5.2.1. Let π be a set of primes and $x \in G$. We say x is a π-element if the order $o(x)$, of x is divisible only by primes in π. In particular, if $\pi = \{p\}$, we have the notion of a p-element. In a similar manner, G is a π-group if $|G|$ is divisible only by primes in π. A complementary set of primes to π will be denoted by π'. By $|G|_p$ we mean the highest power of a prime p dividing $|G|$.

Thus, from the definition above, we also have the notion of π'- and p'-elements as well as π'- and p'-groups. For example, a $2'$-element (group) is simply an element (group) of odd order.

Definition 5.2.2. A subgroup H of G is called a **Sylow** p-subgroup of G if H is a maximal p-group for some prime p dividing the order of G. In other words, a Sylow subgroup is a group of order $|G|_p$.

Definition 5.2.3. A subgroup H of G is called a **Hall** π-subgroup if H is a π-group and the index $|G : H|$, of H in G is not divisible by any prime in π. When $\pi = \{p\}, H$ is a Sylow p-subgroup of G.

Theorem 5.2.3. (Sylow) *Let G be a group and p a prime. Then*

(i) G possesses a subgroup of order $|G|_p$ and every p-subgroup of G is contained in a subgroup of order $|G|_p$ (A Sylow p-subgroup).

(ii) Any two Sylow p-subgroups are conjugate in G.

(iii) The number of distinct Sylow p-subgroups is of the form $1+kp$ for some non-negative integer k.

The following theorem is also useful.

Theorem 5.2.4. *(i) G is a π-group if and only if each element of $G^{\times}$ is a π-element.*

(ii) A normal p-subgroup of G is contained in every Hall p-subgroup of G.

(iii) G possesses a unique Hall p-subgroup if and only if a Hall subgroup of G is normal in G.

For proofs of the theorems above we refer the reader to Algebra introductory texts such as [1, 41]. An exercise in elementary group theory shows that if $|G| = p^n$, then for $1 \leq k \leq n$, G possesses a normal subgroup of order p^k (See for example [41, Ex 4.2 page 77]). We now state the results giving (non)existence criteria for self-dual permutation codes.

Proposition 5.2.5. *Let F be a field of odd characteristic. Further let X be a transitive G-set and $x \in X$. If the intersection of the stabilizer G_x of x with a Sylow 2-subgroup of G is a Sylow 2-subgroup of G_x, then there is no self-dual code in FX.*

Proof. Let T be a Sylow 2-subgroup of G. Assume that $|T| = 2^a$, $|T \cap G_x| = 2^b$ ($T \cap G_x$ is a Sylow 2-subgroup of G_x) and $|G_x| = 2^b n$. Then $|G| = 2^a nm$ with nm an odd integer. Consider the action of T on X and let $Y \subset X$ be a T-orbit. Choose an arbitrary $y \in Y$. Then by the transitivity of X there is a $g \in G$ such that $gx = y$. Therefore if $h \in G_x$, we have $ghg^{-1}y = ghg^{-1}(gx) = g(hx) = gx = y$ giving $ghg^{-1} \in G_y$. It follows that $gG_xg^{-1} = G_y$. Therefore,

$$\begin{aligned} T \cap G_y = T \cap gG_xg^{-1} &= gg^{-1}T \cap gG_xg^{-1} \\ &= g(g^{-1}T \cap G_xg^{-1}) \\ &= g(g^{-1}Tgg^{-1} \cap G_xg^{-1}) \\ &= g(g^{-1}Tg \cap G_x)g^{-1}. \end{aligned}$$

In particular $|T_y| = |T \cap G_y| = 2^b$ by the conjugacy of G_y and G_x. An application of the Orbit-Stabilizer Theorem gives the size of Y,

$$|Y| = |T : T_y| = |T|/|T_y| = 2^a/2^b = 2^{a-b}.$$

By transitivity of X and the Orbit-Stabilizer Theorem, $|G| = |X||G_x|$ giving $|X| = |G : G_x| = |G|/|G_x| = 2^a nm/2^b n = 2^{a-b}m$. It follows that the total number of T-orbits is $|X|/|Y| = 2^{a-b}m/2^{a-b} = m$, an odd integer. Therefore, as FT-modules we have $FX \cong \overbrace{FY \oplus \ldots \oplus FY}^{m}$. By Lemma 5.2.2, the trivial module F appears in FY exactly once, so the multiplicity of the trivial FT-module F in FX is the odd number m. Suppose that FG-module FX has a self-dual code C, that is, a submodule of FX and $C = C^{\perp}$. By Lemma 5.1.4, we have an exact sequence of FG-modules: $0 \to C \to FX \to C^* \to 0$, which is also an FT-sequence. Suppose the multiplicity of the FT-module F in C is m'. Then the multiplicity of the dual of the trivial FT-module F in C^* is also

m'. But the multiplicity of the trivial module F in C^* is m', by self-duality of F as an FT-module so the multiplicity of the trivial FT-module F in FX is $2m'$ contradicting the hypothesis that this multiplicity is odd. □

Corollary 5.2.6. *Assume that F is of odd characteristic. Let X be a transitive G-set and $x \in X$. Then there is a self-dual code in FX if one of the following holds:*

(1) $|G_x|$ is odd.

(2) G_x is normal.

(3) G has a normal Sylow 2-subgroup.

Proof. In any of the three cases, the intersection of G_x with any Sylow 2-subgroup of G is a Sylow 2-subgroup of G_x so the result follows. □

Recall from ring theory that a Galois ring $GR(p^r, k)$ is the unique Galois extension $\mathbb{Z}/p^r\mathbb{Z}$. Willems proved the following result.

Proposition 5.2.7. (Willems)[47, Proposition 3.1] *If p and r as above are odd, then no self-dual group codes exist over $R = GR(p^r, k)$.*

Proposition 5.2.8. (Willems) *Let r be odd. Then $GR(2^r, k)G$ contains a self-dual group code if and only if the order of G is even.*

Taking $X = G$ to be the regular G-set and $x = 1_G$, in Corollary 5.2.6, then $FX = FG$ and $G_{1_G} = \{1_G\}$. Conditions (1) and (2) of the hypothesis are satisfied and Willems' result Proposition 5.2.7 is obtained for the case of finite fields.

Proposition 5.2.9. *Suppose F is of characteristic 2. Let X be a finite transitive G-set and $x \in X$. If there is a subgroup H of G containing G_x such that $|H : G_x| = 2$, then there is a self-dual permutation code in FX.*

Proof. By hypothesis we can assume that $H = G_x \dot{\cup} hG_x$ where $h \in H \setminus G_x$ and $h^2 \in G_x$. The last condition is necessary otherwise $h^2 G_x$ would be a distinct coset, contradicting the hypothesis. Further assume that $|G : H| = n$ and $G = g_1 H \dot{\cup} \cdots \dot{\cup} g_n H$ with $g_1 = 1_G$. Let $Y = \{x, hx\} \subset X$. Then $X = Y \cup g_2 Y \cup \cdots \cup g_n Y$ is a disjoint union and as an F-vector space we have the following orthogonal direct sum:

$$FX = FY \oplus F(g_2 Y) \oplus \cdots \oplus F(g_n Y).$$

Consider the FH-submodule FY and let

$$C_1 = F.(x + hx) = \{ax + a(hx) |\ a \in F\}.$$

Then it is not difficult to see that C_1 is an FH-submodule of FY and $C_1 \subseteq C_1^{\perp}$. Because $\dim(C_1) = 1$ and
$\dim(FY) = 2$, by Corollary 5.1.5, $C_1 = C_1^{\perp}$ which is a self-dual code of FY. For $i = 1, 2, \ldots, n$ we have $g_i C_1$ is a subspace of $F(g_i Y)$ and is such that $g_i C_1 = (g_i C_1)^{\perp}$. Further,

$$C = C_1 \oplus g_2 C_1 \oplus \cdots \oplus g_n C_1$$

is an FG-submodule of FX and $C = C^{\perp}$, that is C is a self-dual permutation code in FX. □

If we take $X = G$, the regular G-set and $x = \mathbf{1}$, then we have G_{1_G}. By applying Sylow's Theorem, there exists a subgroup H of G such that $|H : \{1_G\}| = 2$ if and only if $|G|$ is even. Thus we deduce Willems' second result, Proposition 5.2.8 for the case of finite fields.

The following theorem settles completely the question of existence of G-invariant self-dual codes in the case where G is a direct product of finite 2- and $2'$-groups.

Theorem 5.2.10. *Let F be a finite field and $G = T \times S$ be a direct product of a finite 2-group T and a finite $2'$-group S and let X be a finite transitive G-set. Then the permutation FG-module FX has a self-dual code if and only if both the characteristic of F and the length of X are even.*

Proof. If X is odd, then by Corollary 5.2.1 FX has no self-dual code. Given that the characteristic p of the field F is odd, by Corollary 5.2.6 (3), FX has no self-dual code. This establishes necessity.

Assume that both p and X are even. Let $x \in X$ and G_x be the stabilizer of x in G. Then for $a, b \in G_x \cap S$, we have $2 \nmid \mathrm{o}(a)$ and $2 \nmid \mathrm{o}(b)$ as S is a $2'$ group. Because $a, b \in G_x, a.x = x$ and $b.x = x$. It follows that $a^{-1}.x = a^{-1}.(a.x) = (a^{-1}a).x = 1.x = x$ so $a^{-1}, b^{-1} \in G_x$ and hence $G_x \cap S$. For all $g \in G_x$ and $h \in G_x \cap S$, we have

$$\begin{aligned}
(g^{-1}hg).x = (g^{-1}h).(g.x) &= (g^{-1}h).x,\ (g.x = x, g \\
&= g^{-1}.(h.x), \\
&= g^{-1}.x,\ (h.x = x) \\
&= x,\ (g^{-1} \in G_x).
\end{aligned}$$

We conclude that $G_x \cap S \trianglelefteq G_x$. Clearly, the elements of $(G_x \cap S)^\times$ are of odd order, S being a group of odd order. It follows that $G_x \cap S$ is a $2'$ subgroup of G_x, by Theorem 5.2.4 (i). Because G_x contains at least one 2-element, $|G_x : G_x \cap S|$ is even. Therefore, we claim $G_x \cap S$ is a normal Hall $2'$-subgroup of G_x and $G_x \cap T$ is a normal Sylow 2-subgroup of G_x by a similar line of argument. Because $G_x \cap T$ and $G_x \cap S$ are normal subgroups of G_x which intersect trivially, ($(G_x \cap T)^\times$ comprises 2-elements while $(G_x \cap S)^\times$ comprises $2'$-elements). Further, it is not difficult to show that $G_x = (G_x \cap T)(G_x \cap S)$. Hence

$$G_x = (G_x \cap S) \times (G_x \cap T).$$

But $|T| = |T : G_x \cap T||G_x \cap T|$ and
$|S| = |S : G_x \cap S||G_x \cap S|$. We have

$$\begin{aligned} |G : G_x| = \frac{|G|}{|G_x|} &= \frac{|G|}{|(G_x \cap T) \times (G_x \cap S)|} \\ &= \frac{|G|}{|(G_x \cap S)||(G_x \cap T)|} \\ &= |G|.\frac{|S : G_x \cap S|}{|S|}\frac{|T : G_x \cap T|}{|T|} \\ &= |S : G_x \cap S|.|T : G_x \cap T|, \end{aligned}$$

since $\frac{|G|}{|T||S|} = 1$. Thus $|G : G_x| = |S : G_x \cap S|.|T : G_x \cap T|$. Since $|X| = |G : G_x|$ is even, $|T : G_x \cap T| = 2^b$ with $b \geq 1$. Note that $|S : G_x \cap S|$ is odd because $|S|$ is odd so $|G : G_x|$ even implies that $|T : G_x \cap T|$ is even. Because $|T| = 2^n$, the result in the discussion following Theorem 5.2.4 implies that there is a subgroup $R \leq T$ with order $2^k, 1 \leq k \leq n$ such that $R \supset G_x \cap T$ and $|R : G_x \cap T| = 2$. Set

$$H = (G_x \cap S) \times R \leq S \times T = G.$$

Then $H \supset G_x$ and

$$\begin{aligned} |H : G_x| &= \frac{|H|}{|G_x|} \\ &= \frac{|G_x \cap S||R|}{|(G_x \cap S)|G_x \cap T|} \\ &= \frac{|G_x \cap S|(|R : G_x \cap T||G_x \cap T|)}{|G_x \cap S||G_x \cap T|} \\ &= \frac{|G_x \cap S|.2.|G_x \cap T|}{|G_x \cap S||G_x \cap T|} \\ &= 2. \end{aligned}$$

Therefore, by Proposition 5.2.9 the permutation module FX has a self-dual code. □

The theorem above gives a complete answer for the existence of self-dual permutation codes for direct products of finite 2 and $2'$ groups. Hughes proved this result in [24] where there are stringent conditions on the group structure. Willems gave a complete classification in [47] in the case of group codes over Galois rings.

Chapter 6

Collection of results

In this chapter we give results obtained from our study.

6.1 Existence of self-dual codes of length n invariant under S_n

We first state the result for the action of the symmetric groups on their natural (regular) sets. We note that since a necessary condition for the existence of self-dual codes of length n is that the dimension of the code should be $\frac{n}{2}$ precludes odd n. Thus we study $S_n, n = 2m$, for $m \geq 2$. The case of S_2 produces a unique self-dual code.

Proposition 6.1.1. *Let $G = S_n$ or $A_n, n = 2m$ with $2 \leq m \leq 50$. Then there are no self-dual codes of length n admitting G as automorphism group. (Note that G does not necessarily have to be the full automorphism group).*

6.2 Self-dual codes invariant under some sporadic simple and almost simple groups

In this section we give the results of existence and non-existence of self-dual codes invariant under some sporadic simple and almost simple groups. In some cases complete classification was possible but in many instances we could only determine the number of self-dual codes invariant under a prescribed permutation group but no information on the (non)equivalence

or (non)isomorphism of the codes of a particular length could be obtained with computational resources available. Further, MAGMA can compute the minimum weights of codes of modest dimension. Where possible we provide such data. We use libraries of groups in the algebra packages GAP and MAGMA to obtain permutation groups and their subgroups to construct the code spanned by the sets of fixed points of involutions of these groups. For many of the groups, the GAP Burnside Table Of Marks was used to get a group and its representations of various degree. In the ensuing tables, by Rep we refer to the representation index in the GAP table of marks, Length is the cardinality of the G-set $\Omega = G/H$ for some $H \leq G$, Number is the quantity of self-dual codes of length "Length" invariant under the group "Group" and $\sharp$ is placed where information could not be obtained about minimum weights and equivalence. In instances where information about minimum weights and isomorphism could not be determined we use the symbol $\sharp$ under the remarks column. In some of the cases we have $[n, k, d]$ (α) under the remarks column to signify that there are α codes with the parameters $[n, k, d]$.

We now catalogue results obtained from sporadic simple and almost simple groups in the following tables.

Table 6.1: M_{11}-invariant self-dual codes.

Group	Length	Rep	Number	Remarks
M_{11}	12	37	0	
	22	36	1	$[22, 11, 2]$-code
	66	34	0	
	110	33	1	$[110, 55, 2]$-code
		32	1	$[110, 55, 2]$-code isomorphic with the one above
		31	3	2 isomorphic $[110, 55, 6]$-codes and one $[110, 55, 2]$-code isomorphic to the one of the previous representation
	132	30	3	$[132, 66, 12]$ (2) $[132, 66, 6]$ (1)
		29	3	$[132, 66, 4]$ (2) $[132, 66, 2]$ (1), ♯
	144	28	0	
	220	26	9	♯
		25	27	$[220, 110, 4]$ (14), $[220, 110, 10]$ (2) $[220, 110, 12]$ (10), $[220, 110, 2]$ (1)
		24	27	$[220, 110, 4]$ (24), $[220, 110, 2]$ (3)
	330	23	3	$[330, 165, 6]$ (1), $[330, 165, 8]$ (2)
		22	1	$[330, 165, 2]$ (1)
	396	21	0	
	440	20	15	$[440, 220, 8]$ (12), $[440, 220, 4]$ (2), $[440, 220, 2]$ (1)
		19	♯	♯
	660	17	0	
		16	567	♯
	720	15	0	
	792	14	♯	♯

Table 6.2: M_{12}-invariant self-dual codes.

Group	Length	Rep	Number	Remarks
M_{12}	12	146	0	
		145	0	
	66	144	0	
		143	0	
	132	142	3	$[132, 66, 2]$ (1), $[132, 66, 4]$ (2)
		141	3	$[132, 66, 2]$ (1), $[132, 66, 4]$ (2)
		140	9	$[132, 66, 8]$ (4), $[132, 66, 6]$ (2)
				$[132, 66, 4]$ (2), $[132, 66, 2]$ (1)
		139	3	$[132, 66, 2]$ (1), $[132, 66, 4]$ (2)
		138	9	$[132, 66, 8]$ (4), $[132, 66, 6]$ (2),
				$[132, 66, 4]$ (2), $[132, 66, 2]$ (1)
		137	3	$[132, 66, 2]$ (1), $[132, 66, 4]$ (2)
	144	136	0	
		135	0	
	220	134	3	$[220, 110, 18]$ (1), $[220, 110, 20]$ (2)
		133	3	$[220, 110, 18]$ (1), $[220, 110, 20]$ (2)
	264	132	183	♯
		131	183	♯
	396	130	0	
	440	129	11	♯
		128	11	♯
	660	125	0	
		124	0	
		123	0	
		122	0	
	792	121	243	♯
		120	735	♯
		119	243	♯
	880	118	0	
	990	117	5	
		116	5	
	1320	113	0	
	1728	101	0	
	1980	97	0	
		96	0	
		95	0	

Table 6.3: M_{12}:2-invariant codes.

Group	Length	Rep	Number	Remarks
M_{12}:2	24	211	1	$d = 8$. See Example 3.2.1
	132	210	3	♯
	144	209	0	
		208	0	
	264	207	27	♯
		206	187	♯
		205	27	♯
	288	204	57	♯
		203	267	♯
	396	202	0	
	440	201	35	♯
	792	196	327	♯
		195	615	♯
	880	194	0	
		192	299	♯
	990	189	439	♯
		188	439	♯
		187	299	♯
	1320	185	0	
	1584	183	555	♯
	1728	178	0	
	1980	174	0	

Table 6.4: M_{22}, M_{22}:2-invariant self-dual codes.

Group	Length	Rep	Number	Remarks
M_{22}	22	155	1	$d = 6$
	176	153	0	
		152	0	
	330	150	1	$d = 10$
		149	0	
	462	148	83	♯
		147	171	♯
	616	146	0	
	672	145	0	
	770	144	0	
	1232	140	549	
	1386	137	0	
M_{22}:2	22	488	1	$d = 6$
	44	487	6	$[44, 22, 2]$ (1), $[44, 22, 4]$ (2), $[44, 22, 6]$ (1), $[44, 22, 8]$ (2)
	154	485	6	$[154, 77, 2]$ (1), $[154, 77, 8]$ (1), $[154, 77, 10]$ (4), ♯
	330	483	1	$d = 10$
	352	482	10	♯
		481	0	
		480	53	♯
	462	479	106	♯
		478	55	♯
		477	99	♯
	616	476	0	
	672	474	0	
	770	473	0	
	1386	462	0	

Table 6.5: $M_{23}, M_{24}, J_1, HS, HS{:}2$ and Co_3-invariant codes

Group	Length	Rep	Number	Remarks
M_{23}	506	200	0	
		199	16	♯
	1288	198	0	
	24	1528	1	$\mathcal{G}_{24}$. See Example 2.3.1
M_{24}	276	1527	0	
	562	1526	20	♯
	1288	1524	0	
	266	39	0	
J_1	1540	36	0	
	1596	35	0	
	100	588	0	
	176	587	0	
	176	586	0	
HS	352	585	7	♯
	352	584	7	♯
	1100	583	0	
	1100	582	0	
	2	533	1	[2, 1, 2]
	100	2056	0	
	200	532	13	[200,100,4] (2),[200,100,2] (1) [200,100,12](6),[200,100,16](4)
$HS{:}2$	352	531	3	♯
	704	530	31	♯
	1100	2055	0	
	1100	2054	0	
Co_3	276	2482	0	
	552	2481	0	

Table 6.6: Self-dual codes invariant under J_2 and J_2:2

Group	Length	Rep	Number	Remarks
J_2	100	145	3	♯
	280	144	0	
	560	141	0	
	840	140	0	
	1008	139	0	
	1050	138	240	♯
	1800	135	0	
	1890	134	0	
J_2:2	100	371	1	a $[100, 50, 10]$-code
	200	370	23	♯
	280	369	0	
	560	366	165	♯
		365	295	♯
		364	201	♯
	630	363	25	♯
	840	362	0	
	1008	361	0	
	1050	360	61	♯
		359	25	♯
		358	25	♯
	1800	353	0	
	1890	352	0	

6.3 Concluding remarks

Remark 6.3.1. For the case of $G = M_{12}$:2 or M_{24}, and $|\Omega| = 24$ we obtain $C(G, \Omega) = \mathcal{G}_{24}$, the extended Golay code. See Example 4.2.7.

Remark 6.3.2. Let $G = M_{22}$ or M_{22}:2 and let $|\Omega| = 22$. Then $C(G, \Omega)$ is a $[22, 11, 6]$-code. This result was reported in [35].

Remark 6.3.3. Take $G = J_2$:2 and $|\Omega| = 100$. Then $C(G, \Omega)$ is the unique self-dual code invariant under G for this length. In particular, this code has parameters $[100, 50, 10]$. This result appears in [35].

Remark 6.3.4. If $G = M_{22}$:2 and $|\Omega| = 330$. Then we have $C(G, \Omega)$ is a $[330, 165, 10]$. This result appears in [35].

Remark 6.3.5. In the case $G = J_2$ and $|\Omega| = 100$, the three self-dual codes found are according to [35, Theorem 3.9], each one of C_{10}, C_{16} or C'_{16} the authors constructed in [36].

Remark 6.3.6. Let $G = M_{11}$ and $|\Omega| = 132$. By the GAP Table of Marks, [19], M_{11} has two inequivalent imprimitive representations of degree 132, namely those of indices 30 and 29 in the list of subgroups (see Table 6.1). Let Ω_1 and Ω_2 be the corresponding coset spaces for the groups which are the images of the permutation action of G on 132 points. Then by MAGMA, we have $C(G, \Omega_1)$ is a $[132, 67, 6]$-code and $C(G, \Omega_2)$ is a $[132, 67, 2]$-code. There are three self-dual codes between $C(G, \Omega_1)^\perp$ and $C(G, \Omega_1), \mathcal{C}_1, \mathcal{C}_2$ and $\mathcal{C}_3$, say. Two of these, $\mathcal{C}_1$ and $\mathcal{C}_2$, have minimum weight 12 and $\mathcal{C}_3$ has minimum weight 6. The group G acts on the set $\{\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3\}$ of the codes $\mathcal{C}_i$. By the Orbit-Stabilizer Theorem, we have $|G : G_{\mathcal{C}_i}| \leq 3$, using the fact that the set $\{\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3\}$ has three elements. But G has no subgroups of index ≤ 3, (see [37]). It follows that $\mathcal{C}_i, 1 \leq i \leq 3$ is G-invariant. Further, $G = \mathrm{Aut}(C(G, \Omega_1))$, whence $G \subseteq \mathrm{Aut}(\mathcal{C}_i) \subseteq \mathrm{Aut}(C(G, \Omega_1)) = G$. Therefore $\mathrm{Aut}(\mathcal{C}_i) = G$ for $i = 1, 2, 3$ and by Lemma 4.2.5, the three codes are inequivalent. These codes are the same as those obtained in [35].

There are three self-dual codes between $C(G, \Omega_2)^\perp$ and $C(G, \Omega_2)$. We could not ascertain (in)equivalence of the codes.

Appendix A

MAGMA Routines

```
//=============================================
//code_gen_by is a function that forms the
// vector space spanned by vectors <bas> given
// as sequences
//=============================================

code_gen_by:=function(bas)
V:=VectorSpace(GF(2),#bas[1]);
l:=[V!bas[j]:j in [1..#bas]];
 return sub<V|l>;
end function;

//=========================================
//the routine dual_code finds the dual
//  of the vector space <code>
//=========================================
dual_code:=function(code)
 if Dimension(code) eq 0 then
      basis:=[[i*0:i in [1..Degree(code)] ]];
    else
 basis:=Basis(code);
 basis:=[Eltseq(v): v in basis];
 end if;
  if Dimension(code) eq Degree(code) then
return code_gen_by([[i*0:i in [1..Degree(code)]]]);
```

```
 end if;
return Nullspace(Transpose(Matrix(GF(2),basis)));
end function;

//================================================
// is_self_dual is a function that tests whether a
//given code is self-dual
//================================================
is_self_dual:=function(code)
local dual;
         dual:=dual_code(code);
if dual eq code then
 return true;
  else
   return false;
end if;
end function;

//================================================
// Invoulutions(<group>) is a function that returns
//the conjugacy class representatives of a group
// <group> that are invoulutions of the group
//================================================
Involutions:=function(group)
local X,l;
      X:=ConjugacyClasses(group);
l:=[];
 for i in [1..#X] do
  if X[i,1] eq 2 then
 l:=Append(l,X[i,3]);
end if;
end for;
return l;
end function;

//================================================
//the function FixedPoints(permutation,setsize) returns
//the fixed points of the action of the permutation
```

```
// <permutation> on the set of size setsize
//=================================================
FixedPoints:=function(permutation,setsize)
 if Degree(permutation) gt setsize then
  print "fail";
 end if;
 return [x:x in [1..setsize]|x^permutation eq x];
end function;

//=================================================
//SetFixedPointsOnConjClass returns the sets of fixed
//points of the involutions in the conjugacy class
// with representative <rep>
//=================================================
SetFixedPointsOnConjClass:=function(group,setsize,rep)
Cl:=Setseq(Conjugates(group,rep));
Bl:=[];
  for i in [1..#Cl] do
     if not (FixedPoints(Cl[i],setsize) in Bl) then
       Bl:=Append(Bl,FixedPoints(Cl[i],setsize));
     end if;
  end for;
return Bl;
end function;
//================================

//=================================================
//PointsToBinary takes a set of points and returns
//a binary vector given as a list.
//=================================================
PointsToBinary:=function(codelength,points)
   if #points eq 0 then
      return [a*0: a in [1..codelength]];
   end if;
   if Maximum(points) gt codelength then
      return "Error! Code Length not sufficient";
   end if;
   code:=[];
```

```
      for i in [1..codelength] do
          if i in points then
         code[i]:=1;
          else
         code[i]:=0;
          end if;
      end for;
    return code;
end function;

//=======================================================
//SetPointsToBinary(codelength,points) takes a list
//<points> of vectors and applies PointsToBinary
// to each
//=======================================================
SetPointsToBinary:=function(codelength,points)
return [PointsToBinary(codelength,x):x in points];
end function;
//------------------------

//=======================================================
//SparseFixPointsCode is a subroutine of the next
// code
//=======================================================
SparseFixPointsCode:=function(group)
 setsize:=Degree(group);
 invconjreps:=Involutions(group);
 fixpts:=[];
 temp_code:=code_gen_by([[i*0:i in [1..setsize]]]);
 V:=VectorSpace(GF(2),setsize);
 for x in invconjreps do
     temp:=SetFixedPointsOnConjClass(group,setsize,x);
     binaries:=SetPointsToBinary(setsize,temp);
        for v in binaries do
           if (V!v in temp_code) eq false then
             fixpts:=Append(fixpts,v);
             temp_code:=code_gen_by(fixpts);
           end if;
```

```
        end for;
 end for;
return temp_code;
end function;

//=========================================================
//FixPointsCode(<group>) is a routine that returns the
//code spanned by the sets of fixed points of
// involutions of the group <group>
//=========================================================
FixPointsCode:=function(group)
           setsize:=Degree(group);
           sparse:=SparseFixPointsCode(group);
           module:=GModule(group,GF(2));
           code:=sub<module|Basis(sparse)>;
           bas:=Basis(code);
               if #bas eq 0 then
                  bas:=[b*0:b in [1..setsize]];
                   return code_gen_by([bas]);
                 else
                    phi:=Morphism(code,module);
                    bas1:=[phi(b):b in bas ];
theta:=map<bas1->VectorSpace(GF(2),
                           Dimension(module))|x:->x>;
                  bas2:=[theta(x):x in bas1];
return sub<VectorSpace(GF(2),Dimension(module))| bas2>;
                end if;
        end function;
//=====================================================
//GInvSelfDualCodes is a Function that finds the
// G-Invariant self-dual codes for a group G.
//=====================================================
GInvSelfDualCodes:=function(group)
 if (Degree(group)  eq 1 mod 2) then
    return [];
 end if;
 dualcode:=FixPointsCode(group);
  V:=VectorSpace(GF(2),Degree(group));
```

```
 if Dimension(dualcode) eq 0 then
    modu:=GModule(group,GF(2));
    dim:=Dimension(modu);
    bases:=[Basis(m):m in Submodules(modu)];
    bases:=[m:m in bases|#m eq dim/2];
    bases1:=[];
       for i in [1..#bases] do
    theta:=map<bases[i]->V|x:->x>;
     bas:=[theta(v):v in bases[i]];
           bases1:=Append(bases1,bas);
       end for;
    return [sub<V|b>:b in bases1];
 end if;//First case
 code:=dual_code(dualcode);
 if not (dualcode subset code) then
    return [];
 end if;
 if is_self_dual(code) eq true then
    return [code];
 end if;
 modu:=GModule(group,GF(2));
 submods:=Submodules(modu);
 bases:=[Basis(m):m in submods];
 codebases:=[];
    for i in [1..#bases] do
     theta:=map<bases[i]->V|x:->x>;
      bas:=[theta(v):v in bases[i]];
          codebases:=Append(codebases,bas);
     end for;
codes:=[sub<V|b>: b in codebases];
codes:=[c:c in codes|c subset code];
codes:=[c:c in codes|dualcode subset c];  //dito
d:=Degree(group)
selfdualcodes:=[c:c in codes|Dimension(c)eq d/2];
selfdualcodes:=[c:c in selfdualcodes|dual_code(c) eq c];
return selfdualcodes;
end function;
```

References

[1] R. B. J. T. Allenby. *Rings, Fields, and Groups: An Introduction to Abstract Algebra*. E. Arnold, 1983.

[2] J. L. Alperin. *Local Representation Theory: Modular Representations as an Introduction to the Local Representation Theory of Finite Groups*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1993.

[3] J. L. Alperin and R. B. Bell. *Groups and Representations*. Graduate Texts in Mathematics. Springer, 1995.

[4] M. Aschbacher. *Finite Group Theory*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2000.

[5] E. F. Assmus, Jr. and J. D. Key. *Designs and their Codes*. Cambridge: Cambridge University Press, 1992. Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).

[6] E. F. Assmus, Jr and H. F. Mattson, Jr. Coding and combinatorics. *SIAM Review*, 16:349–388, 1974.

[7] D. J. Benson. Modular Representation Theory. Autumn Session 2007, Aberdeen.

[8] P. E. Bland. *Rings and Their Modules*. De Gruyter Textbook Series. De Gruyter, 2011.

[9] W. Bosma and J. Cannon. *Handbook of Magma Functions*. Department of Mathematics, University of Sydney, November 1994. http://www.maths.usyd.edu.au:8000/u/magma/.

[10] W. Bosma and J. Cannon. *Discovering Mathematics with Magma: Reducing the Abstract to the Concrete*. Algorithms and Computation in Mathematics. Springer-Verlag, 2006. Vol 19, 1st Ed.

[11] P. J. Cameron and J. H. van Lint. *Designs, Graphs, Codes and their Links*. Cambridge: Cambridge University Press, 1991. London Mathematical Society Student Texts 22.

[12] J. Cannon and C. Playoust. *An Introduction to Magma*. School of Mathematics and Statistics, University of Sydney, 1994.

[13] C. W. Curtis and I. Reiner. *Representation Theory of Finite Groups and Associative Algebras*. Pure and Applied Mathematics. Interscience Publishers, 1962.

[14] L. L. Dornhoff. *Group Representation Theory: Ordinary Representation Theory*. Pure and Applied Mathematics. M. Dekker, 1971.

[15] L. L. Dornhoff. *Group Representation Theory: Modular Representation Theory*. Pure and Applied Mathematics. M. Dekker, 1972.

[16] D. S. Dummit and R. M. Foote. *Abstract Algebra*. John Wiley & Sons Canada, Limited, 2004.

[17] N. D. Elkies. Math 256x: The Theory of Error-Correcting Codes. `http://www.math.harvard.edu/~elkies/M256.13/`. Lecture Notes Fall 2013.

[18] W. Feit. *The Representation Theory of Finite Groups*. North-Holland Mathematical Library. Elsevier Science, 1982.

[19] GAP. Groups, Algorithms and Programming, Version 4. The GAP Group, Lehrstuhl D für Mathematik, RWTH Aachen, Germany and School of Mathematical and Computational Sciences, University of St. Andrews, Scotland. http://www.gap-system.org/.

[20] D. Gorenstein. *Finite Groups*. AMS Chelsea Publishing Series. American Mathematical Society, 2007.

[21] L. C. Grove. *Groups and Characters*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley-Interscience, 1996.

[22] A. Günther and G. Nebe. Automorphisms of doubly-even self-dual codes. *Bull. London Math. Soc.*, 41:769–778, 2009.

[23] R. Hill. *A First Course in Coding Theory*. Oxford Applied Mathematics and Computing Science Series. Oxford: Oxford University Press, 1986.

[24] G. Hughes. Structure theorems for group ring codes with an application to self-dual codes. *Des., Codes Cryptogr.*, 40:5–14, 2001.

[25] B. Huppert and N. Blackburn. *Finite Groups II*. Grundlehren Der Mathematischen Wissenschaften. Springer London, Limited, 2011.

[26] I. M. Isaacs. *Character Theory of Finite Groups*. Academic Press, New York, 1976.

[27] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson. *Atlas of Finite Groups*. Clarendon Press, Oxford, 1985.

[28] J. D. Key and J. Moori. Codes, designs and graphs from the Janko groups J_1 and J_2. *J.Combin. Math. Combin. Comput.*, 40:143–159, 2002.

[29] J. D Key and J Moori. Correction to Designs, codes and graphs from the Janko groups J_1 and J_2. *J. Combin. Math and Combin. Comput.*, 40: 143–159, 2002. *J. Combin. Math and Combin. Comput.*, 64:153, 2008.

[30] W. Knapp and P. Schmid. Codes with prescribed permutation group. *J. Algebra*, 67:415–435, 1980.

[31] S. Lang. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2002.

[32] K. Lux and H. Pahlings. *Representations of Groups: A Computational Approach*. Cambridge University Press, Cambridge, 2010.

[33] F. J. MacWilliams and N. J. A. Sloane. *The Theory Of Error-Correcting Codes*. North-Holland, Amsterdam, 1977.

[34] J. Moori. *Finite Groups and Representation Theory*. Lecture notes, AIMS, 2011.

[35] M. Harada N. Chigira and M. Kitazume. Permutation groups and binary self-orthogonal codes. *J. Algebra*, 309:610–621, 2007.

[36] N. Chigira, M. Harada and M. Kitazume. Some self-dual codes invariant under the Hall–Janko group. *J. Algebra*, 316:578 – 590, 2007.

[37] T. Occonor. The subgroup lattice of M_{11}. `http://homepages.ulb.ac.be/~tconnor/atlaslat/m11.pdf`.

[38] V. Pless. *Introduction to the Theory of Error-Correcting Codes*. Wiley Interscience, New York, 1998.

[39] B. Sundar Rajan and M. U. Siddiqi. A generalized DFT for abelian codes over $\mathbb{Z}_m$. *IEEE Trans. Inform. Theory*, 40:2082–2090, 1994.

[40] C. M. Rooney-Dougal. The primitive permutation groups of degree less than 2500. *J. Algebra*, 252:154–183, 2005.

[41] J. J. Rotman. *An Introduction to the Theory of Groups*. Graduate Texts in Mathematics. Springer, 1995.

[42] L. H. Rowen. *Ring theory*. Pure and Applied Mathematics. Elsevier Science, 1988. Volume I.

[43] L. H. Rowen. *Ring theory*. Pure and Applied Mathematics. Elsevier Science, 1988. Volume II.

[44] D. Seiple. An investigation of binary self-dual codes invariant under simple groups. Master's thesis, The University of Arizona, 2009.

[45] J. Thévenaz. *G-Algebras and Modular Representation Theory*. Oxford Mathematical Monographs. Oxford University Press, Inc, 1995.

[46] V. D. Tonchev. A characterization of Designs Related to Dodecads in the Witt System S(5,8,24). *J. Combin. Theory Ser. A*, 43:219–227, 1986.

[47] W. Willems. A note on self-dual group codes. *IEEE Trans. Inform. Theory*, 48:3107–3109, 2002.

[48] R. Wilson. *The Finite Simple Groups*. Graduate Texts in Mathematics. Springer, 2009.

[49] F. Yun and Y. Yuan. On self-dual permutation codes. *Acta Mathematica Scientia*, 28B:633–638, 2008.