

Codes of Designs and Graphs from Finite Simple Groups

by

Bernardo Gabriel Rodrigues

Submitted in fulfillment of the
requirements for the degree of
Doctor of Philosophy
in the

School of Mathematics, Statistics and Information Technology
University of Natal
Pietermaritzburg.

December 2002

Abstract

Discrete mathematics has had many applications in recent years and this is only one reason for its increasing dynamism. The study of finite structures is a broad area which has a unity not merely of description but also in practice, since many of the structures studied give results which can be applied to other, apparently dissimilar structures. Apart from the applications, which themselves generate problems, internally there are still many difficult and interesting problems in finite geometry and combinatorics. There are still many puzzling features about sub-structures of finite projective spaces, the minimum weight of the dual codes of polynomial codes, as well as about finite projective planes. Finite groups are an ever strong theme for several reasons. There is still much work to be done to give a clear geometric identification of the finite simple groups. There are also many problems in characterizing structures which either have a particular group acting on them or which have some degree of symmetry from a group action.

Codes obtained from permutation representations of finite groups have been given particular attention in recent years. Given a representation of group elements of a group G by permutations we can work modulo 2 and obtain a representation of G on a vector space V over \mathbb{F}_2 . The invariant subspaces (the subspaces of V taken into themselves by every group element) are then all the binary codes C for which G is a subgroup of $\text{Aut}(C)$. Similar methods produce codes over arbitrary fields. Through a module-theoretic approach, and based

on a study of monomial actions and projective representations, codes with given transitive permutation group were determined by various authors.

Starting with well known simple groups and defining designs and codes through the primitive actions of the groups will give structures that have this group in their automorphism groups. For each of the primitive representations, we construct the permutation group and form the orbits of the stabilizer of a point. Taking these ideas further we have investigated the codes from the primitive permutation representations of the simple alternating and symplectic groups of odd characteristic in their natural rank-3 primitive actions. We have also investigated alternative ways of constructing these codes, and these have come about by noticing that the codes constructed from the primitive permutations of the groups could also be obtained from graphs. We achieved this by constructing codes from the span of adjacency matrices of graphs. In particular we have constructed codes from the triangular graphs and from the graphs on triples.

The simple symplectic group $PSp_{2m}(q)$, where m is at least 2 and q is any prime power, acts as a primitive rank-3 group of degree $\frac{q^{2m}-1}{q-1}$ on the points of the projective $(2m-1)$ -space $PG_{2m-1}(\mathbb{F}_q)$. The codes obtained from the primitive rank-3 action of the simple projective symplectic groups $PSp_{2m}(q)$, where $q = 2^t$ with t an integer such that $t \geq 1$, are the well known binary subcodes of the projective generalized Reed-Muller codes.

However, by looking at the simple symplectic groups $PSp_{2m}(q)$, where q is a power of an odd prime and $m \geq 2$, we observe that in their rank-3 action as primitive groups of degree $\frac{q^{2m}-1}{q-1}$ these groups have 2-modular representations that give rise to self-orthogonal binary codes whose properties can be linked to those of the underlying geometry. We establish some properties of these codes, including bounds for the minimum weight and the nature of some classes of codewords.

The knowledge of the structures of the automorphism groups has played a key

role in the determination of explicit permutation decoding sets (PD-sets) for the binary codes obtained from the adjacency matrix of the triangular graph $T(n)$ for $n \geq 5$ and similarly from the adjacency matrices of the graphs on triples. The successful decoding came about by ordering the points in such a way that the nature of the information symbols was known and the action of the automorphism group apparent.

Although the binary codes of the triangular graph $T(n)$ were known, we have examined the codes and their duals further by looking at the question of minimum-weight generators for the codes and for their duals. In this way we find bases of minimum weight codewords for such codes. We have also obtained explicit permutation-decoding sets for these codes.

For a set Ω of size n and $\Omega^{\{3\}}$ the set of subsets of Ω of size 3, we investigate the binary codes obtained from the adjacency matrix of each of the three graphs with vertex set $\Omega^{\{3\}}$, with adjacency defined by two vertices as 3-sets being adjacent if they have zero, one or two elements in common, respectively. We show that permutation decoding can be used, by finding PD-sets, for some of the binary codes obtained from the adjacency matrix of the graphs on $\binom{n}{3}$ vertices, for $n \geq 7$.

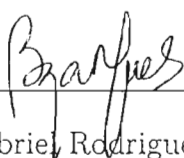
To *Bevanildo*

Preface

The work described in this thesis was carried out under the supervision and direction of Professor Jamshid Moori, School of Mathematics, Statistics and Information Technology, University of Natal, Pietermaritzburg and Professor Jennifer Denise Key, Department of Mathematical Sciences, Clemson University, South Carolina, USA, from February 2000 to August 2002.

The thesis represents original work by the author and has not otherwise been submitted in any form for any degree or diploma to any other University. Where use has been made of the work of others it is duly acknowledged in the text.

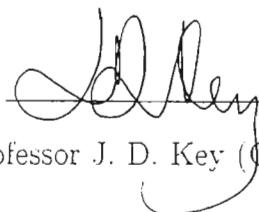
Signed:



Bernardo Gabriel Rodrigues



Professor Jamshid Moori (Supervisor)



Professor J. D. Key (Co-Supervisor)

Acknowledgements

I wish to thank both my advisors, Professors Jamshid Moori and Jennifer Denise Key for the advice, encouragement and guidance given to me during my studies which led to the compilation of this thesis. I am uncertain as to what extent words like thankfulness and gratitude could express the relevance of their dedication and devoted attention to me. In the absence of a word or words which could convey my sense of humble gratitude I would like to say it in the way I know best : muito obrigado.

I am grateful for the facilities made available to me by the School of Mathematics, Statistics and Information Technology of the University of Natal, Pietermaritzburg and by the School of Mathematical Sciences at Clemson University, South Carolina. I also wish to express my sincere gratitude to the Department of Mathematics at the University Agostinho Neto in Luanda for making all the contacts with the sponsors of my studies. I gratefully acknowledge the German Embassy in Angola and Professor Otto Berg who have made possible my first encounter with the Deutscher Akademischer Austausch Dienst (DAAD) from which I have had my scholarship. Special thanks are also due to the Ministry of Petroleum of the Republic of Angola (bursary), the University of Natal (graduate assistantship) and the National Research Foundation of South Africa (NRF)(bursary). My special thanks go to my wife Verónica Patricia L. d'Ornelas Sebastião and our son Bevanildo Derick de Ornelas Rodrigues for their

unfailing support and enormous patience during my studies. Special thanks are also due to both our families, for enduring me at almost any time. Finally I would like to thank my roommates Winter, Legesse and Kyle, for creating a pleasant working environment and to all my non mathematics friends Mr Gastão Lukangu and family, and Mrs Meryl Savage whose help and comfort I will always keep in mind. Last, but not least my thanks are due to my friend Faryad Ali whose valuable help and encouragement have paved the way for my getting to this stage.

Notation and conventions

Throughout this thesis all groups will be assumed to be finite. We will use notation and terminology from [3] and the ATLAS [27].

$[n, k, d]_q$	a q -ary code of length n , dimension k and minimum distance d
C	a q -ary code
\mathcal{D}	an incidence structure
Γ	a graph
$T(n)$	the triangular graph
$PG(V)$	the projective geometry
$AG(V)$	the affine geometry
G	a group
\mathcal{G}	a generator matrix for C
$\bar{\mathcal{G}}$	a generator matrix for C^\perp
1_G	the identity element of G
$K \leq G$	K is a subgroup of G
$K \not\leq G$	K is not a subgroup of G
$N \trianglelefteq G$	N is a normal subgroup of G
\mathbb{F}	a field
\mathbb{F}^*	$\mathbb{F} - \{0\}$
$\text{char}(\mathbb{F})$	characteristic of the field \mathbb{F}
$x \cdot y$	the dot product of x and y
$\text{Aut}(G)$	the automorphism group of G
$N \cdot K$	an extension of N by K
$N : K$	a split extension of N by K
k^g	conjugation of k by g
$N_G(K)$	the normalizer of the subgroup K in G
$C_G(K)$	the centralizer of the subgroup K in G

Ω, Λ	sets
\emptyset	empty set
$ \Omega $	the cardinality of the set Ω
\mathbb{F}_q	the Galois field of q elements
$GL_n(q)$	general linear group of dimension n over \mathbb{F}_q
$GL(V)$	general linear group over V
$Sc(V)$	the centre of $GL(V)$
$\dim(V)$	the dimension of a vector space V
$\text{pdim}(U)$	the projective dimension of U
S_n	the symmetric group on n symbols
A_n	the alternating group on n symbols
$V_n(q)$	a vector space of dimension n over \mathbb{F}_q
$Sp_{2m}(q)$	symplectic group of dimension $2m$ over \mathbb{F}_q
$\langle x_1, x_2, \dots, x_n \rangle$	the subspace spanned over \mathbb{F} by the subset $\{x_1, x_2, \dots, x_n\}$
$\text{Aut}(C)$	the automorphism group of a code C

Contents

1	Introduction	1
2	Groups	9
2.1	Permutation groups	9
2.2	Permutation representations	10
2.3	Primitive groups	14
2.4	Rank-3 primitive permutation groups	16
2.4.1	Symplectic groups	17
2.4.2	Alternating groups	22
3	Codes and Combinatorial Structures	24
3.1	Codes	24
3.2	Designs	29
3.3	Graphs	32
3.4	Finite geometries	35
3.4.1	Projective geometries	36
3.4.2	Affine geometries	38

<i>CONTENTS</i>	xi
3.5 Decoding schemes	39
3.5.1 Nearest neighbour decoding	40
3.5.2 Majority logic decoding	40
3.5.3 Permutation decoding	42
4 Codes from Combinatorial Structures	47
4.1 Codes from designs	47
4.2 Codes from graphs	50
4.3 Codes from geometries	52
5 Codes from Groups	55
5.1 Introduction	55
5.2 Codes from primitive groups	58
5.3 Codes from the Janko groups J_1 and J_2	61
5.3.1 The computations for J_1	62
5.3.2 The computations for J_2	64
6 A conjecture of Key and Moori	66
6.1 Introduction	66
6.2 Symplectic groups	68
6.3 Alternating groups	70
6.3.1 Computations for A_6	70
6.3.2 Computations for A_9	72
7 Binary Codes from Symplectic Groups	77

<i>CONTENTS</i>	xii
7.1 Introduction	77
7.2 The binary codes	78
8 Binary Codes of Triangular Graphs	88
8.1 Introduction	88
8.2 The binary codes	89
9 Binary Codes from Graphs on Triples	98
9.1 Introduction	98
9.2 The binary codes	100
10 Permutation Decoding	124
10.1 Introduction	124
10.2 Codes of the triangular graphs	125
10.3 Codes of the graphs on triples	130
10.4 PD-sets through computation	137
10.4.1 Codes from A_6 and A_9	137
10.4.2 Binary codes of the Chang graphs	139
Appendices	141
A Programmes $A1$ and $A2$	142
A.1 Programme $A1$	142
A.2 Programme $A2$	144
B Generators for $O_8^+(2) : 2$	149

<i>CONTENTS</i>	xiii
C PD-sets Through Computation	151
D Minimum Weights	153
E Gordon Bound	155
F $w(\pi)$ for Lemma 9.2.14	157
G Construction of codes from graphs	158
H Constructing the Chang codes	161
I A PD-set for the Chang 2 code	163
Bibliography	164
Index	174

Chapter 1

Introduction

Codes are built to transmit messages reliably from a sender to a receiver. During transmission a message is encoded, sent through a channel, and then decoded. At any stage during the transmission of a message, an error could be introduced. The error-correction and error-detection capabilities of a code are dependent on the smallest difference between any two words in the code, that is, the minimum distance. For linear codes the minimum distance is the same as the minimum weight of the code.

In [3], Assmus and Key describe codes, designs, finite geometries, and their interconnections. The codes associated with finite geometries are members of the class of well known and frequently used generalized Reed-Muller codes. These codes have a number of convenient properties, including that established by Delsarte [31, 32, 33], Goethals [35] and MacWilliams [36], and in related papers (see [5] for a full set of references) that the minimum weight of these codes is the block size of the geometrical design, and that the minimum-weight vectors generate the code. Thus a basis of minimum words exist, and in [45], Gao and Key constructed an explicit basis in the case of the designs of points and hyperplanes from geometries over a prime field.

Related to the prior problem, the question arises as to whether the other generalized Reed-Muller codes are generated by their minimum words. Ding and Key examined this in [42] where it is established exactly which of these codes are generated by their minimum words.

The projective and affine geometries over finite fields provide a wide range of combinatorial designs that can in many cases serve as classifying tools for other designs with the same parameters. This association has led to a productive exchange of ideas between the realms of finite geometries, design theory and coding theory. The codes from geometries first came to importance in applications when it was seen that the combinatorics could lead to a very effective decoding algorithm, known as the majority logic decoding (see [81]). The codes actually used in this algorithm are the dual codes of the codes from geometries or designs, and thus knowledge of the minimum weight of the dual code became an important issue. Such knowledge has not been established in the vast majority of cases. For the binary case, in [18] the actual minimum weight for the codes from finite geometries is obtained. For the odd case, and for non-desarguesian planes, the results are sporadic, but the papers [26, 63, 64, 65] go some way in getting improved bounds. In general the dual codes of these codes are not generalized Reed-Muller codes; these are the so-called polynomial codes. Their minimum weight is not known in general and in [61, Section 7] some new results that deduce the minimum weight from the geometrical properties of the designs are described.

Although drawing on results and definitions from a broad spectrum of mathematical fields, this thesis is concerned principally with the study of the interplay between groups and combinatorial structures such as codes, designs, graphs and finite geometries. A general methodological aim of this thesis has been to illustrate the theory presented as richly as possible with examples.

Coding theory has made many contributions to the theory of combinatorial designs. A code generated by the incidence matrix of designs has been useful in

either constructing new designs or showing that certain designs do not exist, as it is for example the case of the projective plane of order 10. Coding theory has also been used to extend designs. In [59] Kennedy and Pless extended designs “held” by vectors of a code. The connection between designs and codes leads to the construction of new designs. Using the knowledge about codes and the existence of designs in codes can be useful for decoding purposes. For example a binary vector x of weight w is said to determine the block of w points corresponding to the positions where x has non-zero coordinates. In such case we say that vectors of a fixed weight w in a binary code of length n hold a t -design if the blocks determined by these vectors are the blocks of a t -design on n points. This means that there must exist t and λ so that every set of t coordinate positions occurs as non-zero positions for exactly λ vectors of weight w . The knowledge of the number of vectors of each weight existing in a code is crucial in determining whether or not the supports of these vectors could form a design. For $q = 2$ the supports are in a one-to-one correspondence with the codewords. The celebrated Assmus-Mattson Theorem gives conditions on the weight enumerators of a code and its dual that are sufficient to ensure that the support of the minimum weight vectors (and other weights also) yield a t -design where t is less than the minimum weight.

On the other hand designs have had tremendous impact in coding theory since the geometry of the design helps in the determination of the weight distribution of the code. Also, design properties can be used in decoding algorithms, and geometrical configurations can be used to define good codes.

Throughout this thesis using a construction method outlined in [66] we will consider the construction of codes from designs obtained from primitive permutation representations of some finite simple groups as well as codes from graphs.

Given a non-empty set Ω of size n we form graphs Γ whose vertices are the k element subsets ($k > 1$) of Ω and adjacency is defined according to whether these

subsets meet or are disjoint. For example for any n , the triangular graph $T(n)$ is the graph whose vertices are the 2-element subsets of a set of cardinality n in which two distinct vertices are adjacent if and only if they are not disjoint. It is a strongly regular graph on $\binom{n}{2}$ vertices, that is on the pairs of letters $\{i, j\}$ where $i, j \in \{1, \dots, n\}$.

The code formed by the span of the adjacency matrix of Γ is also the code of the $1-(v, k, k)$ design obtained by taking the rows of the adjacency matrix as the incidence vectors of the blocks. The automorphism group of this design will contain the automorphism group of the graph, the latter of which is the symmetric group S_n . In a similar manner, given a set Ω of size n and $\Omega^{\{3\}}$ the set of subsets of Ω of size 3, we examine the binary codes obtained from the adjacency matrix of each of the three graphs with vertex set $\Omega^{\{3\}}$, with adjacency defined by two vertices as 3-sets being adjacent if they have zero, one or two elements in common, respectively.

Codes obtained from permutation representations of finite groups have been given particular attention in recent years. Given a representation of group elements of a group G by permutations we can work modulo 2 and obtain a representation of G on a vector space V over \mathbb{F}_2 . The invariant subspaces (the subspaces of V taken into themselves by every group element) are then all the binary codes C for which G is a subgroup of $\text{Aut}(C)$. This modular technique has been used in [12, 13, 74]. Similarly we could produce codes over fields of characteristic p , where $p > 2$. In [74], Knapp and Schmid consider $[n, k, d]_q$ codes where the monomial automorphism group is a particular group. The groups examined were the alternating groups A_n , the symmetric groups S_n and the Mathieu groups written as permutation groups of degree n and associated with codes of length n . Important information about these codes can be obtained from the theory of modular representations of groups. Calderbank and Wales in [17] have used this idea to construct a binary code of length 176 and dimension 22

whose automorphism group is the Higman-Sims group. Brooke in [12, 13] has found all codes obtainable this way from the primitive permutation representations of the simple groups $PSU_4(2)$ and $PSU_3(3)$. In particular are examined all binary codes arising from primitive permutation representations of these groups. In [49] a $[276, 23, 100]_2$ self-orthogonal doubly-even code left invariant by the Conway simple group Co_3 was constructed. Its residual code with respect to a minimum weight codeword is the $[176, 22, 50]_2$ code left invariant by the Higman-Sims simple group HS referred to above and constructed in [17].

Also, starting with well known simple groups and defining designs and codes through the primitive actions of the groups will give structures that have the groups in their automorphism groups. In [66] Key and Moori have examined all such designs, graphs and some associated codes, for the Janko groups J_1 and J_2 . For each of the primitive representations, the permutation groups were constructed and the orbits of the stabilizer of a point were formed.

In the preliminary chapters (Chapter 2 and Chapter 3) we present general results on group theory and combinatorial structures that will be required in the sequel.

The link between combinatorial design theory, graph theory and algebraic coding theory has proved useful to further understanding of these structures. For example, codes have helped in the characterization of designs, and design theory has provided examples of codes with effective encoding and decoding algorithms and whose minimum weights and weight distributions can be found through the combinatorial properties of the designs. In Chapter 4 we establish the interplay between these combinatorial structures. The methods employed to exploit this link include use of geometrical and combinatorial properties of the designs and their automorphism groups.

In Chapter 5 we examine some of the successful applications of the association

between combinatorial designs and groups. In particular we look at codes obtained from primitive permutation representations of some finite simple groups. In a manner of illustration we describe the codes derived from the primitive permutation representations of two sporadic simple groups, namely the first and the second Janko groups J_1 and J_2 . These codes and their respective properties have been established in [66]. For each of the primitive representations the permutation groups were constructed, formed the orbits of the stabilizer of a point, and for each of the non-trivial orbits, the self-dual symmetric 1-designs and subsequently binary linear codes were obtained. In fact the work described in [66] constitutes the berth for the ideas and results established in this thesis as a whole.

In Chapter 6, we deal with a conjecture that has been stated by Key and Moori in [66]. In examining the codes and designs arising from the primitive representations of the first two Janko groups, Key and Moori in [66, Section 7] suggested that the computations made for these Janko groups could lead to the conjecture: “any design \mathcal{D} obtained from a primitive permutation representation of a simple group G will have the automorphism group $\text{Aut}(G)$ as its full automorphism group, unless the design is isomorphic to another one constructed in the same way, in which case the automorphism group of the design will be a proper subgroup of $\text{Aut}(G)$ containing G ”. While the conjecture is true for the Janko groups J_1 and J_2 , and some other simple groups, we show that it is not always true. We found examples of finite simple groups G with a primitive representation giving a design \mathcal{D} such that the automorphism group of G does not contain the automorphism group of \mathcal{D} . Furthermore, there are finite simple groups that have automorphisms that do not preserve the design. Specifically, we considered computationally all the primitive permutation representations of G where G is the alternating group A_6 or A_9 .

In their natural primitive rank-3 action on the points of projective space of dimension $2m - 1$, the projective symplectic groups $PSp_{2m}(q)$, where q is a power

of an odd prime and $m \geq 2$, have 2-modular representations that give rise to self-orthogonal binary codes whose properties can be linked to those of the underlying geometry. In Chapter 7, we establish some properties of these codes, including bounds for the minimum weight and the nature of some classes of codewords. Alternatively these codes could be obtained by taking the row span over \mathbb{F}_2 of an adjacency matrix of the strongly regular graph defined by the rank-3 action of $PSp_{2m}(q)$. Since we are looking at rank-3 groups, the graphs are actually strongly regular.

In Chapter 8, we examine the codes of the triangular graph $T(n)$ and their duals, and in particular we show that the symmetric group S_n on n letters is the full automorphism group of each code for $n \geq 5$ except in the case $n = 6$. We also look at the question of minimum-weight generators of the codes and of their duals. The triangular graph $T(n)$ is defined to be the line graph of the complete graph K_n , for any n . It is a strongly regular graph of type $((\binom{n}{2}), 2(n-2), n-2, 4)$. Alternatively $T(n)$ ($n > 4$) may be viewed as the graph whose vertices are the 2-element subsets of a set of cardinality n in which two distinct vertices are adjacent if and only if they are not disjoint. The code formed by the span of the adjacency matrix is also the code of the $1-(\frac{n(n-1)}{2}, 2(n-2), 2(n-2))$ design \mathcal{D} obtained by taking the rows of the adjacency matrix as the incidence vectors of the blocks. An alternative way to construct these codes is through the primitive rank-3 action of the simple alternating group A_n , for $n \geq 5$, on the 2-subsets (or duads) $\Omega^{\{2\}}$ of a set Ω of size n . The orbits of the stabilizer in A_n of a duad $P = \{a, b\}$ consist of $\{P\}$ and one of length $2(n-2)$ and the other of length $\frac{(n-2)(n-3)}{2}$. We take as points the duads of Ω that is, $\mathcal{P} = \Omega^{\{2\}}$ and for each $P \in \Omega^{\{2\}}$ we define a block \bar{P} to be $\{Q \in \Omega^{\{2\}} \mid P \cap Q \neq \emptyset, Q \neq P\}$, that is the orbit of length $2(n-2)$. The duads $\mathcal{P} = \Omega^{\{2\}}$ and blocks $\mathcal{B} = \{\bar{P} \mid P \in \mathcal{P}\}$ form a symmetric $1-(\frac{n(n-1)}{2}, 2(n-2), 2(n-2))$ design whose binary code is examined. In particular the dimension and weight enumerator of the codes are determined.

In Chapter 9, in a manner similar of that described in Chapter 8, given a set Ω of size n and $\Omega^{\{3\}}$ the set of subsets of Ω of size 3, we examine the binary codes obtained from the adjacency matrix of each of the three graphs with vertex set $\Omega^{\{3\}}$ and adjacency defined by two vertices as 3-sets being adjacent if they have zero, one or two elements in common, respectively.

Chapter 10 is entirely dedicated to applications of our results in that we obtain the so-called PD-sets. A PD-set for a t -error-correcting code C is a set S of automorphisms of C such that every possible error vector of weight t or less can be moved by some member of S to another vector where the s non-zero entries for, $s \leq t$ have been moved out of the information positions. In other words, every t -set of coordinate positions is moved by at least one member of S to a t -set consisting only of check-position coordinates. For small t , PD-sets can be found computationally. PD-sets are given in both computational and explicit forms. The knowledge of the structures of the automorphism groups has played a key role in the determination of explicit permutation decoding sets for the binary codes obtained from the triangular graphs and those of the graphs on triples. The success of decoding these codes came about by ordering the points in such a way that the nature of the information symbols was known and the action of the automorphism group apparent. Since most of the groups we have dealt with act naturally as primitive rank-3, the graphs obtained are in fact strongly regular. We have also investigated the cases where the graphs are not strongly regular and the action of the groups is not rank-3. This is the case of the binary codes from graphs on triples.

All computations were carried out with the aid of Magma [11] versions 2.7 and 2.8 running on a Sun GX2 computer in Pietermaritzburg and on a Sun Blade 1000 computer at Clemson. We have developed various programmes for dealing with designs, codes, graphs and PD-sets and these are outlined in the Appendices of the thesis.

Chapter 2

Groups

The aim of this chapter is to assemble in readily usable form a selection of mostly standard results from the theory of groups, which will be required in the sequel. We will not give proofs of every result. Most of the results could be found in standard texts such as [10, 21, 85].

2.1 Permutation groups

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

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

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

where $\alpha, \beta \in \Omega$ and $g \in G$. The number of orbits of G on $\Omega \times \Omega$ is called the **rank** of G on Ω , which is denoted by $\text{rank}(G)$. If α, β are distinct points of Ω , then the pairs (α, α) and (α, β) lie in different orbits of G on $\Omega \times \Omega$. Thus, for $|\Omega| > 1$, the rank of G is at least 2. A permutation group is said to be **2-transitive** (or **doubly transitive**) on Ω if it is transitive on the ordered pairs of distinct points of Ω . Thus, for $|\Omega| > 1$ the 2-transitive groups are precisely the permutation groups of rank 2.

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

If G has rank r on $\Omega \times \Omega$ then a point stabilizer will have exactly r orbits on Ω and we say that such a stabilizer is a **rank- r** subgroup of G .

2.2 Permutation representations

Definition 2.2.1 *Let G be a group and Ω be a set. An **action** of G on Ω is a function which associates to every $\alpha \in \Omega$ and $g \in G$ an element α^g of Ω such that, for all $\alpha \in \Omega$ and all $g, h \in G$, $\alpha^1 = \alpha$ and $(\alpha^g)^h = \alpha^{gh}$. In a natural way, an action defines a **permutation representation** of G on Ω , which is a homomorphism ψ from G into S_Ω .*

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

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

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

Theorem 2.2.2 *Let G act on a set Ω . Then $|\alpha^G| = [G : G_\alpha]$, that is the number of elements in the orbit of α is equal to $[G : G_\alpha]$.*

Proof: See [85]. ■

Corollary 2.2.3 *If G is a finite group acting on a finite set Ω then $\forall \alpha \in \Omega$ we have $|\alpha^G| \mid |G|$.*

Proof: By Theorem 2.2.2 we have $|\alpha^G| = [G : G_\alpha] = \frac{|G|}{|G_\alpha|}$. Hence $|G| = |\alpha^G| \cdot |G_\alpha|$. Thus $|\alpha^G|$ divides $|G|$. ■

Theorem 2.2.4 (i) *If G is a finite group, then $\forall g \in G$ the number of conjugates of g in G is equal to $[G : C_G(g)]$.*

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

Proof: (i) Since G acts on itself by conjugation, using Theorem 2.2.2 we have $|g^G| = [G : C_g]$. But since $g^G = \{g^h \mid h \in G\} = \{hgh^{-1} \mid h \in G\} = [g]$ and

$G_g = \{h \in G \mid g^h = g\} = \{h \in G \mid hgh^{-1} = g\} = \{h \in G \mid hg = gh\} = C_G(g)$, we have $|g^G| = |[g]| = [G : C_G(g)] = \frac{|G|}{|C_G(g)|}$.

(ii) Let G act on the set of all its subgroups by conjugation. Then by the Theorem 2.2.2 we have $|H^G| = [G : G_H]$. Since $H^G = \{H^g \mid g \in G\} = \{gHg^{-1} \mid g \in G\} = [H]$ and $G_H = \{g \in G \mid H^g = H\} = \{g \in G \mid gHg^{-1} = H\} = N_G(H)$ we have $|[H]| = |H^G| = [G : G_H] = [G : N_G(H)] = \frac{|G|}{|N_G(H)|}$. ■

Note 2.2.5 If G is a finite transitive group acting on a finite set Ω , then Theorem 2.2.2 (ii) implies that

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

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

Definition 2.2.6 Let G act on a set Ω . Let $|\Omega| = n$ and $1 \leq k \leq n$ be a positive integer. We say that G is **k -transitive** on Ω if for every two ordered k -tuples $(\alpha_1, \alpha_2, \dots, \alpha_k)$ and $(\beta_1, \beta_2, \dots, \beta_k)$ with $\alpha_i \neq \alpha_j$ and $\beta_i \neq \beta_j$ for $i \neq j$ there exists $g \in G$ such that $\alpha_i^g = \beta_i$ for $i = 1, 2, \dots, k$.

Lemma 2.2.7 Let G be a transitive group on a set Ω , $|\Omega| = n \geq 2$. If G_α is $(k-1)$ -transitive on $\Omega \setminus \{\alpha\}$ for every $\alpha \in \Omega$, then G is k -transitive on Ω .

Proof: See [10, Lemma 1.3.6]. ■

Theorem 2.2.8 [85] If G is a k -transitive group on a set Ω with $|\Omega| = n$, then

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

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

Definition 2.2.9 *The automorphism group of a group G , denoted by $\text{Aut}(G)$, is the set of all automorphisms of G , under the operation of composition.*

Definition 2.2.10 *Let g be any element of G . Define a map $\phi_g : G \longrightarrow G$ by $\phi_g(x) = gxg^{-1}$ for all $x \in G$. Then ϕ_g is an automorphism of G , known as an inner automorphism of G .*

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

Theorem 2.2.11 (1) *If H is a subgroup of G , then $C_G(H) \trianglelefteq N_G(H)$ and $N_G(H)/C_G(H)$ can be embedded in $\text{Aut}(H)$, that is $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$.*

(2) *The set of all inner automorphisms of G , denoted by $\text{Inn}(G)$, is a normal subgroup of $\text{Aut}(G)$ and $G/Z(G) \cong \text{Inn}(G)$.*

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

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

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

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

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

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

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

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

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

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

2.3 Primitive groups

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

and $\{\alpha\}$ for $\alpha \in \Omega$ are called **trivial blocks of imprimitivity**. All other blocks of Ω are said to be **non-trivial**.

Definition 2.3.1 A permutation group G is said to be **primitive** on Ω if G is transitive on Ω and the only G -invariant partitions of Ω are the trivial partitions. Also G is said to be **imprimitive** on Ω if G is transitive on Ω and G preserves some non-trivial partition of Ω .

Theorem 2.3.2 (i) For every n , the symmetric group S_n acts n -transitively on $\Omega = \{1, 2, \dots, n\}$,
(ii) for $n \geq 3$ the alternating group A_n acts $(n-2)$ -transitively, but not $(n-1)$ -transitively on Ω .

Proof: (i) Since S_n contains all permutations of the set Ω , it is clearly n -transitive on Ω .

(ii) We use induction on n , beginning with the fact that A_3 is transitive, but not 2-transitive, on $\{1, 2, 3\}$. For $n > 3$ we have that $(A_n)_n = A_{n-1}$, and A_{n-1} is $(n-3)$ -transitive on $\{1, 2, \dots, n-1\}$ by the induction hypothesis. So A_n is $(n-2)$ -transitive, by Lemma 2.2.7. Now suppose that A_n is $(n-1)$ -transitive, then there is $g \in A_n$ fixing each $1, 2, \dots, n-2$ and taking $n-1$ to n . But the only $g \in A_n$ which does this is the transposition $(n-1 \ n) \notin A_n$. ■

Theorem 2.3.3 Every k -transitive group G (with $k \geq 2$) acting on a set Ω , is primitive.

Proof: See [10, Lemma 1.6.3]. ■

Theorem 2.3.4 (Characterization of primitive permutation groups) Let G be a transitive permutation group on a set Ω . Then G is primitive if and only if for each $\alpha \in \Omega$, the stabilizer G_α is a maximal subgroup of G .

Proof: See [10, Theorem 1.6.5]. ■

2.4 Rank-3 primitive permutation groups

In this section we consider finite primitive permutation groups of rank-3.

Given a transitive permutation group G on Ω , the number of orbits of the point stabilizer G_α is independent of the particular $\alpha \in \Omega$ and it is equal the rank of G . From Section 2.1 we know that for $|\Omega| \geq 2$ we have $\text{rank}(G) \geq 2$.

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

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

In [95] Wielandt shows that a primitive group of degree $2p$ with p a prime has at most rank-3. In fact $p = 5$ is the only prime for which a transitive group of degree $2p$ is known to exist. Any 4-transitive group has rank-3 when considered as a group of permutations of the unordered pairs of distinct symbols. Thus, in addition to the symmetric and alternating groups, the Mathieu groups are included among the rank-3 groups. The projective (classical) groups of linear type are doubly transitive on the points of the projective space, but are primitive of rank-3 on the lines when the degree is at least 4. Those of symplectic and unitary types of degree at least 4 are primitive of rank-3 when considered as group of permutations of the absolute points (see Section 2.4.1). Those of orthogonal type of degree at least 5 are primitive of rank-3 on the singular points, the groups of characteristic 2 being excluded for odd degrees. The study of finite primitive permutation groups has lead to the discovery of interesting new groups (for instance, some sporadic simple groups) and to application of new techniques in the theory of permutation groups. For more information on rank-3 permutation groups the reader is encouraged to consult [43, 55, 58, 76, 77] and [51, Section 2].

In light of the preamble we will study the alternating and the symplectic groups as examples of finite primitive permutation groups of rank-3. Both these groups will be of use in Chapter 7 and Chapter 8 respectively. In the next section we give a brief account of the symplectic groups followed by the alternating groups in Section 2.4.2.

2.4.1 Symplectic groups

For the classical background on symplectic forms and symplectic groups see [1, 37, 41, 40, 55, 91].

Definition 2.4.1 *Let V be a finite dimensional vector space over a field \mathbb{F} . A function \langle, \rangle from the set $V \times V$ of ordered pairs in V to \mathbb{F} is called a **bilinear form** on V if for each $v \in V$, the functions $\langle v, \rangle$ and $\langle, v \rangle$ are linear functionals on V . In this case we say that (V, \langle, \rangle) is an **inner product space**.*

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

Remark 2.4.2 A bilinear form \langle, \rangle is called **alternating (symplectic)** on V if $\langle x, x \rangle = 0$ for all $x \in V$.

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

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

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

Definition 2.4.3 Let V be a vector space over a field \mathbb{F} . Let $\langle, \rangle : V \times V \longrightarrow \mathbb{F}$ be a bilinear form on V such that

- (i) $\langle x, x \rangle = 0, \quad \forall x \in V$
- (ii) $\langle x, y \rangle = -\langle y, x \rangle, \quad \forall x, y \in V.$

Then we say that (V, \langle, \rangle) is a **symplectic space** over the field \mathbb{F} .

Remark 2.4.4 If $\text{char}(\mathbb{F}) \neq 2$, then the properties (i) and (ii) in the above definition are equivalent.

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

Definition 2.4.5 Let (V, \langle, \rangle) be a symplectic space. If $x, y \in V$, then x and y are **orthogonal** if $\langle x, y \rangle = 0$. If W is a subspace of V then the **orthogonal complement** of W is defined by

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

Note 2.4.6 Note that for all $x \in W$ we have $\langle 0, x \rangle = \langle x - x, x \rangle = \langle x, x \rangle - \langle x, x \rangle = 0 - 0 = 0$, so that $0 \in W^\perp$. Now if $x, y \in W^\perp$, then for any $\alpha, \beta \in F$ and $z \in W$ we have

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

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

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

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

Definition 2.4.9 Consider (V, \langle, \rangle) with \langle, \rangle bilinear. If $\{v_1, v_2, \dots, v_m\}$ is an ordered basis of V , then the **inner product matrix** of \langle, \rangle relative to this basis is given by an $m \times m$ matrix $A = [\langle v_i, v_j \rangle]_{m \times m}$.

$$\langle u, v \rangle = u M v^T \quad (2.1)$$
$$B = \begin{bmatrix} & & & & 1 \\ & & & 1 & \\ & & \ddots & & \\ & & & \ddots & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ 1 & & & & \end{bmatrix},$$

then

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

Thus

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

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

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

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

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

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

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

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

The projective symplectic groups are simple except for $PSp_2(2) = PSL_2(2)$, $PSp_2(3) = PSL_2(3)$ and $PSp_4(2)$. The order of $PSp_{2m}(q)$ is given by

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

Now if we let $\mathcal{P}(V)$ denote the projective space defined by V , that is $\mathcal{P}(V) = PG_{2m-1}(q)$ (see Section 3.4 for more details on projective geometry). The symplectic form on V defines a **polarity** on $\mathcal{P}(V)$, a correspondence between

the elements of $\mathcal{P}(V)$ that reverses inclusion and has order 2. If we denote this polarity by σ , then for any $U \in \mathcal{P}(V)$ we have $\sigma : U \mapsto U^\sigma$ where

$$U^\sigma = \{v \mid v \in V, uMv^T = 0, \forall u \in U\}. \quad (2.2)$$

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

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

If P is a point of the projective $(2m - 1)$ -space $PG_{2m-1}(q)$ then the affine subgroup of $G = PSp_{2m}(q)$ is the stabilizer G_P of the form $N : PSp_{2m-2}(q)$, a split extension, where N is a p -group of order q^{2m-1} (see [47]).

If $q = p^r$ where p is an odd prime, N will be a non-abelian special p -group of order q^{2m-1} . If $p = 2$, then N is an elementary abelian 2-group. For further information on the affine subgroups of the symplectic group, see ([84, Chapter 10]).

The simple symplectic group $PSp_{2m}(q)$, where m is at least 2 and q is any prime power, acts as a primitive rank-3 group of degree $\frac{q^{2m}-1}{q-1}$ on the points of the projective $(2m - 1)$ -space $PG_{2m-1}(\mathbb{F}_q)$, (see Theorem 2.4.10). The orbits of the stabilizer of a point P consist of $\{P\}$ and one of length $\frac{q^{2m-1}-1}{q-1} - 1$ and the other of length q^{2m-1} .

Theorem 2.4.10 *If $m \geq 2$, then $PSp_{2m}(q)$ acts as a primitive permutation group of rank-3 on the points of $\mathcal{P}(V)$.*

Proof: See [91, Theorem 8.2 and Theorem 8.3]. ■

2.4.2 Alternating groups

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

Lemma 2.4.11 *If $n \geq 3$ then the alternating group A_n acts transitively on $\Omega^{\{2\}}$ the set of duads of $\Omega = \{1, 2, \dots, n\}$.*

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

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

Theorem 2.4.12 *The alternating group A_n where $n \geq 5$ acts primitively as a rank-3 permutation group of degree $\frac{n(n-1)}{2}$ on $\Omega^{\{2\}}$ where $\Omega = \{1, 2, \dots, n\}$.*

Proof: That the action is transitive follows from Lemma 2.4.11. Since A_n acts on $\Omega^{\{2\}}$ and $|\Omega^{\{2\}}| = \binom{n}{2}$ we have that

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

Now

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

Clearly

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

and

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

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

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

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

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

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

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

Remark 2.4.13 If $n = 4$, then Theorem 2.4.12 is not true since $(A_4)_{\{\sigma_1, \sigma_2\}} \cong S_2 = \{1_{S_2}, (\sigma_1 \sigma_2)(\sigma_3 \sigma_4)\}$ and A_4 is clearly not a rank-3 group on $\Omega^{\{2\}}$ where $\Omega = \{1, 2, 3, 4\}$.

Chapter 3

Codes and Combinatorial Structures

In this chapter we focus on codes, designs and finite geometries. For a more detailed account and additional information the reader is advised to consult [3, 9, 21] and [80].

3.1 Codes

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

If V is a vector space over the field \mathbb{F}_q , an **invertible semilinear transformation** from the vector space V onto V is a pair (S, α) such that S is a bijection from V onto V , α is an automorphism of \mathbb{F}_q , and for all x and y in

V and a, b in \mathbb{F}_q we have

$$S(ax + by) = \alpha(a)S(x) + \alpha(b)S(y).$$

The group of all invertible semilinear transformations from V to V is denoted by $\Gamma L(V)$. The subgroup of $\Gamma L(V)$ whose elements are of the form (S, α) where α is the identity map on \mathbb{F}_q , is the group of all invertible linear transformations $GL(V)$. The groups $\Gamma L(V)$ and $GL(V)$ are known as the semilinear group and the general linear group, respectively. The group of all invertible scalar transformations $Sc(V)$ is the centre of $GL(V)$ and is a normal subgroup of $\Gamma L(V)$. The quotient groups $\Gamma L(V)/Sc(V)$ and $GL(V)/Sc(V)$ are the projective semilinear group $P\Gamma L(V)$ and the projective linear group $PGL(V)$ of V , respectively. The affine linear group $AGL(V)$ is the semi-direct product the additive group of V with $GL(V)$. The affine semilinear group $A\Gamma L(V)$ is the semi-direct product the additive group of V with $\Gamma L(V)$. The action of the element (S, v) in $AGL(V)$ on a vector x is defined by $(S, v) : x \mapsto S(x) + v$. The action of the element $((S, \alpha), v)$ of $A\Gamma L(V)$ on a vector x is defined similarly.

Definition 3.1.1 *Let F be a set of q elements. A q -ary code C is a set of finite sequences of the elements of F , called codewords (words) . If all the codewords are sequences of the same length n , then C is called a **block code** of length n .*

Definition 3.1.2 *Let C be a q -ary code and x and y words in C . The **Hamming distance** between x and y , denoted by $d(x, y)$, is the number of positions in which the words x and y differ. The **minimum distance** d of C is the smallest Hamming distance between any two distinct words in C , that is $d = \min\{d(x, y) \mid x, y \in C, x \neq y\}$.*

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

Definition 3.1.3 A linear code C of length n over the field \mathbb{F}_q is a subspace of \mathbb{F}_q^n . We write $C = [n, k]_q$ where $\dim(C) = k$.

Two linear codes of length n over the field \mathbb{F}_q are **equivalent** if each can be obtained from the other by permuting the coordinate positions of \mathbb{F}_q^n and multiplying each coordinate by a non-zero element of the field. They are **isomorphic** if each can be obtained from the other by a permutation of the coordinate positions. Every linear code of length n over \mathbb{F}_q contains the zero vector $0 \in \mathbb{F}_q^n$ whose entries are all the zero element of the field. If $d(x, y)$ is the Hamming distance of x, y in C , then $x - y$ is in C and $d(x, y) = d(0, x - y)$. This implies that for a linear code, the minimum distance d of the code is the smallest number of non-zero entries of the codewords of the code.

Definition 3.1.4 If C is a linear code of length n over the field \mathbb{F}_q then the **weight** of a word x in C is defined to be $\text{wt}(x) = d(0, x)$.

It then follows that the minimum distance of a linear code C is the **minimum weight** of the code. When the minimum weight d of a linear code $C = [n, k]$ is known, we write $C = [n, k, d]_q$. For a linear code $C = [n, k, d]_q$, we have the **Singleton bound** $d \leq n - k + 1$ (see [3]).

Let C be a linear $[n, k, d]_q$ code. We let $A_i(c)$ denote the number of codewords at distance i from a codeword $c \in C$. The numbers $A_i(c)$ where $0 \leq i \leq n$, are called the **weight distribution** of C with respect to c . Obviously $A_0(c) = 1$, $A_i(c) \geq 0$, and $\sum_i A_i(c) = q^k$. For linear codes (and some non-linear codes) $A_i(c)$ is independent of c and will be denoted by A_i .

Definition 3.1.5 Let C be a linear code. Then the **weight enumerator** of C is the polynomial $W_C(x, y) = \sum_{c \in C} x^{n-\text{wt}(c)} y^{\text{wt}(c)} = \sum_{i=0}^n A_i x^{n-i} y^i$.

Remark 3.1.6 The weight enumerator classifies codewords according to the number of non-zero coordinates. More detailed information is supplied by the

complete weight enumerator, which gives the number of codewords of each composition.

Definition 3.1.7 Let C be a $[n, k]_q$ code. A **generator matrix** for C denoted by \mathcal{G} is a $k \times n$ matrix obtained from any k linearly independent vectors of C .

Definition 3.1.8 Let C be a $[n, k]_q$ code. The **dual code** or **orthogonal code** of C denoted by C^\perp , is the orthogonal under the standard inner product, that is $C^\perp = \{v \in F_q^n \mid (v, c) = 0 \text{ for all } c \in C\}$.

From elementary linear algebra we have that $\dim(C) + \dim(C^\perp) = n$, since C^\perp is simply the null space of a generator matrix for C . Taking \mathcal{G} to be the generator matrix for $C = [n, k]_q$, a generator matrix $\bar{\mathcal{G}}$ for C^\perp is a $(n - k) \times n$ matrix that satisfies $\mathcal{G}\bar{\mathcal{G}}^T = 0$, that is $c \in C$ if and only if $c\bar{\mathcal{G}}^T = 0 \in F_q^{n-k}$. For any vector y in F_q^n the vector $y\bar{\mathcal{G}}^T$ is called the **syndrome** of y , denoted $\text{Syn}(y)$. If x and y are in F_q^n , then $\text{Syn}(x) = \text{Syn}(y)$ if and only if x and y are in the same coset of C . We will see in Section 3.5 that syndromes can be used to decode a received message more efficiently.

Definition 3.1.9 Any generator matrix $\bar{\mathcal{G}}$ for C^\perp is called a **parity-check** or **check matrix** for C . If \mathcal{G} is written in the standard form $[I_k \mid A]$, then $\bar{\mathcal{G}} = [-A^T \mid I_{n-k}]$ is a check matrix for the code with generator matrix \mathcal{G} .

Any code is isomorphic to a code with generator matrix in standard form. The first k coordinates are called the **information symbols** and the last $n - k$ coordinates are the **check symbols**.

We can use the generator matrix for a linear code to encode a message. In fact a generator matrix in standard form simplifies encoding. Suppose that we have a set of data consisting of q^k messages that are to be transmitted. We encode the message using a code C with a generator matrix \mathcal{G} . To do this we identify

the data with the vectors in \mathbb{F}_q^k . Then for $u \in \mathbb{F}_q^k$, we encode u by forming the vector $u\mathcal{G}$. If $u = (u_1, u_2, \dots, u_k)$ and \mathcal{G} has rows R_1, R_2, \dots, R_k , where each R_i is in \mathbb{F}_q^n , then u is encoded as:

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

But when \mathcal{G} is in standard form, the encoding takes the simpler form $u \mapsto (u_1, u_2, \dots, u_k, x_{k+1}, \dots, x_n)$, and here the u_1, u_2, \dots, u_k are the message or information symbols, and the last $n-k$ entries are the check symbols, and represent the redundancy.

In general it is not easy to say anything about the minimum weight of C^\perp knowing only the minimum weight of C but, of course either a generator matrix or a check matrix gives a complete information about both C and C^\perp . In particular, a check matrix for C determines the minimum weight of C in a useful way:

Theorem 3.1.10 *Let $\bar{\mathcal{G}}$ be a check matrix for a $[n, k, d]$ code C . Then every choice of $d-1$ or fewer columns of $\bar{\mathcal{G}}$ forms a linearly independent set. Moreover if every $d-1$ or fewer columns of a check matrix for a code C are linearly independent, then the code has minimum weight at least d .*

Proof: See [3, Theorem 2.3.1]. ■

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

Definition 3.1.11 *If C is a linear code of length n over \mathbb{F}_q , then any isomorphism of C onto itself is called an **automorphism** of C . The set of all automorphisms of C is called **automorphism group** of C , denoted by $\text{Aut}(C)$.*

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

The automorphism group of C is thus a subgroup of S_n , or of S_Ω if $C \subseteq \mathbb{F}_q^\Omega$. The existence of automorphism for C can provide a richer structure for the code and allow the use of deeper results from group theory. In particular when C has a regular automorphism group $G \subseteq \text{Aut}(C)$; this means that G is transitive on Ω and that $|G| = |\Omega| = n$, the block length of C .

3.2 Designs

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

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

Definition 3.2.1 *An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set \mathcal{P} , block set \mathcal{B} and incidence \mathcal{I} is a t -(v, k, λ) **design** if*

- (1) $|\mathcal{P}| = v$;
- (2) every block $B \in \mathcal{B}$ is incident with precisely k points;
- (3) and every t distinct points are together incident with precisely λ blocks.

Remark 3.2.2 A t -(v, k, λ) design is also referred to as a t -design. We shall assume that all the parameters are positive integers, and that $v > k \geq t$ (to avoid trivial cases). Also the members of \mathcal{B} must be distinct, thus repeated blocks are not allowed.

Theorem 3.2.3 A t -design \mathcal{D} is also an s -design, for $1 \leq s \leq t$. If the given design has parameters t -(v, k, λ) then its parameters as an s -design are s -(v, k, λ_s) where

$$\lambda_s = \lambda \cdot \frac{(v-s)(v-s-1)\dots(v-t+1)}{(k-s)(k-s-1)\dots(k-t+1)} \quad (3.1)$$

Proof: See [10, Theorem 3.2.2]. ■

Definition 3.2.4 Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with $|\mathcal{P}| = v$ and $|\mathcal{B}| = b$. Let the points be labelled $\{p_1, p_2, \dots, p_v\}$ and the blocks be labelled $\{B_1, B_2, \dots, B_b\}$. An **incidence matrix** for \mathcal{D} is a $b \times v$ matrix $A = (a_{ij})$ of 0's and 1's such that

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

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

A design is **trivial** if every k -set of points is incident with a block of the design. A design is called **simple** if distinct blocks are not incident with the same set of k points. In this thesis all designs will be simple and non-trivial designs. We define λ_i to be the number of blocks incident with i points, $0 \leq i \leq t$. It follows that $\lambda_t = \lambda$, $\lambda_0 = b$ and λ_1 is the number of blocks through any point in the

design, referred to as the **replication number** for the design, and denoted by r . A counting argument proves the well known relationship between the parameters

$$\lambda_i = \lambda_{i+1} \frac{(v-i)}{(k-i)}. \quad (3.2)$$

In particular,

$$vr = bk. \quad (3.3)$$

Definition 3.2.5 The **dual** structure of \mathcal{D} is $\mathcal{D}^t = (\mathcal{B}^t, \mathcal{P}^t, \mathcal{I}^t)$, where $\mathcal{P}^t = \mathcal{B}$, $\mathcal{B}^t = \mathcal{P}$ and $\mathcal{I}^t = \{(B, p) \mid (p, B) \in \mathcal{I}\}$.

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

Definition 3.2.6 Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$. Then the **complement** of \mathcal{D} is the structure $\overline{\mathcal{D}} = (\overline{\mathcal{P}}, \overline{\mathcal{B}}, \overline{\mathcal{I}})$, where $\overline{\mathcal{P}} = \mathcal{P}$, $\overline{\mathcal{B}} = \mathcal{B}$ and $\overline{\mathcal{I}} = \mathcal{P} \times \mathcal{B} - \mathcal{I}$.

Theorem 3.2.7 If \mathcal{D} is a $t - (v, k, \lambda)$ design with $v - k \geq t$, then $\overline{\mathcal{D}}$ is a $t - (v, v - k, \overline{\lambda})$ design, where

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

Proof: See [3, Theorem 1.3.1] ■ .

Definition 3.2.8 An **automorphism** of a design $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is a permutation π of \mathcal{P} such that $B \in \mathcal{B}$ implies $\pi(B) \in \mathcal{B}$.

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

Lemma 3.2.9 [10] *Let \mathcal{D} be a t -design with $t \geq 2$. Then the group of automorphisms of the design acts faithfully on \mathcal{B} .*

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

Theorem 3.2.10 *Let G be a t -transitive permutation group on a finite set Ω , with $t \geq 2$, and suppose that Δ is a subset of Ω , with $|\Delta| = k$, $|\Omega| = v$, and $1 < k < v - 1$. Then the set $\mathcal{B} = \{\Delta^g \mid g \in G\}$ is the set of blocks of a t -design \mathcal{D} , and G is a group of automorphisms acting transitively on \mathcal{B} .*

Proof: See [10, Theorem 3.4.3]. ■

Only a few symmetric designs are known to enjoy the property that a primitive nonsolvable group of automorphisms acts on points and blocks. In [57], Kantor classified all designs with 2-transitive group of automorphisms. In [38, Section 1], Dempwolff determined the symmetric designs \mathcal{D} which admit $G \leq \text{Aut}(\mathcal{D})$ such that G has a socle and is a primitive rank-3 group on points and on blocks.

In this thesis we shall be concerned mostly with self-dual symmetric $1-(v, k, k)$ designs. In Theorem 5.2.1 we give a method to construct such designs. These designs will result from the primitive permutation representations of groups. In particular we are concerned with the primitive permutation representations of finite simple groups.

3.3 Graphs

In this section we shall be concerned with the relationship between permutation groups, graphs and designs. The theory of designs concerns itself with questions about subsets of a set (or relations between two sets) possessing a high degree of regularity. By contrast graph theory is mainly concerned with questions about

general relations on a set. The generality usually means that either the questions asked are too particular, or the results obtained are not powerful enough, to have useful consequences for design theory. There are instances where the two theories have interacted fruitfully. The unifying theme is provided by a class of graphs called strongly regular graphs, whose definition reflects the symmetry inherent in t -designs.

Definition 3.3.1 A graph $\Gamma = (V, E)$, consists of a finite set of vertices V together with a set of edges E , where an edge is a subset of the vertex set of cardinality 2.

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

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

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

Definition 3.3.2 A **strongly regular graph** with parameters (n, k, λ, μ) is a graph Γ with n vertices, not complete or null, in which the number of common neighbours of x and y is k , λ or μ according as x and y are equal, adjacent or non-adjacent respectively.

Remark 3.3.3 Notice that the complement of a strongly regular graph is strongly regular.

Definition 3.3.4 Let Γ be a graph with vertex set $\{x_1, x_2, \dots, x_n\}$. The **adjacency matrix** $A(\Gamma) = (a_{ij})$ of Γ is the $n \times n$ matrix given by

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

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

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

The line graph of K_n is the **triangular graph** $T(n)$, and it is strongly regular with parameters $(\frac{n(n-1)}{2}, 2(n-2), n-2, 4)$. The automorphism group of the triangular graph $T(n)$ for $n > 4$ is the symmetric group S_n . This follows by a Theorem of Whitney [94], which states that if Γ is a connected graph with more than 4 vertices, then $\text{Aut}(L(\Gamma)) = \text{Aut}(\Gamma)$. Now $T(n) = L(K_n)$ implies $\text{Aut}(T(n)) = S_n$ for all $n > 4$.

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

O_1 and O_2 are orbitals implies that the number of common neighbours of two adjacent vertices, or two non-adjacent vertices, is constant; and the transitivity of G shows that Γ is regular. So Γ is a rank-3 strongly regular graph.

Sporadic simple groups are often related with strongly regular graphs. For example, there is a strongly regular graph with parameters $(162, 105, 81)$ and the MacLaughlin group of order 898, 128, 000 is a subgroup of index 2 of the automorphism group of this graph. Similarly there is a strongly regular graph with parameters $(416, 100, 96)$ and the Suzuki group of order 448, 345, 497, 600 is a subgroup of index 2 of the automorphism group of this graph. For a survey on strongly regular graphs and rank-3 groups the reader is encouraged to consult [14, 15, 10].

The code formed by the span of the adjacency matrix of a graph Γ is also the code of the $1-(v, k, k)$ design obtained by taking the rows of the adjacency matrix as the incidence vectors of the blocks; the automorphism group of this design will contain the automorphism group of the graph. Thus a relation is established between graphs, designs, codes and groups. The interplay between these structures will be more clear in Chapter 4, where these relations undergo a considerable development and are explicitly defined. In Chapters 7, 8 and 9 we construct codes from the adjacency matrices of the graphs defined therein and an interplay between codes and graphs is established.

3.4 Finite geometries

We give a brief introduction to projective and affine geometries. The reader is encouraged to consult any standard text in this area for a more complete discussion: see for example [3] or [9].

3.4.1 Projective geometries

Let V be a vector space over the field \mathbb{F} . The **projective geometry** (space) defined by V is denoted by $PG(V)$. If the vector space V has dimension m over \mathbb{F} , then the projective geometry $PG(V)$ has **projective dimension** $m - 1$; $PG(V)$ is also denoted by $\mathcal{P}(V) = PG_{m-1}(\mathbb{F})$. The elements of $PG_{m-1}(\mathbb{F})$ are non-trivial subspaces of V , and the structure of the set is given by set-theoretical containment. The projective dimension of an element U in $PG_{m-1}(\mathbb{F})$ is denoted by $pdim(U)$ and is defined to be one less than the dimension of U as a vector space over \mathbb{F} . Thus the **points** of $PG(V)$ are the 1-dimensional subspaces of V , the **lines** are the 2-dimensional subspaces of V , and the **hyperplanes** are the $(m - 1)$ -dimensional subspaces of V .

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

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

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

$$pdim(U) + pdim(W) - pdim(U \cap W) = pdim(U + W). \quad (3.4)$$

If H is a hyperplane of $PG(V)$ and U is an element of $PG(V)$ with $pdim(U) = t$, then from the identity 3.4 we get that $pdim(H \cap U) = t$ or $t - 1$, and the former occurs if and only if $U \subseteq H$.

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

$$N_{m,k}(q) = \frac{(q^m - 1)(q^m - q) \dots (q^m - q^{k-1})}{(q^k - 1)(q^k - q) \dots (q^k - q^{k-1})}. \quad (3.5)$$

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

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

$$\frac{(q^m - q^r)(q^m - q^{r+1}) \dots (q^m - q^{k-1})}{(q^k - q^r)(q^k - q^{r+1}) \dots (q^k - q^{k-1})}. \quad (3.6)$$

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

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

Theorem 3.4.1 (Fundamental Theorem of Projective Geometry) *The full automorphism group of $PG_{m-1}(\mathbb{F}_q)$ is $PGL_m(q)$ for any $q \geq 2$ and $m \geq 3$.*

Proof: See [8]. ■

The elements of $PGL_m(q)$ preserve the subspaces of $V = \mathbb{F}_q^m$, and thus they form a permutation group on the points of $PG_{m-1}(V)$. We may construct within this group an automorphism α of order $\frac{q^m - 1}{q - 1}$ that permutes the points of the geometry in a single cycle of this length, called a **Singer cycle**, see [9, Theorem 6.2]. The group generated by a Singer cycle is called a **Singer group**.

3.4.2 Affine geometries

Definition 3.4.2 An **affine geometry** (space) of an m -dimensional space V over a field \mathbb{F} consists of all cosets $x + U$ where U is a subspace of V and x is an element of V , and is denoted by $AG(V)$ or $AG_m(\mathbb{F})$.

The dimension of the geometry is the same as the dimension of the vector space and **affine dimension** of an element $x + U$ in $AG(V)$ is the dimension of U as a subspace of V . The points of this space are all the vectors of V , the lines are the cosets of the 1-dimensional subspaces of V , and the hyperplanes are the cosets of the $(m-1)$ -dimensional subspaces of V . If a subspace U has dimension r , then any coset of U is called an **r -flat** of $AG(V)$. Two r -flats $x + U$ and $y + W$ in $AG(V)$ are **parallel** if $U = W$. The number of r -flats in $AG_m(F_q)$, where $0 \leq r \leq m$, is

$$\overline{N}_{m,r}(q) = \frac{q^{m-r}(q^m - 1)(q^{m-1} - 1) \dots (q^{m-r+1} - 1)}{(q^r - 1)(q^{r-1} - 1) \dots (q - 1)}. \quad (3.7)$$

Theorem 3.4.3 (Fundamental Theorem of Affine Geometry) *The full automorphism group of $AG_m(\mathbb{F}_q)$, where $m \geq 2$ and $q \geq 2$, is the affine semilinear group $A\Gamma L_m(q)$.*

Proof: See [9]

■

The affine semilinear group $A\Gamma L_m(q)$ preserves the cosets of V and thus acts as a permutation group on all the points of $AG_m(\mathbb{F}_q)$.

For both projective and affine geometries, the full automorphism groups are doubly transitive on the points. This will be of use later in the construction of designs from the geometries $PG_m(\mathbb{F}_q)$ and $AG_m(\mathbb{F}_q)$ where $m \geq 2$.

3.5 Decoding schemes

Codes have been used with great efficiency in some important applications. In [62] Key, gives a survey of some of the codes used in technical applications by showing how they could be constructed and where they are used. We list some of the successful applications that codes have enjoyed.

- Computer memories: the codes used are the extended binary Hamming codes, which are perfect single error-correcting-codes.
- Photographs from spacecraft: the codes used initially were the first order Reed-Muller codes, these can be constructed as the dual of the extended Hamming codes; later the binary extended Golay codes were used.
- Compact discs: codes used here are the Reed-Solomon codes, constructed using certain finite fields of large prime-power order.

Perhaps the most immediate application of codes is that which relates them with the encoding and decoding of “messages”, as we will see next.

Our primary interest is the capability of a code that is constructed from a design. We will assume that a **symmetric q -ary channel** is used, where each symbol in the alphabet of the code has the same probability of being transmitted erroneously and has the same probability to occur when an error has been made. We will describe the techniques of **syndrome decoding** and **majority logic decoding**. These methods are often used in decoding projective geometry codes. Subsequently we will describe the method of **permutation decoding** by obtaining the so-called PD-sets. In particular we shall be more concerned with the permutation decoding and in Chapter 10 we give PD-sets obtained through computations as well as explicitly.

The following result establishes the exact measurement of the error-detection and error-correction capability of a code assuming the use of a symmetric channel. The proof can be found in any standard text in coding theory: see for example [3, Chapter 2].

Theorem 3.5.1 *Let C be a code with minimum distance d . Then C can detect $d - 1$ errors or correct $\lfloor \frac{d-1}{2} \rfloor$ errors.*

Proof: See [3]. ■

3.5.1 Nearest neighbour decoding

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

3.5.2 Majority logic decoding

The majority decoding schemes are useful in decoding several families of codes: see ([86, 35, 34]). We describe the one-step majority logic decoding algorithm. In

[25, Section 3.3], Clark shows that this algorithm is an effective decoding scheme for binary codes of the projective planes. Multi-step majority decoding can be implemented with codes of designs from geometries: see [86].

Definition 3.5.2 *A set of $1 \times n$ vectors $\{v_1, v_2, \dots, v_r\}$ is said to be **orthogonal at position i** if the vectors form an $r \times n$ matrix with all entries in the i^{th} column equal to 1, and every column has either all zeros or exactly one 1 and $r - 1$ zeros.*

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

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

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

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

use this capability as long as $r \geq \lfloor \frac{d-1}{2} \rfloor$, that is $r \geq \frac{d-1}{2}$ if d is odd and $r \geq \frac{d-2}{2}$ if d is even.

3.5.3 Permutation decoding

Permutation decoding was first developed by MacWilliams [79]. It involves finding a set of permutations that preserve a code, called a PD-set. The method is described fully in MacWilliams and Sloane [80, Chapter 16] and, more recently, in Huffman [53, Section 8]. In this section we will give a brief, but complete, description of the method and in Chapter 10 we make extensive use of this method, and discuss some recent results. In particular we will look at codes defined by designs or graphs, where the automorphism group is known and large.

Definition 3.5.3 *A PD-set for a code is a set \mathcal{S} of automorphisms of the code which is such that, if the code can correct t errors, then every possible error vector of weight t or less can be moved by some member of \mathcal{S} out of the information positions.*

That such a set will fully use the error-correction potential of the code follows from Theorem 3.5.4 quoted below. That such a set exists at all is clearly not always true. There is a bound on the minimum size that the set \mathcal{S} may have, and we will quote the relevant result in Theorem 3.5.5. Using this algorithm, in Chapter 10, we obtain both computational and explicit permutation decoding sets for some codes from permutation primitive representations of some simple groups as well as codes obtained from the triangular graph $T(n)$ and the codes from graphs on triples. In particular explicit permutation decoding sets for the binary codes of the triangular graphs and the codes from graphs on triples are found.

Theorem 3.5.4 [53] *Let C be an $[n, k, d]_q$ t -error-correcting code. Suppose \bar{G} is a check matrix for C in standard form, that is such that I_{n-k} is in the redundancy*

positions. Let $y = c + e$ be a vector, where $c \in C$ and e has weight less than or equal to t . Then the information symbols in y are correct if and only if the weight of the syndrome of y is less than or equal to t .

Proof: Suppose C has generator matrix \mathcal{G} in standard form, that is $\mathcal{G} = [I_k \mid A]$ and that the encoding is done using \mathcal{G} , that is the data set $x = (x_1, \dots, x_k)$ is encoded as $x\mathcal{G}$. The information symbols are then the first k symbols, and the check matrix $\bar{\mathcal{G}}$ is $\bar{\mathcal{G}} = [-A^T \mid I_{n-k}]$. Suppose the information symbols of y are correct. Then $\bar{\mathcal{G}}y^T = \bar{\mathcal{G}}e^T = e^T$, and thus $\text{wt}(\bar{\mathcal{G}}y^T) \leq t$.

Conversely, suppose that not all the information symbols are correct. Then if $e = e_1 \dots e_n$, and $e' = e_1 \dots e_k, e'' = e_{k+1} \dots e_n$, we assume that e' is not the zero vector. Now use the fact that for any vectors $\text{wt}(x + y) \geq \text{wt}(x) - \text{wt}(y)$. Then

$$\begin{aligned} \text{wt}(\bar{\mathcal{G}}y^T) &= \text{wt}(\bar{\mathcal{G}}e^T) = \text{wt}(-A^T e'^T + e''^T) \\ &\geq \text{wt}(-A^T e'^T) - \text{wt}(e''^T) \\ &= \text{wt}(e'A) - \text{wt}(e'') \\ &= \text{wt}(e'A) + \text{wt}(e') - \text{wt}(e') - \text{wt}(e'') \\ &= \text{wt}(e'\mathcal{G}) - \text{wt}(e) \geq d - t \geq t + 1, \end{aligned}$$

since $d \geq 2t + 1$ by Theorem 3.5.1. Hence the result. ■

The algorithm for permutation decoding then is as follows: we have a t -error-correcting $[n, k, d]_q$ code C with check matrix $\bar{\mathcal{G}}$ in standard form. Thus the generator matrix \mathcal{G} for C that is used for encoding has I_k as the first k columns, and hence as the information symbols. Any k -tuple v is encoded as $v\mathcal{G}$. Suppose x is sent and y is received and at most t errors occur. Let $\mathcal{S} = \{g_1, \dots, g_s\}$ be the PD-set. Compute the syndromes $\bar{\mathcal{G}}(yg_i)^T$ for $i = 1, \dots, s$ until an i is found such that the weight of this vector is t or less. Now look at the information symbols in this vector, and obtain the codeword c that has these information symbols (see [79]). Now decode y as cg_i^{-1} . Note that this is valid since permutations of

the coordinate positions correspond to linear transformations of \mathbb{F}_q^n , so that if $y = x + e$, where $x \in C$, then $yg = xg + eg$ for any $g \in S_n$, and if $g \in \text{Aut}(C)$, then $xg \in C$.

The following result which can be found in [53] and originally from Gordon [46] establishes a bound for the minimum size a PD-set can have:

Theorem 3.5.5 *If \mathcal{S} is a PD-set for a t -error-correcting $[n, k, d]_q$ code C , and $r = n - k$, then*

$$|\mathcal{S}| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil.$$

In Gordon [46] and Wolfman [96], small PD-sets for the binary Golay codes were found. In Chabanne [24] abelian codes, that is ideals in the group algebra of an abelian group, are looked at using Groebner bases, and the ideas of permutation decoding are generalized. Note that PD-sets need not be sought, in general, for codes with minimum weight 3 or 4, since correcting a single error is in fact simply done by using syndrome decoding, because in that case multiples of the columns of the check matrix will give the possible syndromes. Thus the syndrome of the received vector need only be compared with the columns of the check matrix, by looking for a multiple.

In general it is rather hard to find these PD-sets, and they need not even exist. However, if C is a single-error-correcting code, it is somewhat easier to find such sets. In fact we use the following observation which we state as a lemma:

Lemma 3.5.6 *Suppose C is a $[n, k, d]_q$ t -error-correcting code, and let $r = n - k$. Let \mathcal{T} denote the set of t -tuples of elements of $\{1, 2, \dots, n\}$ and \mathcal{E} be set of t -tuples of elements of the check positions $\{k+1, k+2, \dots, n\}$. Then a set $\mathcal{S} = \{g_1, \dots, g_s\}$ of automorphisms will be a PD-set for C if*

$$\bigcup_{g \in \mathcal{S}} \mathcal{E}^{g^{-1}} = \mathcal{T}.$$

Furthermore, for any $g \in \text{Aut}(C)$ the set $gS = \{gg_1, \dots, gg_s\}$ will also be a PD-set.

Proof: Let $\beta \in \mathcal{T}$. Then $\beta \in \bigcup_{g \in \mathcal{S}} \mathcal{E}^{g^{-1}}$. Hence there exists $g_i \in \mathcal{S}$ such that $\beta = \mathcal{E}^{g_i^{-1}}$, so that $\beta^{g_i} \in \mathcal{E}$. For the second statement we proceed as follows: we need to show that any t -tuple $\beta \in \mathcal{T}$ satisfies $\beta = \alpha^{e^{-1}}$ for some $\alpha \in \mathcal{E}$ and $e \in gS$. If $\beta^g = \gamma = \alpha^{h^{-1}}$ for some $\alpha \in \mathcal{E}$ and $h \in \mathcal{S}$, then $\beta = \alpha^{h^{-1}g^{-1}} = \alpha^{(gh)^{-1}}$, as required. ■

MacWilliams [79] developed a theory for finding PD-sets for cyclic codes. A $[n, k, d]_q$ code C is said to be **cyclic** if whenever $c = c_1c_2 \dots c_n \in C$ then every cyclic shift of c is in C . Thus the mapping $\tau \in S_n$ defined by $\tau : i \mapsto i + 1$ for $i \in \{1, 2, \dots, n\}$, is in the automorphism group of C , and $\tau^n = 1$. If a message c is sent and t errors occur, then if e is the error vector and if there is a sequence of k zeros between two of the error positions, then τ^j for some j will move the sequence of zeros into the information positions, and thus all the errors will occur in the check positions. Thus $\langle \tau \rangle$ will be a PD-set for C if $k < \frac{n}{t}$.

As shown in [79], if q is a number prime to the length n , then the map $\rho : i \mapsto qi$ is also an automorphism of the cyclic code and it is in the normalizer N of $\langle \tau \rangle$. MacWilliams examines the cases where N contains a PD-set.

As an illustration of this ideas of MacWilliams we give in Chapter 10 a PD-set for the $[15, 4, 8]_2$ code obtained through computations with Magma [11] from a primitive permutation representation of the simple alternating group A_6 . In fact this code is the dual code of the well known Hamming code of length 15. Since this code is in fact a cyclic code, a PD-set for it was found in a Singer group.

For small t , PD-sets can be found computationally. Using Magma we have designed a programme (see Appendix C) which could be used to determine the PD-sets with small t , and $t \leq 7$. A list of these codes and corresponding PD-sets can be found at the website:

<http://www.ces.clemson.edu/~keyj>

under the list of PD-sets.

In [60] Key found computationally some PD-sets for single-error-correcting codes of the Hermitian and Ree unitals on 28 points.

Other instances of PD-sets found through computations are given in [53], (see for example Huffman [53, Example 8.3]), where a PD-set of 14 elements for the $[27, 12, 8]_2$ extended binary Golay code is given.

Chapter 4

Codes from Combinatorial Structures

As a mathematical theory, coding theory is relatively young, with its roots in Shannon's [88] seminal paper in 1948. The practical gains, due to coding, demonstrated there, and elsewhere since, have provided motivation for much of coding theory. It is fascinating how a large mathematical theory was and is continuing to be developed. The mathematical areas needed in classical coding have been mainly algebraic. However through time, subsequent developments have expanded this mathematical theory considerably. A frequent question in coding theory is "how one constructs a code, or structure related to a code, that is optimal in some mathematical or applied sense". In this chapter we relate some ways in which codes have been constructed.

4.1 Codes from designs

Coding theory has made many contributions to the theory of combinatorial designs. A code generated by the incidence matrix of designs has been useful

in either constructing new designs or showing that certain designs do not exist, as it is for example the case of the projective plane of order 10. Coding theory has also been used to extend designs. In [59] Kennedy and Pless extended designs “held” by vectors of a code. The connection between designs and codes leads to the construction of new designs. Using the knowledge about codes and the existence of designs in codes can be useful for decoding purposes. For example a binary vector x of weight w is said to determine the block of w points corresponding to the positions where x has non-zero coordinates. In such case we say that vectors of a fixed weight w in a binary code of length n hold a t -design if the blocks determined by these vectors are the blocks of a t -design on n points. This means that there must exist t and λ so that every set of t coordinate positions occurs as non-zero positions for exactly λ vectors of weight w . The knowledge of the number of vectors of each weight existing in a code is crucial in determining whether or not the supports of these vectors could form a design. For $q = 2$ the supports are in a one-to-one correspondence with the codewords. The celebrated Assmus-Mattson Theorem ([3, Theorem 2.11.2]) establishes the connection between designs and codes, in that vectors of certain weight in a q -ary code hold a design, and we can determine the number of vectors of such weight. Clearly the knowledge of the number of vectors of each weight existing in a code is crucial in determining whether or not the supports of these vectors could form a design. Notice that if S is the support of a vector in a code over \mathbb{F}_q then it is the support of at least $q - 1$ such vectors, in fact precisely $q - 1$ vectors if the minimum weight of the code is $|S|$. For $q = 2$ the supports are in a one-to-one correspondence with the codewords. Once again the Assmus-Mattson Theorem gives conditions on the weight enumerators of a code and its dual that are sufficient to ensure that the support of the minimum weight vectors (and other weights also) yield a t -design where t is a positive integer less than the minimum weight.

For a general incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ and any field \mathbb{F} , we denote the

vector space of functions from \mathcal{P} to \mathbb{F} by $\mathbb{F}^{\mathcal{P}}$. For $w \in \mathbb{F}^{\mathcal{P}}$, the value of w at the point p is $w(p)$ in \mathbb{F} .

Definition 4.1.1 *The **support set** of a function w in $\mathbb{F}^{\mathcal{P}}$ is defined to be the subset of points in \mathcal{P} whose images under w are non-zero, that is, $\text{Supp}(w) = \{p \in \mathcal{P} \mid w(p) \neq 0\}$. The **characteristic function** for a block B is denoted by v^B and defined to be*

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

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

Definition 4.1.2 *A q -ary code of a design $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is the subspace of the function space $\mathbb{F}_q^{\mathcal{P}}$ generated by the characteristic functions of the blocks of \mathcal{D} and is denoted by $C_q(\mathcal{D})$.*

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

In general the minimum weight is less than the block size of \mathcal{D} , but for the p -ary codes of geometry designs, where p is the characteristic of the underlying field of the geometry, we have equality by the work of Delsarte et al: see [36] and [25, Section 6.1].

The following Lemma which can be found in [66] is an important result on the automorphism group of codes obtained from incidence structures.

Lemma 4.1.3 *Let C be the linear code of length n of an incidence structure \mathcal{I} over a field \mathbb{F} . Then the automorphism group of C is the full symmetric group if and only if $C = \mathbb{F}^n$ or $C = \mathbb{F}_{\mathcal{J}^\perp}$.*

Proof: Suppose $\text{Aut}(C)$ is S_n . C is spanned by the incidence vectors of the blocks of \mathcal{I} . Let B be such a block and suppose it has k points, and so it gives a vector of weight k in C . Clearly C contains all the incidence vector of any set of k points, and thus we see that C contains all the vectors of weight 2 having as non-zero entries 1 and -1 . Thus $C = \mathbb{F}_2^\perp$ or \mathbb{F}^n . The converse is clear. ■

4.2 Codes from graphs

In [29] Curtis showed how the binary Golay code can be obtained in a revealing way straight from the edge-graph of the icosahedron. This construction not only yields a natural basis for the code, but also supplies a simple description of all codewords. It is also shown that the above is merely a special case of a general method of constructing codes from graphs. Codes with certain properties, such as self-duality, are obtained by putting certain conditions on the starting graph. In [30] Curtis and Morris outlined a construction of codes from adjacency matrices of graphs which we briefly describe as follows: let Γ to be a graph without multiple edges (but possibly with loops) and vertex set $\Omega = \{1, 2, \dots, n\}$ and $A(\Gamma) = A = (\gamma_{ij})$ its adjacency matrix and further consider $V(\Omega)$ the n -dimensional vector space over \mathbb{F}_2 with basis the set $B = \{v_i \mid i \in \Omega\}$. Then A is the matrix of a linear transformation from V into itself with respect to the basis B . Now identify each vector in V with the subset of the vertices of Γ to which it corresponds. Further, consider the eigenspaces of $V^{(\lambda)}$ of A , where $\lambda \in \mathbb{F}_2$ and $V^{(0)}$ consisting of those set of vertices X for which any vertex of Γ is adjacent to an even number of vertices in X , and $V^{(1)}$ consists of those sets X for which every vertex not in X is adjacent to an even number of vertices in X and every vertex in X is joined to an odd number of vertices in X . Define a bipartite graph $\hat{\Gamma}$ with twice as many vertices as Γ , as follows:

- (1) the vertices are $1, 2, \dots, n, \bar{1}, \bar{2}, \dots, \bar{n}$;

(2) i is joined to \bar{j} if and only if i is adjacent to j in Γ , and these are the only adjacencies. Now \hat{A} the adjacency matrix of $\hat{\Gamma}$ has the form

$$\hat{A} = \begin{pmatrix} 0 & A \\ A & 0 \end{pmatrix}$$

and the codes are constructed from the adjacency matrix \hat{A} .

However, the only codes considered by Curtis and Morris are the eigenspaces of \hat{A} for the eigenvalue 1.

The codes constructed in this thesis follow a much simpler construction which we outline as follows: let $\Omega = \{1, 2, \dots, n\}$ and we define graphs Γ whose vertices are the k element subsets ($k > 1$) of Ω and adjacency is defined according to whether these subsets meet or are disjoint. The binary codes of the graph Γ are formed by the span of the adjacency matrix of Γ . It turns out that the code is also the code of the $1-(v, k, k)$ design obtained by taking the rows of the adjacency matrix as the incidence vectors of the blocks; the automorphism group of this design will contain the automorphism group of the graph.

For example for any n , the triangular graph $T(n)$ is the graph whose vertices are the 2-element subsets of a set of cardinality n in which two distinct vertices are adjacent if and only if they are not disjoint. It is a strongly regular graph on the $\binom{n}{2}$ vertices that is, on the pairs of letters $\{i, j\}$ where $i, j \in \{1, \dots, n\}$ and the binary codes of these graphs are studied in detail in Chapter 8.

Similarly, given a set Ω of size n and $\Omega^{\{3\}}$ the set of subsets of Ω of size 3, we examine the binary codes obtained from the adjacency matrix of each of the three graphs with vertex set $\Omega^{\{3\}}$, with adjacency defined by two vertices as 3-sets being adjacent if they have zero, one or two elements in common, respectively. In Chapter 9 we investigate the binary codes of these graphs as well as establish some of their properties.

For the construction of the graphs on triples and their codes we designed

a Magma programme which we outline in the Appendix G. Using this programme with necessary changes the triangular graph $T(n)$ and its code could be constructed.

4.3 Codes from geometries

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

Proposition 4.3.1 [61] *$PG_{m,r}(\mathbb{F}_q)$ is a $2-(v, k, \lambda)$ design with*

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

$AG_{m,r}(\mathbb{F}_q)$ is a $2-(v, k, \lambda)$ design with

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

The codes over \mathbb{F}_p of any of the designs defined by a projective or affine geometry over a field of characteristic p are some form of generalized Reed-Muller

code, that is possibly a so-called subfield code or a non-primitive sub-field code. This fact follows from the work of Delsarte [31] and Delsarte and MacWilliams [36]. The full results are described in [3, Chapter 5] and [4, Chapter 5]. If x is any number and $x = \sum_i x_i q^i$ where $0 \leq x_i \leq q - 1$, then the q -weight of x is defined to be $\text{wt}(q) = \sum_i x_i$. In the following theorems which could be found in [61] these codes are described:

Theorem 4.3.2 [61] *The code over \mathbb{F}_p of the projective geometry design $PG_{m,r}(\mathbb{F}_q)$, where $q = p^t$ and p is a prime, and $0 < r < m$, is the (non-primitive subfield code) generalized Reed-Muller code $C = \mathcal{R}_{\mathbb{F}_q/\mathbb{F}_p}^{q-1}((m-r)(q-1), m+1)$. It has minimum weight $\frac{q^{r+1}-1}{q-1}$ and the minimum weight vectors are the multiples of the incidence vectors of the blocks.*

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

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

There is a similar theorem for the affine geometry designs:

Theorem 4.3.3 [61] *The code over \mathbb{F}_p of the affine geometry design $AG_{m,r}(\mathbb{F}_q)$, where $q = p^t$ and p is a prime, and $0 < r < m$, is the (subfield code) generalized Reed-Muller code $C = \mathcal{R}_{\mathbb{F}_q/\mathbb{F}_p}((m-r)(q-1), m)$. It has minimum weight q^r and the minimum weight vectors are the multiples of the incidence vectors of the r -flats.*

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

The dual code C^\perp contains the code

$$\mathcal{R}_{\mathbb{F}_q/\mathbb{F}_p}(r(q-1)-1, m) = \langle v^M - v^N \mid M, N \text{ parallel } (m-r) - \text{flats in } V \rangle$$

which has minimum weight $2q^{m-r}$ with minimum weight vectors multiples of the difference of incidence vectors of two parallel $(m-r)$ -flats. The minimum weight d^\perp of C^\perp satisfies $(q+p)q^{m-r-1} \leq d^\perp \leq 2q^{m-r}$.

When $q = p$ we have equality, that is

$$\mathcal{R}_{\mathbb{F}_q/\mathbb{F}_p}((m-r)(p-1), m)^\perp = \mathcal{R}_{\mathbb{F}_p}(r(p-1)-1, m),$$

and the lower and upper bounds for d^\perp are the same.

In general the dual codes of these codes are not generalized Reed-Muller codes; these are the so-called polynomial codes. Their minimum weight is not known in general and in [61, Section 7] some new results that deduce the minimum weight from the geometrical properties of the designs are described.

Chapter 5

Codes from Groups

5.1 Introduction

The link between combinatorial design theory, finite group theory and algebraic coding theory has proved useful to further understanding of these structures. For example, codes have helped in the characterization of designs, and design theory has provided examples of codes with effective encoding and decoding algorithms and whose minimum weights and weight distributions can be found through the combinatorial properties of the designs.

The methods employed to exploit this link include use of geometrical and combinatorial properties of the designs, and their automorphism groups. We will examine some of the successful applications of this association, and in particular look at codes obtained from primitive permutation representations of finite simple groups.

Codes obtained from permutation the representations of finite groups have been given particular attention in recent years. Given a representation of group elements of a group G by permutations we can work modulo 2 and obtain a

representation of G on a vector space V over \mathbb{F}_2 . The invariant subspaces (the subspaces of V taken into themselves by every group element) are then all the binary codes C for which G is a subgroup of $\text{Aut}(C)$. Similarly we could produce codes over fields of characteristic p , where $p > 2$. This modulo-theoretic technique has been used in [12, 13, 74]. In [74], Knapp and Schmid consider $[n, k, d]_q$ codes where the monomial automorphism group is a particular group. The groups examined were the alternating groups A_n , the symmetric groups S_n and the Mathieu groups written as permutation groups of degree n and associated with codes of length n . Important information about these codes can be obtained from the theory of modular representations of groups. Using these ideas, Calderbank and Wales in [17] construct a binary $[176, 22, 50]_2$ code whose automorphism group is the Higman-Sims (HS) group. Various arguments yield the Hoffman-Singleton graph on 50 vertices, a 2- $(176, 50, 14)$ design discovered by G. Higman, and the original rank-3 construction of HS .

Brooke in [12, 13] has found all codes obtainable this way from the primitive permutation representations of the simple groups $PSU_4(2)$ and $PSU_3(3)$. In particular are examined all binary codes arising from primitive permutation representations of these groups. The simple group $PSU_4(2)$ of order 25920 has an especially rich structure. It is the simple constituent of the groups $Sp_4(3)$, $U_4(2)$, $O_6^-(2)$, $O_5(3)$, and of $W(E_6)$, the Weyl group of type E_6 . In [12], representations of $PSU_4(2)$ on the 27 lines of the general cubic surface, on the root system of type E_6 as well as some complex 4- and 5-dimensional representations are described. These are used to construct the five primitive permutation representations of degrees 27, 36, 40, 40 and 45. These representations lead to 6, 10, 6, 10 and 22 codes respectively (excluding the zero code and the ambient space). These codes are all inequivalent except for the repetition code (\mathbb{F}_2) and its dual which appear in both representations of degree 40. The group $PSU_3(3)$ has order 6040 and has four permutation representations of degrees 28, 36, 63 and 63 leading

to 4, 10, 26 and 42 codes, respectively, all of which are inequivalent except for the repetition code and its dual appearing in both degree 63 representations. A detailed description of the corresponding modular representations over the field with two elements is presented. In each case the complete lattice of submodules is given. Irreducible modules of degrees 1, 6, 8, and 14 are involved. Further the weight distribution of subcodes (that is, submodules) with respect to the standard basis is determined.

Taking G to be a permutation group of degree n , and V the corresponding \mathbb{F}_2 permutation module. The submodules of V can be regarded as being G -invariant binary linear codes in V , and one may therefore ask for the weight distribution of these codes. In [13] a search is carried out when (G, V) corresponds to one of the four primitive permutation modules associated with the simple unitary group $G = U_3(3)$, of order 6048. The approach is to regard G as acting 2-transitively on a certain Steiner system $S(2, 4, 28)$, and then to obtain the other primitive representations of G in terms of the action of $U_3(3)$ on various geometric and algebraic objects that live in $S(2, 4, 28)$. Of particular interest is the description of $S(2, 4, 28)$ in terms of the Cayley integers and therefore provide an explicit isomorphism between $U_3(3)$ and $G'_2(2)$.

In [49] a $[276, 23, 100]_2$ self-orthogonal doubly-even code left invariant by the Conway simple group Co_3 was constructed. Its residual code with respect to a minimum weight codeword is the $[176, 22, 50]_2$ code left invariant by the Higman-Sims simple group HS referred to above and constructed in [17]. For a collected list of references and more details on codes from permutation representations, the reader is encouraged to consult [28] and [53, Section 7.4].

5.2 Codes from primitive groups

In this thesis, following the construction method outlined in [66, Proposition 1] we construct designs, graphs and codes from primitive permutation representations of some finite simple groups. Our construction differ from the ones outlined above in that we are particularly concerned with graphs and self-dual symmetric $1 - (v, k, k)$ designs. It is easy to describe the coverage of this thesis by first referring to the present section, in which this perspective first emerges and undergoes considerable development. We have developed some programmes in Magma (see Appendix A) which were determinant in establishing the results concerning designs and their codes. In this regard the results described in this thesis are theoretical generalizations of the computations carried out. We have essentially based the constructions of the designs in a standard method developed by Key and Moor [66, Proposition 1] given below as Theorem 5.2.1. This theorem could be regarded as a generalization of Theorem 3.2.10 in that incorporates the study of 1-designs and graphs.

Theorem 5.2.1 [66] *Let G be a finite primitive permutation group acting on the set Ω of size n . Let $\alpha \in \Omega$, and let $\Delta \neq \{\alpha\}$ be an orbit of the stabilizer G_α of α . If*

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

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

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

then B forms a self-dual $1-(n, |\Delta|, |\Delta|)$ design with n blocks, and \mathcal{E} forms the edge set of a regular connected graph of valency $|\Delta|$, with G acting as an automorphism group on each of these structures, primitive on vertices of the graph, and on points and blocks of the design.

Proof: It follows immediately from Theorem 2.2.2 that $|G| = |\Delta^G||G_\Delta|$, and clearly $G_\Delta \geq G_\alpha$. Since G is primitive on Ω , G_α is maximal in G , and thus $G_\Delta = G_\alpha$, and $|\Delta^G| = |\mathcal{B}| = n$. Thus a $1-(n, |\Delta|, |\Delta|)$ design is formed.

For the graph notice that the vertices adjacent to α are the vertices in Δ . Now as these pairs are orbited under G , nk ordered pairs are formed, and thus $nk/2$ edges, where $k = |\Delta|$. Since the graph has G acting, it is clearly regular, and thus the valency is k as required, that is, the only vertices adjacent to α are those in the orbit Δ . The graph must be connected, as a maximal connected component will form a block of imprimitivity, contradicting the group's primitive action.

Now notice that an adjacency matrix for the graph is simply an incidence matrix for the 1-design, so that the 1-design is necessarily self-dual. This proves all assertions. ■

Remark 5.2.2 Notice that by forming any union S , where $\{\alpha\} \neq S \neq \Omega$, of orbits of the stabilizer of a point, including the orbit consisting of the single point, and orbit this under the full group, the design obtained is still a self-dual symmetric 1-design with the group operating.

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

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

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

Lemma 5.2.3 *If the group G acts primitively on the points and the blocks of a symmetric 1-design \mathcal{D} , then the design can be obtained by orbiting a union of orbits of a point-stabilizer, as described in Theorem 5.2.1.*

Proof: Suppose that G acts primitively on points and blocks of the $1-(v, k, k)$ design \mathcal{D} . Let \mathcal{B} be the block set of \mathcal{D} ; then if B is any block of \mathcal{D} , $\mathcal{B} = B^G$. Thus $|G| = |\mathcal{B}||G_B|$, and since G is primitive, G_B is maximal and thus $G_B = G_\alpha$ for some point. Thus G_α fixes B , so this must be a union of orbits of G_α . ■

Remark 5.2.4 If G is simple, then the maximality of the point stabilizer, implies that there is only one orbit of length 1.

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

The following two theorems deal with the automorphism groups of the designs and codes constructed from a finite primitive permutation group in a manner described in Theorem 5.2.1.

Theorem 5.2.5 *Let \mathcal{D} be a self-dual 1-design obtained by taking all the images under G of a non-trivial orbit Δ of the point stabilizer in any of G 's primitive representations, and on which G acts primitively on points and blocks, then the automorphism group of \mathcal{D} contains G .*

Proof: Suppose that G acts primitively on $\Omega = G/G_\alpha$. Primitivity of G implies that G_α is a maximal subgroup. Let $\mathcal{B} = \{\Delta^g : g \in G\}$ and suppose that $B = \Delta^g$, and $B' = \Delta^{g'}$. Then we have that $(\Delta^g)^{g^{-1}g'} = \Delta^{gg^{-1}g'} = \Delta^{g'}$, and so G acts transitively on \mathcal{B} . Now, if $h \in G$ and $\alpha \in \Delta^g$ then $\alpha^h \in (\Delta^g)^h$. Hence, we have that $\alpha^h \in \Delta^{gh}$ and therefore $G \subseteq \text{Aut}(\mathcal{D})$. ■

Theorem 5.2.6 *If C is a linear code of length n of a symmetric $1 - (v, k, k)$ design \mathcal{D} over a finite field \mathbb{F}_q , then the automorphism group of \mathcal{D} is contained in the automorphism group of C .*

Proof: Suppose that \mathcal{D} is a $1 - (v, k, k)$ design with $\mathcal{P} = \{p_1, p_2, \dots, p_v\}$ the point set of \mathcal{D} and $\mathcal{B} = \{B_1, B_2, \dots, B_v\}$ the block set. Let A be an incidence matrix for \mathcal{D} , then \mathcal{P} determines uniquely the rows of A , since each point is incident with precisely k blocks. If $\alpha \in \text{Aut}(\mathcal{D})$, then α sends p_i to p_j for $1 \leq i, j \leq v$ and $B_{i'}$ to $B_{j'}$ where $1 \leq i', j' \leq v$, and α preserves the incidence relation. Now if C is a code from \mathcal{D} , then we have that the columns of A span C . Let R_i and R_j denote the i -th and j -th columns of A respectively, with the entries of R_i and R_j labelled as the blocks indices. Then R_i and R_j have each exactly k non-zero entries, since they represent the incidence relation of a point with the corresponding k blocks of \mathcal{D} . Now the self-duality of \mathcal{D} implies that R_i and R_j are weight k vectors in C . Now since α permutes the coordinate positions of the k non-zero entries of R_i to R_j , we deduce that α is an automorphism of C . ■

5.3 Codes from the Janko groups J_1 and J_2

As a particular example of application of the construction method outlined in Theorem 5.2.1, in this section we describe the work of Key and Moori [66]. By considering the primitive representations of the simple Janko groups J_1 and J_2 , as described in the ATLAS [27], in [66], Key and Moori using Magma [11], have constructed designs and graphs that have the group acting primitively on points as an automorphism group, and codes derived from the designs or graphs that have the group acting as an automorphism group.

Where possible by means of computations it is shown that the full automorphism group of these designs and graphs are J_1 , J_2 or \bar{J}_2 , the extension

of J_2 by its outer automorphism, and shown that for some of the codes the same is true.

Note that J_1 has no outer automorphisms, and thus is its own automorphism group, whereas J_2 has an involutory outer automorphism, so its automorphism group, which we will denote by \bar{J}_2 , is a split extension of J_2 by \mathbb{Z}_2 , with double the order.

They have looked first at J_1 , which is of order 175560, and its maximal subgroups and primitive permutation representations via the coset action on these subgroups, see [27, 44]. There are seven distinct primitive representations, of degree 266, 1045, 1463, 1540, 1596, 2926, and 4180, respectively. They have then looked at J_2 , of order 604800, which has nine primitive representations, of degree 100, 280, 315, 525, 840, 1008, 1800, 2016 and 10080, respectively.

For each of these groups, using Magma [11], the designs and graphs as described in Theorem 5.2.1 were found, and found the p -rank of the designs for some small set of values of the prime p . To aid in the classification, the dimension of the hull of the design for each of these primes were also found. Also looked for strongly regular graphs for each group, finding as a result three for J_2 .

5.3.1 The computations for J_1

For each of the seven primitive representations, the permutation group were constructed and formed the orbits of the stabilizer of a point. For each of the non-trivial orbits, the symmetric 1-design as described in Theorem 5.2.1 was formed.

There are 245 designs formed in this manner and that none of them is isomorphic to any other of the designs in this set. In every case the full automorphism group of the design or graph is J_1 . In all but 34 of the designs, the dimensions of the code or the hull over the set of primes given above distinguished the designs. For the 34 remaining, these occurred in 17 pairs in which the set of

dimensions for each pair was identical, but distinct from all the other pairs.

In Table 5.1, the first column gives the degree, the second the number of orbits, and the remaining columns give the length of the orbits of length greater than 1, with the number of that length in parenthesis behind the length in case there is more than one of that length. The pairs that had the same code dimensions

Degree	#	length				
266	4	132	110	12	11	
1045	10	168(5)	56(3)	28	8	
1463	21	120(7)	60(9)	20(2)	15(2)	12
1540	20	114(9)	57(6)	38(4)	19	
1596	18	110(13)	55(2)	22(2)	11	
2926	66	60(34)	30(27)	15(5)		
4180	106	42(95)	21(6)	14(4)	7	

Table 5.1: Orbits of the point-stabilizer of J_1

occurred as follows: for degrees 266, 1045 and 1596, there were no such pairs; for degree 1463 there were two pairs, both for orbit size 60; for degree 1540, there were two pairs, for orbit size 57 and 114 respectively; for degree 2926 there was one pair for orbit size 60; for degree 4180 there were 12 pairs, for orbit size 42.

For each one of these 245 designs (or graphs) there was at least one prime from the small set that gave an “interesting code”, that is a code that is not the full space or of codimension 1. Full details of the numbers obtained can be found at the web site:

<http://www.ces.clemson.edu/~keyj/>

under the file “Janko groups and designs”.

Proposition 5.3.1 [66] *If G is the first Janko group J_1 , there are precisely 245 non-isomorphic self-dual 1-designs obtained by taking all the images under G of the non-trivial orbits of the point stabilizer in any of G 's primitive representations, and on which G acts primitively on points and blocks. In each case the full automorphism group is J_1 . Every primitive action on symmetric 1-designs can be obtained by taking the union of such orbits and orbiting under G .*

5.3.2 The computations for J_2

This group has nine primitive representations, as already mentioned, but computations were not carried with the largest degree. Thus the results cover only the first eight. The results for J_2 are different from those for J_1 , due to the existence of an outer automorphism.

The main difference is that usually the full automorphism group of the design is \bar{J}_2 , and that in the cases where it was only J_2 , there would be another orbit of that length that would give an isomorphic design, and which, if two orbits were joined, would give a design of double the block size and automorphism group \bar{J}_2 . A similar conclusion held if some union of orbits was taken as a base block.

From these eight primitive representations, in all 51 non-isomorphic symmetric designs on which J_2 acts primitively were obtained. Table 5.2 gives the same information for J_2 that Table 5.1 gives for J_1 . The automorphism group of the design in each case was J_2 or \bar{J}_2 . Where J_2 was the full group, there is another copy of the design for another orbit of the same length. This occurred in the following cases: degree 315, orbit length 32; degree 1008, orbit lengths 60, 100 and 150; degree 1800, orbit lengths 42, 42, 84 and 168; degree 2016, orbit lengths 50, 75, 75, 150, 150, and 300. We note again that the p -ranks of the designs and their hulls gave an initial indication of possible isomorphisms and clear non-isomorphisms, so that only the few mentioned needed be tested.

Degree	#	length						
100	3	63	36					
280	4	135	108	36				
315	6	160	80	32(2)	10			
525	6	192(2)	96	32	12			
840	7	360	240	180	24	20	15	
1008	11	300	150(2)	100(2)	60(2)	50	25	12
1800	18	336	168(6)	84(3)	42(3)	28	21	14(2)
2016	18	300(2)	150(6)	75(5)	50(2)	25	15	

Table 5.2: Orbits of the point-stabilizer of J_2

Three strongly regular graphs were found: that of degree 100 from the rank-3 action, and two more of degree 280 from the orbits of length 135 and 36, giving strongly regular graphs with parameters $(280, 135, 70, 60)$ and $(280, 36, 8, 4)$ respectively. The full automorphism group is \bar{J}_2 in each case. Not all the representations were checked, but note that the representation of degree 280 is the only one with point stabilizer having exactly four orbits. Note that Bagchi [6] found a strongly regular with parameters $(280, 144, 44, 80)$ admitting \bar{J}_2 .

The computations carried out in [66] regarding the Janko groups J_1 and J_2 have been used to conjecture that the automorphism groups of the designs obtained using the construction method outlined in Theorem 5.2.1, from a primitive representation of a simple group G will have the automorphism group $\text{Aut}(G)$ as its automorphism group, unless the design is isomorphic to another one constructed in this way, in which case the automorphism group of the design will be a proper subgroup of the the $\text{Aut}(G)$ containing G .

In [66], Key and Moori have not found a code that has automorphism group bigger than J_1 or \bar{J}_2 but not equal to the full symmetric group.

Chapter 6

A conjecture of Key and Moori

6.1 Introduction

In this chapter we examine a query posed as a conjecture by Key and Moori [66, Section 7] which we have briefly described in the last part of Section 5.3, concerning the full automorphism groups of designs and codes arising from primitive permutation representations of finite simple groups, and based on results for the Janko groups J_1 and J_2 as studied in [66]. Here, following that same method of construction, we show that counter-examples to the conjecture exist amongst some representations of some alternating groups, and that the simple symplectic groups in their natural representation provide an infinite class of counter-examples.

In examining the codes and designs arising from the primitive representations of the first two Janko groups, Key and Moori in [66, Section 7] suggested that the computations made for these Janko groups could lead to the following conjecture:

Conjecture 6.1.1 (Key-Moori) *Any design \mathcal{D} obtained from a primitive permutation representation of a simple group G will have the automorphism group $\text{Aut}(G)$ as its full automorphism group, unless the design is isomorphic to another*

one constructed in the same way, in which case the automorphism group of the design will be a proper subgroup of $\text{Aut}(G)$ containing G .

Here G is naturally a subgroup of $\text{Aut}(\mathcal{D})$, and also of $\text{Aut}(G)$, since it is simple and hence isomorphic to the (normal) subgroup of inner automorphisms. How outer automorphisms of G would define elements of $\text{Aut}(\mathcal{D})$ is not clear but it did occur for those Janko groups, and in fact for most of the primitive representations; certainly the normalizer of G in $\text{Aut}(\mathcal{D})$ will be a subgroup of $\text{Aut}(G)$.

While the Conjecture 6.1.1 is true for the Janko groups J_1 and J_2 , and some other simple groups, we show here that it is not always true: we found examples of finite simple groups G with a primitive representation giving a design \mathcal{D} such that the automorphism group of G does not contain the automorphism group of \mathcal{D} . Furthermore, there are finite simple groups that have automorphisms that do not preserve the design. Specifically, we considered computationally all the primitive permutation representations of G where G is the alternating group A_6 or A_9 . Using Programme A2 (see Appendix A.2), we constructed designs that have the group G acting primitively on points and blocks, and for each prime dividing $|G|$ we constructed the codes of the designs over that prime field. Contradicting the Conjecture 6.1.1, we found for $G = A_6$ of degree 15, two isomorphic designs such that the automorphism group of the design is neither the group $\text{Aut}(A_6)$ nor a proper subgroup of $\text{Aut}(A_6)$ containing A_6 . In fact if \mathcal{D} denotes one of these designs, then $\text{Aut}(A_6) \not\leq \text{Aut}(\mathcal{D})$. Similarly for $G = A_9$ we found that the orbits of length 56 and 63 respectively for A_9 of degree 120 produce designs with the property that the automorphism group is not $\text{Aut}(A_9)$, nor a proper subgroup of $\text{Aut}(A_9)$ containing A_9 . Also, if \mathcal{D} is either of these designs, then $\text{Aut}(\mathcal{D})$ is the orthogonal group $O_8^+(2) : 2$ and $\text{Aut}(A_9) \not\leq \text{Aut}(\mathcal{D})$.

We found other alternating groups that countered the conjecture, for example

A_{10} of degree 2520 using an orbit of length 144, A_{11} of degree 462 using an orbit of length 200, and A_{11} of degree 2520 using orbits of length 495 and 1584, respectively. None of these are rank-3 representations, although all the counter-examples we give in this chapter are. We should point out that most the simple groups we tried did in fact satisfy the conjecture, that is all their primitive representations did satisfy the conjecture. The counter-examples are relatively rare, and interesting.

6.2 Symplectic groups

The simple symplectic groups $PSp_{2m}(q)$, for m at least 2, in their natural primitive rank-3 action on the points of projective $(2m - 1)$ -space over the finite field \mathbb{F}_q , provide an infinite set of groups that do not satisfy the Conjecture 6.1.1, by taking the action on the symmetric design of points and hyperplanes of the $(2m - 1)$ -space, or of its complementary design. For q odd or for q even and $m > 2$, we have the automorphism group of $PSp_{2m}(q)$ as a proper subgroup of the automorphism group of the design. While for $q = 2^t$, $t \geq 2$ and $m = 2$, there are automorphisms of $PSp_{2m}(q)$ that are not automorphisms of the design.

From Theorem 2.4.10 we know that $PSp_{2m}(q)$, where m is at least 2 and q is any prime power, acts as a primitive rank-3 group of degree $\frac{q^{2m}-1}{q-1}$ on the points of the projective $(2m - 1)$ -space $PG_{2m-1}(\mathbb{F}_q)$. The orbits of the stabilizer of a point P consist of $\{P\}$, one of length $\frac{q^{2m-1}-1}{q-1} - 1$ and the other of length q^{2m-1} . The point P together with the points of the orbit of length $\frac{q^{2m-1}-1}{q-1} - 1$ form a hyperplane, which is in fact the image of the absolute point P under the symplectic polarity. The symmetric $1-(\frac{q^{2m}-1}{q-1}, q^{2m-1}, q^{2m-1})$ design \mathcal{D} formed following the method of Theorem 5.2.1 by orbiting the orbit of length q^{2m-1} is the complement of the design of points and hyperplanes obtained by taking the union of the other two orbits. This latter design is a symmetric 2-design (see

Proposition 4.3.1) $2-(\frac{q^{2m}-1}{q-1}, \frac{q^{2m-1}-1}{q-1}, \frac{q^{2m-2}-1}{q-1})$ and hence the complement \mathcal{D} is also a 2-design, with parameters $2-(\frac{q^{2m}-1}{q-1}, q^{2m-1}, q^{2m-1} - q^{2m-2})$.

By Theorem 3.4.1 we have that the automorphism group of the design of points and planes, and hence also of its complementary design, is the full projective semi-linear group $P\Gamma L_{2m}(q)$.

The automorphism group of $PSp_{2m}(q)$ is discussed in Dieudonné [41, Chapter 4], but completely determined for the case where $m = 2$ and q is even, by Steinberg [89]: see also Carter [23] for a description. Essentially, the automorphism group is $P\Gamma Sp_{2m}(q)$ except when $m = 2$ and $q > 2$ is even, in which case it is this group extended by an involution σ that is not in $P\Gamma L_4(q)$. Thus the automorphism group of the simple group is a proper subgroup of that of the design in the case of odd q or the case of $m > 2$; for $m = 2$ and $q > 2$ even, it is not a subgroup of the automorphism group of the design. Either way, we have an infinite class of counter-examples to the Conjecture 6.1.1.

The above discussion has thus proved the following theorem:

Theorem 6.2.1 *Let G be the simple symplectic group $PSp_{2m}(q)$, where $m \geq 2$ and even, and q is any prime power, acting as a primitive rank-3 group of degree $\frac{q^{2m}-1}{q-1}$, and let \mathcal{D} be the $1-(\frac{q^{2m}-1}{q-1}, q^{2m-1}, q^{2m-1})$ design formed from the longer orbit of a point-stabilizer. Then \mathcal{D} is a symmetric 2-design with automorphism group $P\Gamma L_{2m}(q)$ which properly contains the automorphism group of $PSp_{2m}(q)$ unless $m = 2$ and $q = 2^t$ where $t \geq 2$. For all cases, $\text{Aut}(\mathcal{D}) \not\leq \text{Aut}(G)$.*

Note 6.2.2 1. The case $PSp_4(2)$ is somewhat different and does not fit into the above class (see the results for A_6 in Section 6.3.1).

2. The codes of the designs in Theorem 6.2.1 are well known and are p -ary subcodes of the projective generalized Reed-Muller codes: see [3, Chapter 5].

6.3 Alternating groups

In this section, in a manner similar to the study in [66], and Section 5.3 we examine the designs and codes from all the primitive permutation representations of A_6 and A_9 , the alternating groups of degree 6 and 9, respectively. Note that $\text{Aut}(A_6) = A_6 : 2^2$, A_6 being the only alternating group whose full automorphism group is not the symmetric group; $\text{Aut}(A_9) = S_9$. We looked first at A_6 , of order 360, and its maximal subgroups and primitive permutation representations via the coset action on these subgroups: see ATLAS [27]. There are five distinct primitive permutation representations of degrees 6, 6, 10, 15 and 15, respectively, and only the representations of degree 15 gave non-trivial designs. We then considered A_9 , of order 181440, which has eight primitive permutation representations of degrees 9, 36, 84, 120, 120, 126, 280 and 840 respectively. For each of these groups, using Programme A2 (see Appendix A.2), we found the corresponding designs as described in Theorem 5.2.1, and computed the full automorphism groups of the designs. We also constructed for each design the associated code for the primes p that divide the order of the simple group. The computations in Appendix A.2 list the p -rank of the designs and the dimension of the hull in each case. Where possible we have also computed the automorphism groups of the codes.

6.3.1 Computations for A_6

Of the five primitive permutation representations of A_6 , only the representations of degree 15 give non-trivial designs. The representations and orbit lengths are shown in Table 6.1: the first column gives the ordering of the primitive representations as given by Magma (or the ATLAS [27]) and as used in our computations (see Appendix A.2); the second gives the maximal subgroups; the third gives the degree (the number of cosets of the point stabilizer); the fourth gives the number of orbits, and the remaining columns give the size of the non-trivial orbits of the

point-stabilizer.

No.	Max. sub.	Deg.	#	length	
1	A_5	6	2	5	
2	A_5	6	2	5	
3	$3^2 : 4$	10	2	9	
4	S_4	15	3	6	8
5	S_4	15	3	6	8

Table 6.1: Orbits of the point-stabilizer of A_6

The first three representations give trivial designs. We used Magma to construct the permutation group and form the orbits of the stabilizer of a point for each of the representations of degree 15. For each of the non-trivial orbits, we formed the symmetric 1-design as described in Theorem 5.2.1. We found that the designs obtained with the same parameters for these two representations were isomorphic. Thus in all there are four non-isomorphic symmetric designs for A_6 formed using single orbits. Note that none of the designs has A_6 acting as the full automorphism group, and neither was there a design whose automorphism group was $\text{Aut}(A_6) = A_6 : 2^2$, since the trivial designs have the symmetric group of degree 6 or 10, respectively, as automorphism group, and those on 15 points have either A_8 or the symmetric group S_6 : see Appendix A.2.

Considering either of the representations of degree 15, an orbit of length 8 produces a 1-(15, 8, 8) design with automorphism group of order 20160. This representation is similar to that described for the symplectic groups, since $A_6 \cong Sp_4(2)'$, the derived group of $Sp_4(2)$. We have a rank-3 group acting on points of the projective 3-space $PG_3(\mathbb{F}_2)$.

Proposition 6.3.1 *For $G = A_6$ of degree 15, the automorphism group A of the*

design \mathcal{D} with parameters $1-(15, 8, 8)$ is $PGL_4(2) \cong A_8$ and does not contain $\text{Aut}(G)$.

Proof: Since A_6 is a subgroup of $Sp_4(2)$, this action is that on the points of $PG_3(\mathbb{F}_2)$ and the $1-(15, 8, 8)$ design is actually a symmetric $2-(15, 8, 4)$ design, and the complement of the $2-(15, 7, 3)$ design of points and planes. Its automorphism group A is thus $PGL_4(2)$, by Theorem 3.4.1. That this is isomorphic to A_8 can be found in Dickson [39].

Since $\text{Aut}(A_6) = A_6 : 2^2$ and since A_8 has no subgroup of index 14 (see [27]), we deduce that $\text{Aut}(A_6)$ is not a subgroup of A_8 . In addition, computation of the normalizer $N_A(G)$ showed that it has order 720, and is thus S_6 . Furthermore, since $|A_8| > |A_6 : 2^2|$, A_8 cannot be a subgroup of $\text{Aut}(A_6) = A_6 : 2^2$. ■

6.3.2 Computations for A_9

From the eight primitive permutation representations, we obtained in all 25 non-isomorphic symmetric designs formed using Theorem 5.2.1 from single orbits, on which A_9 acts primitively. The full list of designs and codes is given in Appendix A.2. From the list of designs and codes produced by our computations we have singled out for discussion a case where the automorphism groups of both design and code were distinct from A_9 or $\text{Aut}(A_9)$. This arose for A_9 of degree 120 where the orbits of length 56 and 63 yield designs and codes with the orthogonal group $O_8^+(2) : 2$ as automorphism group.

Table 6.2 gives the same information for A_9 as Table 6.1 gives for A_6 . The numbers appearing in parenthesis represent the number of orbits of the point stabilizer in case there is more than one of that length.

Writing $G = A_9$, there are precisely 25 non-isomorphic self-dual 1-designs obtained by taking all the images under G of single non-trivial orbits of the point

No.	Max. sub.	Deg.	#	len.					
1	A_8	9	2	8					
2	S_7	36	3	14	21				
3	$(A_6 \times 3) : 2$	84	4	18	20	45			
4	$L_2(8) : 3$	120	3	56	63				
5	$L_2(8) : 3$	120	3	56	63				
6	$(A_5 \times A_4) : 2$	126	5	5	20	40	60		
7	$3^3 : S_4$	280	5	27	36	54	162		
8	$3^2 : 2A_4$	840	12	8	24(2)	27	36	72(4)	216(2)

Table 6.2: Orbits of the point-stabilizer of A_9

stabilizer in any of G 's primitive representations, and on which G acts primitively on points and blocks. Our computations show that the full automorphism groups of the designs are either A_9 , $S_9 = \text{Aut}(A_9)$ or the orthogonal group $O_8^+(2) : 2$.

Our results for A_9 show that for A_9 of degree 120, the fourth or fifth rank-3 representation, an orbit of length 56 gives a 1-(120, 56, 56) design. Since the representation is of rank-3, the orbits also define strongly regular graphs on 120 vertices, of valency 56 and 63 respectively: these graphs are well-known and appear in the list of Brouwer[14, page 675]. This design yields a $[120, 8]_2$ self-orthogonal doubly-even code.

Proposition 6.3.2 *For $G = A_9$ of degree 120, the automorphism group of the design \mathcal{D} with parameters 1-(120, 56, 56) is the orthogonal group $O_8^+(2) : 2$, which neither contains nor is contained in $\text{Aut}(G)$.*

Proof: Let $G = A_9$ and \overline{G} denote $\text{Aut}(\mathcal{D})$ where \mathcal{D} is constructed from an orbit of length 56 for A_9 of degree 120. Magma computations show that \overline{G} is a non-abelian group of order 348364800 generated by the permutations which we denote by a, b, c, d, e, f, g and h listed in the appendix (see Appendix B). Computations with

Magma show that there exists a non-abelian subgroup N of \overline{G} of order 174182400. Since $[\overline{G} : N] = 2$ we have that $N \trianglelefteq \overline{G}$. We claim that $N \cong O_8^+(2)$. A composition series for \overline{G} found by using Magma is $\overline{G} \geq N \geq 1_{\overline{G}}$; this is in fact a chief series for \overline{G} . Thus N is a non-abelian chief factor of \overline{G} . Since $|N| = 174182400 = |O_8^+(2)|$, we have that $N \cong O_8^+(2)$, as asserted.

It follows that $\overline{G} \cong O_8^+(2).2$. The permutation $\alpha =$

(1, 84) (2, 31) (5, 62) (8, 83) (10, 26) (11, 113) (12, 103) (13, 75) (14, 38)
 (15, 67) (17, 37) (22, 72) (23, 102) (24, 82) (25, 70) (27, 52) (29, 120)
 (41, 90) (45, 117) (47, 59) (48, 104) (50, 94) (58, 89) (63, 101) (64, 108)
 (71, 85) (78, 97) (87, 112)

is in $\overline{G} - N$ and $o(\alpha) = 2$. Hence \overline{G} is a split extension of N by $\langle \alpha \rangle$.

We know that $\text{Aut}(A_9) = S_9$, and since the normalizer $N_{\overline{G}}(G) = G$, we have $\text{Aut}(G) \not\leq \text{Aut}(\mathcal{D})$, as asserted. Note however that from the ATLAS [27] we know that S_9 is a maximal subgroup of $O_8^+(2):2$ of index 960, so \overline{G} does contain isomorphic copies of $\text{Aut}(A_9)$. ■

The design discussed in Proposition 6.3.2 is another counter-example to the Conjecture 6.1.1.

We found that the 1-(120, 56, 56) design yields a $[120, 8]_2$ binary code whose automorphism group has order 348364800. This leads to:

Proposition 6.3.3 *The orthogonal group $O_8^+(2):2$ is the automorphism group of the $[120, 8]_2$ binary code C derived from the 1-(120, 56, 56) design \mathcal{D} . The code C is self orthogonal and doubly-even, with minimum distance 56. Its dual is a $[120, 112, 3]_2$ with 1120 words of weight 3.*

Proof: The automorphism group of the $[120, 8]_2$ binary code C derived from the 1-(120, 56, 56) design constructed from A_9 of degree 120 contains \overline{G} , the

automorphism group of the design, and has, by computation, the same order, and thus is equal to \overline{G} .

Since the dimension of C equals the dimension of the hull (see Appendix A.2) it follows that $C \subseteq C^\perp$ and so C is self orthogonal. Since the incidence vectors of the blocks of the design span the code, and the vectors have weight 56, C is doubly-even. In fact Magma gives the weight distribution:

$\langle 0, 1 \rangle, \langle 56, 120 \rangle, \langle 64, 135 \rangle$

That C^\perp has minimum weight 3 was found using Magma. The full weight distribution can be obtained. ■

Conjecture 6.1.1 does thus not generally hold, although it does hold for most representations.

In addition to the above results we have also found codes with interesting properties and parameters, from the representations of A_9 .

- The hull of the 1-(126, 60, 60) design is a $[126, 26, 32]_2$ doubly-even self-orthogonal code with automorphism group of order 3628800, which is isomorphic to S_{10} . This is also the automorphism group of the 1-(126, 60, 60) design's code, a $[126, 74, d]_2$, where $d \leq 12$ and its dual, a $[126, 52, 14]_2$ code. This then provides an example of the automorphism group of the code being larger than that of the design. The weight distribution of the hull is as follows:

```
> WeightDistribution(hull);
[<0,1>,<32,1575>,<36,2520>,<40,630>,<44,119700>,<48,278775>,
<52,2926350>,<56,9239940>,<60,16352280>,<64,17803800>,
<68,13894650>,<72,5005350>,<76,1313172>,<80,114345>,<84,55650>,
<100,126> ]
```

The words of weight 100 form a 1 -(126,100,100) design with S_{10} as automorphism group, and with the code of the design the hull found above. The design can also be formed by orbiting the union of an orbit of length 40 with one of length 60. The complementary design is a 1 -(126,26,26) whose code is a $[126, 27, 26]_2$ that contains the code of the hull shown above, and is obtained from that code by adding the all-one vector.

- The binary code of the 1 -(280, 36, 36) design is a $[280, 42, 36]_2$ self-orthogonal doubly-even code.
- The ternary code of the 1 -(120, 63, 63) design is a $[120, 36, 24]_3$ self-orthogonal code with $O_8^+(2) : 2$ acting on it.

Chapter 7

Binary Codes from Symplectic Groups

7.1 Introduction

In their natural primitive rank-3 action on the points of projective space of dimension $2m - 1$, the projective symplectic groups $PSp_{2m}(q)$, where q is a power of an odd prime, and $m \geq 2$, have 2-modular representations that give rise to self-orthogonal binary codes whose properties can be linked to those of the underlying geometry. In this chapter we establish some properties of these codes, including bounds for the minimum weight, and the nature of some classes of codewords.

From Theorem 2.4.10 we have that the simple symplectic group $PSp_{2m}(q)$, where $m \geq 2$ and q is any prime power, acts as a primitive rank-3 group of degree $\frac{q^{2m}-1}{q-1}$ on the points of the projective $(2m - 1)$ -space $PG_{2m-1}(\mathbb{F}_q)$. The orbits of the stabilizer of a point P consist of $\{P\}$ and one of length $\frac{q^{2m-1}-1}{q-1} - 1$ and the other of length q^{2m-1} . The point P together with the points of the orbit of length $\frac{q^{2m-1}-1}{q-1} - 1$ form a hyperplane, which is, in fact, the image of the absolute point P

under the symplectic polarity. The symmetric $1-(\frac{q^{2m}-1}{q-1}, \frac{q^{2m-1}-1}{q-1} - 1, \frac{q^{2m-1}-1}{q-1} - 1)$ design \mathcal{D} formed by orbiting the orbit of length $\frac{q^{2m-1}-1}{q-1} - 1$ under $PSp_{2m}(q)$ gives the binary code that we will be examining when q is odd. When q is even, we still obtain the designs and codes, but the interesting binary codes in these cases are then the binary codes of the projective geometry design of points and hyperplanes, with the larger projective semi-linear group acting: they are the well-known generalized Reed-Muller codes (see, for example, Theorem 6.2.1 or [5, Chapter 5]).

Alternatively this code can be obtained by taking the row span over \mathbb{F}_2 of an adjacency matrix of the strongly regular graph defined by the rank-3 action of $PSp_{2m}(q)$. Since in this chapter we are looking at rank-3 groups, the graphs are actually strongly regular: see Section 3.3 and Higman [51]. The codes are the binary span of the adjacency matrix of the graph. The dimension of these codes has been determined previously (see [15, 51, 75] for collected results), but here we look more closely at the codes and use the geometry to gain some insight into the nature of possible codewords, in particular those of small weight. We obtain the results through a series of lemmas in Section 7.2, and sum up our results in Theorem 7.2.11.

7.2 The binary codes

In all the following we will take G to be the symplectic group $PSp_{2m}(q)$, where $m \geq 2$ and q is a power of an odd prime, in its natural primitive rank-3 action of degree $\frac{q^{2m}-1}{q-1}$ on the points of the projective $(2m-1)$ -space $\mathcal{P}(V) = PG_{2m-1}(\mathbb{F}_q)$, where $V = V_{2m}(\mathbb{F}_q)$. For the orbits Δ of the stabilizer of a point, as described in Theorem 5.2.1, we take the one of length $\frac{q^{2m-1}-1}{q-1} - 1$ and get a symmetric $1-(\frac{q^{2m}-1}{q-1}, \frac{q^{2m-1}-1}{q-1} - 1, \frac{q^{2m-1}-1}{q-1} - 1)$ design \mathcal{D} . In all that follows C will denote the binary code of this design. Clearly G acts as an automorphism group on \mathcal{D} and

on C , and on C^\perp .

Notice that in our construction of the design, if we use the stabilizer of the point P of \mathcal{P} , then G_P fixes also the polar of P , that is the hyperplane P^σ . Thus the orbit of length $\frac{q^{2m-1}-1}{q-1} - 1$ that we orbit to get the design is $P^\sigma \setminus \{P\}$. Let \mathcal{H} denote the set of hyperplanes of $\mathcal{P}(V)$. By Theorem 5.2.1 we have that $\mathcal{B} = \{\Delta^g \mid g \in G\}$, so if we let $H_0 = \Delta \cup \{P\}$, then $H_0^\sigma = \{P\}$ and so $\mathcal{H} = \{H_0^g \mid g \in G\} = \{(\Delta \cup \{P\})^g \mid g \in G\} = \{\Delta^g \cup \{P^g\} \mid g \in G\}$, this is so, since the symplectic group is a transitive group on hyperplanes. Hence for $H \in \mathcal{H}$ we have that $v^H + v^{H^\sigma} = v^{\Delta^g \cup \{P^g\}} + v^{\{P^g\}} = v^{\Delta^g} + v^{\{P^g\}} + v^{\{P^g\}} = v^{\Delta^g}$. Therefore we can consider the binary code C to be

$$C = \langle v^H + v^{H^\sigma} \mid H \in \mathcal{H} \rangle = \langle v^{\Delta^g} \mid g \in G \rangle = \langle v^B \mid B \in \mathcal{B} \rangle.$$

We will now prove a series of lemmas that lead to some properties of the codes C and C^\perp , where, in all the lemmas, C is the binary code of the

$$1 - \left(\frac{q^{2m}-1}{q-1}, \frac{q^{2m-1}-1}{q-1} - 1, \frac{q^{2m-1}-1}{q-1} - 1 \right)$$

design \mathcal{D} . The results will be summarized in Theorem 7.2.11.

Lemma 7.2.1 *C is self-orthogonal, that is $C \subseteq C^\perp$. Furthermore, C is doubly-even for all $m \geq 2$ if $q \equiv 3 \pmod{4}$ and for m odd if $q \equiv 1 \pmod{4}$.*

Proof: We need to show that, using the standard inner product (\cdot, \cdot) , $(v^H + v^{H^\sigma}, v^K + v^{K^\sigma}) = 0$ for any hyperplanes H and K in \mathcal{H} . Note first that since H has dimension $2m-1$, and since $H^\sigma \in H$,

$$\text{wt}(v^H + v^{H^\sigma}) = \sum_{i=1}^{2m-2} q^i \equiv 0 \pmod{2},$$

and so the generating vectors of C have even weight, and thus $(v^H + v^{H^\sigma}, v^H + v^{H^\sigma}) = 0$.

Now consider two cases: suppose first that $K^\sigma \in H$. Then also $H^\sigma \in K$.

$$\begin{aligned} (v^H + v^{H^\sigma}, v^K + v^{K^\sigma}) &= (v^H, v^K) + (v^H, v^{K^\sigma}) + (v^{H^\sigma}, v^K) + (v^{H^\sigma}, v^{K^\sigma}) \\ &= \sum_{i=0}^{2m-3} q^i + 1 + 1 + 0 \equiv 0 \pmod{2}. \end{aligned}$$

If $K^\sigma \notin H$, then also $H^\sigma \notin K$ and

$$\begin{aligned} (v^H + v^{H^\sigma}, v^K + v^{K^\sigma}) &= (v^H, v^K) + (v^H, v^{K^\sigma}) + (v^{H^\sigma}, v^K) + (v^{H^\sigma}, v^{K^\sigma}) \\ &= \sum_{i=0}^{2m-3} q^i + 0 + 0 + 0 \equiv 0 \pmod{2}. \end{aligned}$$

This proves the assertion concerning self-orthogonality. The observation about C being doubly-even follows simply by noticing for which values of m , $\text{wt}(v^H + v^{H^\sigma})$, for $H \in \mathcal{H}$, is divisible by 4. ■

Lemma 7.2.2 *If U is a maximal totally isotropic subspace of V , then $v^U \in C^\perp$ if and only if m is odd. If U_1 and U_2 are maximal totally isotropic subspaces, then $v^{U_1} + v^{U_2} \in C^\perp$.*

Proof: Let $U = U^\sigma$ be a maximal totally isotropic subspace, and hence of dimension m . If $H \in \mathcal{H}$,

$$(v^H + v^{H^\sigma}, v^U) = (v^H, v^U) + (v^{H^\sigma}, v^U).$$

Take first the case where $U \not\subseteq H$. Then $H^\sigma \not\subseteq U^\sigma = U$, and thus $(v^{H^\sigma}, v^U) = 0$. Also, $H \cap U$ is a subspace of dimension $m - 1$, and thus

$$(v^H, v^U) = |H \cap U| = \sum_{i=0}^{m-2} q^i \equiv \begin{cases} 1 & \text{if } m \text{ is even,} \\ 0 & \text{if } m \text{ is odd,} \end{cases}$$

and hence

$$(v^H + v^{H^\sigma}, v^U) \equiv \begin{cases} 1 & \text{if } m \text{ is even,} \\ 0 & \text{if } m \text{ is odd.} \end{cases}$$

If $U \subseteq H$, then $H^\sigma \in U^\sigma = U$, and

$$\begin{aligned} (v^H + v^{H^\sigma}, v^U) &= (v^H, v^U) + (v^{H^\sigma}, v^U) \\ &\equiv |U| + 1. \end{aligned}$$

Here

$$|U| = \sum_{i=0}^{m-1} q^i \equiv \begin{cases} 1 & \text{if } m \text{ is odd,} \\ 0 & \text{if } m \text{ is even,} \end{cases}$$

so

$$(v^H + v^{H^\sigma}, v^U) \equiv \begin{cases} 1 & \text{if } m \text{ is even,} \\ 0 & \text{if } m \text{ is odd.} \end{cases}$$

It follows that $v^U \in C^\perp$ if and only if m is odd.

To prove the other statement, clearly if m is odd then $v^{U_1} + v^{U_2} \in C^\perp$. If m is even then $(v^H + v^{H^\sigma}, v^U) = 1$ for any totally isotropic space of dimension m . Thus again $v^{U_1} + v^{U_2} \in C^\perp$. ■

Lemma 7.2.3 $\mathbf{j} \in C$ if and only if m is even; $\mathbf{j} \in C^\perp$ for all m .

Proof: If m is odd, then by Lemma 7.2.2, $v^U \in C^\perp$, where U is a totally isotropic subspace of dimension m . Now $\text{wt}(v^U) = |U| = \sum_{i=0}^{m-1} q^i \equiv 1$, and thus $(\mathbf{j}, v^U) = 1$, and so $\mathbf{j} \notin (C^\perp)^\perp = C$.

Now suppose that m is even and that U is a maximal totally isotropic subspace. Let

$$w = \sum_{U \subset H \in \mathcal{H}} (v^H + v^{H^\sigma}).$$

For $U \subset H$, $H^\sigma \in U$, and so there are exactly $|U|$ hyperplanes that contain U . Write $w = w_1 + w_2$ where $w_1 = \sum_{U \subset H \in \mathcal{H}} v^H$ and $w_2 = \sum_{U \subset H \in \mathcal{H}} v^{H^\sigma}$. Thus $w_2 = v^U$.

For $P \in U$, $w_1(P)$ will register the number of hyperplanes containing U , that is $w_1(P) = \sum_{i=0}^{m-1} q^i \equiv 0 \pmod{2}$, since $m-1$ is odd. For $P \notin U$, $w_1(P)$ will register the number of hyperplanes that contain U and P . This means counting the number of hyperplanes containing the dimension- $(m+1)$ space spanned by P and U , and this is given by Equation (3.6) to be $\sum_{i=0}^{m-2} q^i \equiv 1 \pmod{2}$, since $m-2$ is even. Thus $w_1(P) = 1$ for $P \notin U$. It follows that $w(P) = w_1(P) + w_2(P) = 1$ for all points P , and hence $w = \mathbf{j} \in C$ for m even.

Finally note that it is clear that $\mathbf{j} \in C^\perp$ in all cases since C is spanned by even-weight vectors. ■

Lemma 7.2.4 *If U is a subspace of dimension n where $1 \leq n \leq m$, then*

$$v^U + v^{U^\sigma} \in C \text{ if } n \text{ is odd, and}$$

$$\mathbf{j} + v^U + v^{U^\sigma} \in C \text{ if } n \text{ is even.}$$

Then $v^U + v^{U^\sigma} \in C^\perp$ for all values of m . If n is even, $v^U + v^{U^\sigma} \in C$ if and only if m is even. In particular, if U has dimension m then $v^U + v^{U^\sigma} \in C$. Further, if $U \cap U^\sigma$ has dimension r , where $0 \leq r \leq n \leq m$, then

$$\text{wt}(v^U + v^{U^\sigma}) = 2q^r \sum_{i=0}^{n-r-1} q^i + q^n \sum_{i=0}^{2m-2n-1} q^i.$$

Proof: Given U , let

$$w = \sum_{U \subset H \in \mathcal{H}} (v^H + v^{H^\sigma}) = \sum_{U \subset H \in \mathcal{H}} v^H + \sum_{U \subset H \in \mathcal{H}} v^{H^\sigma} = w_1 + w_2.$$

For each term in the sum, $U \subset H$ implies that $H^\sigma \in U^\sigma$, so $w_2 = v^{U^\sigma}$.

For $P \in \mathcal{P}$, if $P \in U$ then $w_1(P)$ will register the number of hyperplanes that contain U , and thus

$$w_1(P) = \sum_{i=0}^{2m-n-1} q^i \equiv \begin{cases} 1 & \text{if } n \text{ is odd,} \\ 0 & \text{if } n \text{ is even.} \end{cases}$$

If $P \notin U$, then $w_1(P)$ counts the number of hyperplanes containing $\langle P, U \rangle$, and thus

$$w_1(P) = \sum_{i=0}^{2m-(n+1)-1} q^i \equiv \begin{cases} 1 & \text{if } n \text{ is even,} \\ 0 & \text{if } n \text{ is odd.} \end{cases}$$

Thus if n is odd, $w_1 = v^U$, and $w = v^U + v^{U^\sigma} \in C$. If n is even, then $w_1 = \mathbf{j} + v^U$, and $w = \mathbf{j} + v^U + v^{U^\sigma} \in C$. Since by Lemma 7.2.3, $\mathbf{j} \in C$ if and only if m is even, the first part of the result is proved. The weight of the vector $v^U + v^{U^\sigma}$ follows directly. ■

Note 7.2.5 As is customary, if the upper limit of the sum in the above summations is lower than the lower limit, we take the sum to be zero.

Lemma 7.2.6 *For m even, the minimum weight of C^\perp is at most $2q^{m-1}$.*

Proof: By Lemma 7.2.2 we have that $v^{U_1} + v^{U_2} \in C^\perp$ for any pair of totally isotropic subspaces of dimension m . We will show that we can find two such subspaces that intersect in a subspace of dimension $(m-1)$. For this we need to use a specific symplectic form, and we use that described in Equation 2.1 (see Section 2.4.1). With that notation, we take

$$U_1 = \langle e_1, e_2, \dots, e_m \rangle,$$

and

$$U_2 = \langle e_1, e_2, \dots, e_{m-1}, e_{m+1} \rangle.$$

Then $U_1 \cap U_2 = \langle e_1, e_2, \dots, e_{m-1} \rangle$ and hence the vector $v^{U_1} + v^{U_2}$ has weight $2q^{m-1}$. ■

Lemma 7.2.7 *The minimum weight of C is at most $2q^{m-2}(q+1)$.*

Proof: We construct words of this weight using Lemma 7.2.4 by finding an isotropic subspace of dimension m that meets its polar in dimension $(m - 2)$. Note first that an isotropic space U of dimension n meets its polar in dimension $n - r$ where r must be even since $U/(U \cap U^\sigma)$ is a non-degenerate symplectic space of dimension r and thus must have even dimension. Thus we cannot have isotropic spaces of dimension m meeting their polars in dimension $m - 1$. With the notation of Section 2.4.1 again, we first take the case $m = 2$. Here if $U = \langle e_1, e_4 \rangle$, then $U^\sigma = \langle e_2, e_3 \rangle$, and $U \cap U^\sigma = \{0\}$, that is empty in $\mathcal{P}(V)$. For $m > 2$, let

$$U = \langle e_1, e_2, \dots, e_{m-2}, e_{m-1}, e_{m+2} \rangle.$$

Then

$$U^\sigma = \langle e_1, e_2, \dots, e_{m-2}, e_m, e_{m+1} \rangle,$$

and

$$U \cap U^\sigma = \langle e_1, e_2, \dots, e_{m-2} \rangle.$$

It follows that $v^U + v^{U^\sigma} \in C$ and has weight $2(q^{m-1} + q^{m-2})$, as asserted. ■

Lemma 7.2.8 *The minimum weight of C^\perp and also of C is at least $q + 1$.*

Proof: Let $w \in C^\perp$ and let $P \in \text{Supp}(w) = \mathcal{Q}$. Every block of the design \mathcal{D} passing through P must meet \mathcal{Q} again. There are $(\frac{q^{2m-1}-1}{q-1} - 1)$ blocks through P , all of which must meet the \mathcal{Q} again, since $w \in C^\perp$ and we have that $\langle w, w^\mathcal{Q} \rangle = 0$. If a block through P meet \mathcal{Q} only once then we would have $\langle w, w^\mathcal{Q} \rangle \neq 0$ thus contradicting the fact that $w \in C^\perp$. Since blocks of \mathcal{D} are subsets of hyperplanes, the number of blocks through P and another point of \mathcal{Q} is at most the number of hyperplanes through the two points, that is at most $\frac{q^{2m-2}-1}{q-1}$. Thus there are at least

$$\frac{1 + (\frac{q^{2m-1}-1}{q-1} - 1)}{\frac{q^{2m-2}-1}{q-1}} = q + 1$$

points in \mathcal{Q} . ■

Lemma 7.2.9 *For $m \geq 2$ and even*

$$\dim(C) = q \frac{(q^m + 1)(q^{m-1} - 1)}{2(q - 1)} + 1,$$

and for $m \geq 3$ and odd

$$\dim(C) = q \frac{(q^m + 1)(q^{m-1} - 1)}{2(q - 1)}.$$

Proof: The rank of the adjacency matrix of the strongly regular graph has been studied by several authors, and in particular, details are given in Brouwer and van Eijl [15]. The formula, using results of Higman [51, p. 149], is given in Lataille, Sin and Tiep [75], Equation (23) for the case of m odd; for m even this formula needs 1 added, due to the presence of j in the code in the even case. See also Bagchi, Brouwer and Wilbrink [7] for $m = 2$. ■

Lemma 7.2.10 $\text{Aut}(\mathcal{D}) = P\Gamma Sp_{2m}(q)$.

Proof: Let $\alpha \in \text{Aut}(\mathcal{D})$. If we can show that $\alpha \in P\Gamma L_{2m}(q)$ and that $\alpha\sigma = \sigma\alpha$, then we will have the result (see, for example, Dembowski [37, Section 1.4]). Let $G = PSp_{2m}(q)$; we have $G \leq \text{Aut}(\mathcal{D})$.

If \mathcal{P} denotes the set of points of \mathcal{D} then the set of blocks of \mathcal{D} is $\mathcal{B} = \{P^\sigma \setminus \{P\} \mid P \in \mathcal{P}\}$. Let $P^\varphi = P^\sigma \setminus \{P\}$ for $P \in \mathcal{P}$. As an automorphism of the design, α preserves incidence and takes blocks to blocks. We wish to show that $P^{\alpha\varphi} = P^{\varphi\alpha}$ from which it will follow that $\alpha\sigma = \sigma\alpha$.

We first show that α preserves subspaces and thus is in the group of the geometry. Let P and Q be points of \mathcal{P} such that $P \notin Q^\sigma$. Then also $Q \notin P^\sigma$ and $T = P^\sigma \cap Q^\sigma = P^\varphi \cap Q^\varphi$, since P and Q are not in T . Since incidence is preserved by α , T^α is also a subspace, of dimension $2m - 3$. Thus α maps non-isotropic subspaces of dimension $2m - 3$ to themselves, and it follows in the same way that

α preserves non-isotropic subspaces of all dimensions, down to the minimum of non-isotropic lines.

To prove that α also preserves isotropic lines, suppose first that $P^\alpha = P$. Then the non-isotropic lines through P are all mapped to non-isotropic lines through P . Since a line through P is non-isotropic if and only if it meets P^σ at P , it follows that P^σ is fixed by α and $P^{\alpha\varphi} = P^{\varphi\alpha}$. Suppose now that $P^\alpha = Q$. Since G is transitive on points, there exists $g \in G$ such that $Q^g = P$. Thus $P^{\alpha g} = P$, and αg also preserves non-isotropic lines since both α and g do. As in the first case, $(P^\varphi)^{\alpha g} = P^\varphi = (Q^g)^\varphi = (Q^\varphi)^g$, since $g \in G = PSp_{2m}(q)$. So $(P^\varphi)^{\alpha g} = (P^\alpha)^{\varphi g}$, and $(P^\varphi)^\alpha = (P^\alpha)^\varphi$. It follows that $\alpha\varphi = \varphi\alpha$. Since α maps hyperplanes $P \cup P^\varphi = P^\sigma$ to hyperplanes, and preserves incidence, it also maps isotropic lines to isotropic lines, and is hence in $P\Gamma L_{2m}(q)$.

That $\alpha\sigma = \sigma\alpha$ follows from the above, and so $\alpha \in P\Gamma Sp_{2m}(q)$. It is clear that every element of this group is an automorphism of the design, and so the result is proved. ■

Combining all these lemmas, we have thus proved the following theorem:

Theorem 7.2.11 *Let G be the simple symplectic group $PSp_{2m}(q)$, where $m \geq 2$ and q is a power of an odd prime, in its natural action as a primitive rank-3 group of degree $\frac{q^{2m}-1}{q-1}$ on the points of the projective $(2m-1)$ -space $PG_{2m-1}(\mathbb{F}_q)$. Let \mathcal{D} be the symmetric $1-(\frac{q^{2m}-1}{q-1}, \frac{q^{2m-1}-1}{q-1} - 1, \frac{q^{2m-1}-1}{q-1} - 1)$ design whose blocks are the images under G of the orbit of length $\frac{q^{2m-1}-1}{q-1} - 1$ of the stabilizer in G of a point. Then $\text{Aut}(\mathcal{D}) = P\Gamma Sp_{2m}(q)$.*

Let $C = C_2(\mathcal{D})$ denote the binary code, of length $v = \frac{q^{2m}-1}{q-1}$, of \mathcal{D} . Then C is self-orthogonal, and C is doubly-even for all $m \geq 2$ if $q \equiv 3 \pmod{4}$ and for $m \geq 3$ odd if $q \equiv 1 \pmod{4}$.

For $m \geq 2$,

$$\dim(C) = \begin{cases} \frac{1}{2}(v-1-q^m) + 1 & \text{for } m \text{ even;} \\ \frac{1}{2}(v-1-q^m) & \text{for } m \text{ odd.} \end{cases}$$

If d denotes the minimum weight of C and d^\perp the minimum weight of C^\perp , then

$$q+1 \leq d \leq 2q^{m-2}(q+1),$$

and

$$\begin{aligned} q+1 \leq d^\perp &\leq 2q^{m-1} \text{ for } m \text{ even;} \\ q+1 \leq d^\perp &\leq \frac{q^m-1}{q-1} \text{ for } m \text{ odd.} \end{aligned}$$

Note 7.2.12 1. Appendix D includes computations (using Programme A1 listed in Appendix A.1 with G being $PSp_4(3)$ or $PSp_4(5)$) for the minimum weight for C and C^\perp for $m = 2$ and $q = 3, 5$ that meet the upper bound given in the Theorem 7.2.11.

2. The automorphism group of the code contains the automorphism group of the design, but need not be equal to it in general. For the designs and codes looked at here, the group of the code was verified to be the same as the group of the design for $m = 2$ and $q = 3, 5$.

We believe that the minimum words for both the code and its dual are as described by the lemmas and theorem, and that both the properties in the notes above will hold in general.

Chapter 8

Binary Codes of Triangular Graphs

8.1 Introduction

In Section 3.3 we have defined the triangular graph $T(n)$ to be the line graph of the complete graph K_n , for any n . It is a strongly regular graph on $\binom{n}{2}$ vertices, that is the pairs of letters $\{i, j\}$ where $i, j \in \{1, \dots, n\}$. Alternatively $T(n)$ ($n > 4$) may be viewed as the graph whose vertices are the 2-element subsets of a set of cardinality n in which two distinct vertices are adjacent if and only if they are not disjoint. The binary codes formed from the span of the adjacency matrix of such graphs have been examined by Tonchev [92, p. 171] and Haemers, Peeters and van Rijkenvorsel [50, Theorem 4.1]. See also [3, 4, 15, 16]. In particular the dimension and weight enumerator of the codes are easily determined. In this chapter we examine the codes and their duals further, and in particular show how the case $n = 6$ distinguishes itself. In Theorem 8.2.4 we show that S_n is the full automorphism group of the code for $n \geq 5$ except in the case $n = 6$. We also look at the question of minimum-weight generators of the code and of its dual.

The code formed by the span of the adjacency matrix is also the code of the $1-(\frac{n(n-1)}{2}, 2(n-2), 2(n-2))$ design \mathcal{D} obtained by taking the rows of the adjacency matrix as the incidence vectors of the blocks; the automorphism group of this design will contain the automorphism group of the graph, the latter of which is easily seen to be S_n . Similarly for the code. However for $n = 6$ the group of the design and code is larger than the group of the graph (S_6), and we will use the code to explain this, (see Lemma 8.2.1 and Theorem 8.2.4).

An alternative way to approach the designs, graphs and codes that we will be looking at is through the primitive rank-3 action of the simple alternating group A_n , for $n \geq 5$, on the 2-subsets (or duads) $\Omega^{\{2\}}$ of a set Ω of size n . By Theorem 2.4.12 we have that the orbits of the stabilizer in A_n of a duad $P = \{a, b\}$ consist of $\{P\}$ and one of length $2(n-2)$ and the other of length $\frac{(n-2)(n-3)}{2}$. We take as points the duads of Ω and for each $P \in \Omega^{\{2\}}$ we define a block \bar{P} to be $\{Q \in \Omega^{\{2\}} \mid P \cap Q \neq \emptyset, Q \neq P\}$, that is, the members of the orbit of length $2(n-2)$. The duads P and blocks \bar{P} form a symmetric $1-(\frac{n(n-1)}{2}, 2(n-2), 2(n-2))$ design whose binary code we will be examining.

8.2 The binary codes

Let n be any integer and let $T(n)$ denote the triangular graph with vertex set \mathcal{P} the $\binom{n}{2}$ 2-subsets (or duads) of a set Ω of size n . The 1-design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ will have point set \mathcal{P} and for each point (duad) $\{a, b\} \in \mathcal{P}$, $a \neq b$, $a, b \in \Omega$, a block, which we denote by $\overline{\{a, b\}}$, is defined in the following way:

$$\overline{\{a, b\}} = \{\{a, x\}, \{b, y\} \mid x \neq a, b; y \neq a, b\}.$$

Then

$$\mathcal{B} = \{ \overline{\{a, b\}} \mid a, b \in \Omega, a \neq b \}.$$

The incidence vector of the block $\overline{\{a, b\}}$ is then

$$v^{\overline{\{a, b\}}} = \sum_{x \neq a} v^{\{a, x\}} + \sum_{y \neq b} v^{\{b, y\}} \quad (8.1)$$

where, as usual with the notation from [3], the incidence vector of the subset $X \subseteq \mathcal{P}$ is denoted by v^X . Since our points here are actually pairs of elements from Ω , we emphasize that we are using the notation $v^{\{a, b\}}$ instead of the more cumbersome $v^{\{\{a, b\}\}}$, as mentioned in [3]. As a further bit of notation, if a, b, c are distinct points in Ω , we will use

$$v^{\overline{\{a, b, c\}}} = v^{\{a, b\}} + v^{\{b, c\}} + v^{\{a, c\}} \quad (8.2)$$

to denote this vector of weight 3 in the ambient space.

To avoid trivial cases we will take $n \geq 5$. Then in all the following lemmas C will denote the binary code of \mathcal{D} and of $T(n)$, and C^\perp will be its dual code.

Lemma 8.2.1 *The minimum weight of C^\perp for $n \geq 5$ is 3 and any word of the form $v^{\{a, b, c\}}$ is in C^\perp . If $n \neq 6$, these are all the words of weight 3 in C^\perp , and the number of words of weight 3 is thus $\binom{n}{3}$. If $n = 6$, further words of weight 3 have the form $v^{\{a, b\}} + v^{\{c, d\}} + v^{\{e, f\}}$ where $\Omega = \{a, b, c, d, e, f\}$; in this case there are 35 words of weight 3.*

Proof: We first check that the minimum weight cannot be smaller: suppose $w = v^{\{a, b\}} + v^{\{c, d\}}$ where a, b, c, d are all distinct. Then if $e \in \Omega$ is distinct from all these (such an element will exist since we are taking $n \geq 5$), then $(w, v^{\overline{\{a, e\}}}) = (v^{\{a, b\}} + v^{\{c, d\}}, \sum_{x \neq a, e} v^{\{a, x\}} + \sum_{y \neq a, e} v^{\{e, y\}}) = 1$. If $w = v^{\{a, b\}} + v^{\{a, d\}}$, then $(w, v^{\overline{\{a, b\}}}) = (v^{\{a, b\}} + v^{\{c, d\}}, \sum_{x \neq a, b} v^{\{a, x\}} + \sum_{y \neq a, b} v^{\{b, y\}}) = 3 \equiv 1 \pmod{2}$. Hence there are no words of weight smaller than 3. So the minimum weight is at least 3.

Now let $w = v^{\overline{\{a, b, c\}}}$, and consider $(w, v^{\overline{\{x, y\}}})$ for any distinct $x, y \in \Omega$. It is easy to check that this is 0 (mod 2) for all choices of x, y . Furthermore, checking

other possible vectors of weight 3, the only case that is not immediately ruled out is $w = v^{\{a,b\}} + v^{\{c,d\}} + v^{\{e,f\}}$. If there is another element $g \in \Omega$, then $(w, v^{\overline{\{a,g\}}}) = 1$, but if $n = 6$ then $w \in C^\perp$, giving another 15 weight-3 vectors in C^\perp . ■

Lemma 8.2.2 *If n is even then $C \subseteq C^\perp$ and C is doubly-even; if n is odd, $C \oplus C^\perp = \mathbb{F}_2^{\binom{n}{2}}$. For any n , $\mathbf{j} \in C^\perp$.*

Proof: Since blocks are of even size $2(n-2)$, we have that \mathbf{j} meets evenly every vector of C , so $\mathbf{j} \in C^\perp$. For the first statement, consider $(v^{\overline{\{a,b\}}}, v^{\overline{\{c,d\}}})$. If $\{a,b\} = \{c,d\}$ then this is zero. If $d = a$ then the inner product is $n+2 = 0$ if n is even. If a, b, c, d are all distinct, then the inner product is $4 \equiv 0 \pmod{2}$.

For any $a, b \in \Omega$, we have

$$\begin{aligned} \sum_{c \neq a,b} v^{\overline{\{a,b,c\}}} &= \sum_{c \neq a,b} v^{\{a,b\}} + \sum_{c \neq a,b} v^{\{a,c\}} + \sum_{c \neq a,b} v^{\{b,c\}} \\ &= (n-2) v^{\{a,b\}} + v^{\overline{\{a,b\}}}. \end{aligned}$$

Thus if n is odd, $v^{\{a,b\}} \in C + C^\perp$ for any a, b , while for n even we obtain once again that $v^{\overline{\{a,b\}}} \in C^\perp$. Clearly C is doubly-even when n is even. ■

Considering words in the code, note that

$$v^{\overline{\{a,b\}}} + v^{\overline{\{a,c\}}} = v^{\overline{\{b,c\}}}, \quad (8.3)$$

so we need only consider sums of blocks defined by disjoint duads. The following lemma follows easily and the results are mentioned in [50]. Note that in this lemma, the notation $\langle i, A(i) \rangle$ denotes the fact that there are $A(i)$ vectors of weight i .

Lemma 8.2.3 *If $n = 2m$ then C is a $[(\frac{2m}{2}), 2m - 2, 4(m - 1)]_2$ code with weight distribution the zero vector and*

$$< 4(m - 1), \binom{2m}{2} >, < 8(m - 2), \binom{2m}{4} >, \dots, < m^2, \frac{1}{2} \binom{2m}{m} >$$

if m is even, and

$$< 4(m - 1), \binom{2m}{2} >, < 8(m - 2), \binom{2m}{4} >, \dots, < m^2 - 1, \binom{2m}{m-1} >$$

if m is odd.

If n is odd, then C is a $[(\frac{n}{2}), n - 1, n - 1]_2$ code with weight distribution the zero vector and

$$< n - 1, n >, \dots, < 2i(n - 2i), \binom{n}{2i} >, \dots,$$

where $1 \leq i \leq (n - 1)/2$.

Proof: The dimension of these codes is well documented and not hard to deduce (see [50, Theorem 4.1] or [15]). Alternatively the dimension of the codes could also be deduced by using Lemma 8.2.5 and Lemma 8.2.7, which are discussed later. Now the sum of the incidence vectors of the blocks defined by i disjoint duads will give a vector of C of weight $2i(n - 2i)$. Therefore we must have $i \leq \lfloor \frac{n}{2} \rfloor$ and for n even, at $i = \frac{n}{2}$, we get the zero vector. Thus for $n = 2m$ we get increasing weights from a minimum of $2(n - 2)$ up to a maximum when $i = \lfloor \frac{m}{2} \rfloor$, and the weight distribution is seen by simple counting to be as given in the statement, with distinct cases for m even and m odd. In the case of n even the minimum-weight vectors are then the incidence vectors of the blocks of the design.

If n is odd, the maximum number of disjoint duads is $\frac{n-1}{2}$, and all the weights are distinct, with a minimum when $i = \frac{n-1}{2}$, that is, weight $n - 1$. ■

Theorem 8.2.4 *For $n \geq 5$, the automorphism group of the binary code C of the triangular graph $T(n)$ is S_n unless $n = 6$, in which case the automorphism group of the code is $PGL_4(2) \cong A_8$.*

Proof: In all cases, any automorphism of the graph will define an automorphism of the design and of the code. Since the group of the complete graph is obviously S_n , and the group of its line graph is the same (by a theorem of Whitney [94]), the automorphism group of the code will contain S_n . We now use the fact that, for $n \neq 6$, the automorphism group preserves (and is transitive on) both pairs of letters of Ω and triples of letters of Ω to show that any automorphism of C induces a permutation on Ω . We can use this fact since, for $g \in G = \text{Aut}(C)$, g preserves the words of weight 3 in C^\perp , and thus for $n \neq 6$, g maps pairs of elements to pairs of elements, and triples of elements to triples of elements; this will be used to define an action of g on Ω .

Let $g \in G$. Then g is given as an element of $S_{\binom{n}{2}}$. We wish to define an action of g on Ω . Let $x \in \Omega$. For arbitrary $a, b \in \Omega$, $a, b \neq x$, suppose $g : v^{\{a,b,x\}} \mapsto v^{\{a_1,b_1,x_1\}}$. We use this to induce a map on triples of elements of Ω by $g : \{a, b, x\} \mapsto \{a_1, b_1, x_1\}$. Since g preserves incidence of points of \mathcal{D} on words of C^\perp , i.e. g preserves incidence of pairs of elements of Ω on triples, we have, without loss of generality

$$g : \begin{cases} \{a, b, x\} & \mapsto \{a_1, b_1, x_1\} \\ \{a, b\} & \mapsto \{a_1, b_1\} \\ \{a, x\} & \mapsto \{a_1, x_1\} \\ \{b, x\} & \mapsto \{b_1, x_1\} \end{cases}$$

To preserve incidence then we will attempt to define g on Ω by $g : \{a, x\} \cap \{b, x\} \mapsto \{a_1, x_1\} \cap \{b_1, x_1\}$, that is, $g : x \mapsto x_1$ (and $a \mapsto a_1$, $b \mapsto b_1$).

We need to check that this is indeed well-defined. Take first another triple of the form $\{a, c, x\}$ where $c \neq b$. Since $g : \{a, x\} \mapsto \{a_1, x_1\}$ we must have $\{a_1, x_1\}$ incident with $(\{a, c, x\})^g$, and thus $g : \{a, c, x\} \mapsto \{a_1, c_1, x_1\}$. Thus $g : \{c, x\} \mapsto \{c_1, x_1\}$ or $\{a_1, c_1\}$. Suppose $g : \{c, x\} \mapsto \{a_1, c_1\}$ and so also $g : \{a, c\} \mapsto \{x_1, c_1\}$. Then $(\{b, c, x\})^g$ must contain b_1, x_1, a_1, c_1 , and so we must have $b_1 = c_1$. But then $(\{a, b, x\})^g = \{a_1, b_1, x_1\} = \{a_1, c_1, x_1\} = (\{a, c, x\})^g$,

which is impossible since g is a permutation on triples. Thus $g : \{c, x\} \mapsto \{x_1, c_1\}$ and again we get $g : x \mapsto x_1$, and $g : c \mapsto c_1$. If we now take any triple $\{x, y, z\}$ containing x , we look first at $\{a, y, x\}$ as above, and then $\{z, y, x\}$ and have $g : x \mapsto x_1$, as required. Thus g is defined in S_n , and $\text{Aut}(C) = S_n$.

In case $n = 6$, there are more words of weight 3 in C^\perp , so we cannot use this argument since we cannot assume that the vectors of the form $v^{\{a,b,c\}}$ are mapped to one another. In this case C is a $[15, 4, 8]_2$ code and its dual is a $[15, 11, 3]_2$ code. By Theorem 3.1.10 a generator matrix for C must thus have every pair of columns linearly independent, that is distinct, and thus C is the dual of the Hamming code of length 15. Its automorphism group is well known to be $PGL_4(2)$ (see also Theorem 6.3.1). ■

Now we look for bases of minimum-weight vectors for C and C^\perp . Clearly if n is even then C has a basis of minimum-weight vectors since the incidence vectors of the blocks are the minimum-weight vectors and span C by definition.

Lemma 8.2.5 *Let $\Omega = \{a_1, a_2, \dots, a_n\}$. The set of $n - 1$ vectors*

$$\mathcal{S} = \{ v^{\overline{\{a_i, a_{i+1}\}}} \mid 1 \leq i \leq n - 1 \}$$

is a spanning set for C . For n odd \mathcal{S} is a basis; for n even $\mathcal{S} \setminus \{ v^{\overline{\{a_{n-1}, a_n\}}} \}$ is a basis of minimum-weight vectors.

Proof: Note that for $2 \leq i \leq n$

$$v^{\overline{\{a_1, a_i\}}} = v^{\overline{\{a_1, a_2\}}} + v^{\overline{\{a_2, a_3\}}} + \dots + v^{\overline{\{a_{i-1}, a_i\}}},$$

and thus $v^{\overline{\{a_i, a_j\}}} = v^{\overline{\{a_1, a_i\}}} + v^{\overline{\{a_1, a_j\}}}$ can be written as a sum of vectors in \mathcal{S} and thus \mathcal{S} spans C . Since for n odd this is the dimension of C , the set \mathcal{S} gives a basis for C when n is odd.

If $n = 2m$ we know that $\sum v^{\overline{\{a,b\}}} = 0$, where the sum ranges over a set of m disjoint pairs of elements of Ω . Hence for n even we have

$$v^{\overline{\{a_1,a_2\}}} + v^{\overline{\{a_2,a_3\}}} + \dots + v^{\overline{\{a_{n-1},a_n\}}} = v^{\overline{\{a_1,a_n\}}}$$

and

$$v^{\overline{\{a_1,a_n\}}} + v^{\overline{\{a_2,a_3\}}} + v^{\overline{\{a_4,a_5\}}} \dots + v^{\overline{\{a_{n-2},a_{n-1}\}}} = 0,$$

so we have a non-trivial linear relation, and the vectors in \mathcal{S} are linearly dependent.

Since

$$v^{\overline{\{a_1,a_2\}}} + v^{\overline{\{a_3,a_4\}}} + \dots + v^{\overline{\{a_{n-1},a_n\}}} = v^{\overline{\{a_2,a_3\}}} + v^{\overline{\{a_4,a_5\}}} + \dots + v^{\overline{\{a_{n-2},a_{n-1}\}}},$$

we can omit $v^{\overline{\{a_{n-1},a_n\}}}$ from the spanning set. ■

Lemma 8.2.6 *C has a basis of minimum-weight vectors.*

Proof: For n even, this follows from Lemma 8.2.5. For n odd, the minimum weight of C is $n - 1$ and there are exactly n minimum-weight vectors, which have the form, for each $a \in \Omega$,

$$w_a = \sum v^{\overline{\{a_i,a_j\}}},$$

where the sum is over a set of $\frac{n-1}{2}$ disjoint pairs of elements of $\Omega \setminus \{a\}$. Then for $a \neq b$, we can write

$$w_a + w_b = v + v^{\overline{\{b,c\}}} + v + v^{\overline{\{a,c\}}} = v^{\overline{\{a,b\}}},$$

showing that the w_a span C , and hence C is also spanned by minimum-weight vectors when n is odd. Notice that

$$\begin{aligned} \sum_{i=1}^n w_{a_i} &= (w_{a_1} + w_{a_2}) + \dots + (w_{a_{n-2}} + w_{a_{n-1}}) + w_{a_n} \\ &= v^{\overline{\{a_1,a_2\}}} + \dots + v^{\overline{\{a_{n-2},a_{n-1}\}}} + w_{a_n} \\ &= w_{a_n} + w_{a_n} = 0, \end{aligned}$$

and thus $\{w_{a_i} \mid 1 \leq i \leq n - 1\}$ is a basis for C . ■

Lemma 8.2.7 C^\perp has a basis of minimum-weight vectors for n odd, but not for n even.

Proof: Take $\Omega = \{1, 2, \dots, n\}$. For $n \neq 6$, the minimum-weight vectors of C^\perp are of the form

$$v^{\overline{\{a,b,c\}}} = v^{\{a,b\}} + v^{\{a,c\}} + v^{\{b,c\}}.$$

Let S be the following set of these vectors:

$$S = \{ v^{\overline{\{i,j,j+1\}}} \mid 1 \leq i < j \leq n-1 \}.$$

Notice that S has size $\binom{n-1}{2}$. We order the points of \mathcal{P} in the following way:

$$\{1, 2\}, \{1, 3\}, \dots, \{1, n-1\}, \{2, 3\}, \dots, \{2, n-1\}, \dots, \{n-2, n-1\}, \quad (8.4)$$

followed by the remaining points

$$\{1, n\}, \{2, n\}, \dots, \{n-1, n\}. \quad (8.5)$$

We show that for $n \neq 6$ every vector of weight 3 is in the span of S . Using the ordering of the points as given above, it will follow that the vectors in S span a space of dimension $\binom{n-1}{2} = \binom{n}{2} - (n-1)$. Thus for n odd the span of S is the dual code C^\perp , while for n even it is not. In the even case the all-one vector \mathbf{j} needs to be adjoined. If this is done at the bottom of the generator matrix for C^\perp then the points from Equation (8.5) up to $\{n-2, n\}$ can be taken as the last $n-2$ coordinates, while the position corresponding to $\{n-1, n\}$ can be placed in front of this set.

For this, we have, for $1 \leq i < j < j+1 < k \leq n$,

$$v^{\overline{\{i,j,k\}}} = v^{\overline{\{i,j,j+1\}}} + v^{\overline{\{i,j+1,k\}}} + v^{\overline{\{j,j+1,k\}}},$$

and induction will show that every vector of the form $v^{\overline{\{i,j,k\}}}$ is in the span of S . Further, ordering the points as given, and the vectors of S in the same way, by

the smallest two elements, produces an upper triangular matrix which clearly has the rank given above. ■

In Chapter 10 we use the codes considered in this chapter for permutation decoding and give explicit PD-sets for some of the infinite families.

Chapter 9

Binary Codes from Graphs on Triples

9.1 Introduction

In this chapter, given a set Ω of size n and $\Omega^{\{3\}}$ the set of subsets of Ω of size 3, we examine the binary codes obtained from the adjacency matrix of each of the three graphs with vertex set $\Omega^{\{3\}}$, with adjacency defined by two vertices as 3-sets being adjacent if they have zero, one or two elements in common, respectively.

The binary codes formed from the span of the adjacency matrix of graphs, and in particular strongly regular graphs, have been examined in Chapter 8 and by various authors: see [15, 16, 92, 50, 3, 4]. Here we examine a different class of graphs and prove the following theorem:

Theorem 9.1.1 *Let Ω be a set of size n , where $n \geq 7$. Let $\mathcal{P} = \Omega^{\{3\}}$, the set of subsets of Ω of size 3, be the vertex set of the three graphs $A_i(n)$, for $i = 0, 1, 2$, with adjacency defined by two vertices (as 3-sets) being adjacent if the 3-sets meet in zero, one or two elements, respectively. Let $C_i(n)$ denote the code formed from*

the row span over \mathbb{F}_2 of an adjacency matrix for $A_i(n)$. Then

1. $n \equiv 0 \pmod{4}$:

$$(a) C_2(n) = \mathbb{F}_2^{\binom{n}{3}};$$

(b) $C_0(n) = C_1(n)$ is a $[\binom{n}{3}, \binom{n}{3} - n, 4]_2$ code, and $C_0(n)^\perp$ is a $[\binom{n}{3}, n, \binom{n-1}{2}]_2$ code;

$$(c) C_i(n) \cap C_i(n)^\perp = \{0\} \text{ for } i = 0, 1, 2;$$

2. $n \equiv 2 \pmod{4}$:

$$C_i(n) = \mathbb{F}_2^{\binom{n}{3}} \text{ for } i = 0, 1, 2;$$

3. $n \equiv 1 \pmod{4}$:

$$(a) C_0(n) = C_1(n) \cap C_2(n);$$

(b) i. $C_0(n)$ is a $[\binom{n}{3}, \binom{n}{3} - \binom{n}{2}, 8]_2$ code and $C_0(n)^\perp$ is a $[\binom{n}{3}, \binom{n}{2}, n - 2]_2$ code;

ii. $C_1(n)$ is, for $n > 9$, a $[\binom{n}{3}, \binom{n}{3} - n + 1, 4]_2$ code and $C_1(n)^\perp$ is a $[\binom{n}{3}, n - 1, (n - 2)(n - 3)]_2$ code, while $C_1(9)$ is a $[84, 76, 3]_2$ and $C_1(9)^\perp$ is a $[84, 8, 38]_2$ code ;

iii. $C_2(n)$ is a $[\binom{n}{3}, \binom{n-1}{3}, 4]_2$ code and $C_2(n)^\perp$ is a $[\binom{n}{3}, \binom{n-1}{2}, n - 2]_2$ code;

$$(c) C_i(n) \cap C_i(n)^\perp = \{0\} \text{ for } i = 0, 1, 2;$$

4. $n \equiv 3 \pmod{4}$:

$$(a) C_1(n) = \langle v^P + j \mid P \in \mathcal{P} \rangle \text{ of dimension } \binom{n}{3} - 1;$$

(b) $C_0(n) = C_2(n)$ is a $[\binom{n}{3}, \binom{n-1}{3}, 4]_2$ code, and $C_2(n)^\perp$ is a $[\binom{n}{3}, \binom{n-1}{2}, n - 2]_2$ code;

$$(c) C_i(n) \cap C_i(n)^\perp = \{0\} \text{ for } i = 0, 1, 2.$$

Furthermore, the automorphism groups of these codes are S_n or $S_{\binom{n}{3}}$

The theorem will follow from a series of lemmas and propositions proved in Section 9.2.

9.2 The binary codes

Let n be any integer and Ω of size n , and to avoid degenerate cases, we take $n \geq 7$. Taking the set $\Omega^{\{3\}}$ to be the set of all 3-element subsets of Ω , we define three non-trivial undirected graphs with vertex set $\mathcal{P} = \Omega^{\{3\}}$, and denote these graphs by $A_i(n)$ where $i = 0, 1, 2$. The edges of the graph $A_i(n)$ are defined by the rule that **two vertices are adjacent in $A_i(n)$** if as 3-element subsets they have exactly i elements of Ω in common. For each $i = 0, 1, 2$ we define from $A_i(n)$ a 1-design $\mathcal{D}_i(n)$, on the point set \mathcal{P} by defining for each point $P = \{a, b, c\} \in \mathcal{P}$ a block $\overline{\{a, b, c\}}_i$ by

$$\overline{\{a, b, c\}}_i = \{ \{x, y, z\} \mid |\{x, y, z\} \cap \{a, b, c\}| = i \}.$$

Denote by $\mathcal{B}_i(n)$ the block set of $\mathcal{D}_i(n)$, so that each of these is a symmetric 1-design on $\binom{n}{3}$ points with block size, respectively:

- $\binom{n-3}{3}$ for $\mathcal{D}_0(n)$;
- $3\binom{n-3}{2}$ for $\mathcal{D}_1(n)$;
- $3(n-3)$ for $\mathcal{D}_2(n)$.

The incidence vector of the block $\overline{\{a, b, c\}}_i$ for $i = 0, 1, 2$, respectively, is then

$$v_{\overline{\{a, b, c\}}_0} = \sum_{x, y, z \in \Omega \setminus \{a, b, c\}} v^{\{x, y, z\}}; \quad (9.1)$$

$$v_{\overline{\{a, b, c\}}_1} = \sum_{x, y \in \Omega \setminus \{a, b, c\}} v^{\{a, x, y\}} + \sum_{x, y \in \Omega \setminus \{a, b, c\}} v^{\{b, x, y\}} + \sum_{x, y \in \Omega \setminus \{a, b, c\}} v^{\{c, x, y\}}; \quad (9.2)$$

$$v_{\overline{\{a, b, c\}}_2} = \sum_{x \in \Omega \setminus \{a, b, c\}} v^{\{a, b, x\}} + \sum_{x \in \Omega \setminus \{a, b, c\}} v^{\{a, c, x\}} + \sum_{x \in \Omega \setminus \{a, b, c\}} v^{\{b, c, x\}}. \quad (9.3)$$

where, as usual with the notation from [3], the incidence vector of the subset $X \subseteq \mathcal{P}$ is denoted by v^X . Since our points here are actually triples of elements from Ω , we emphasize that we are using the notation $v^{\{a, b, c\}}$ instead of the more cumbersome $v^{\{\{a, b, c\}\}}$, as mentioned in [3].

We will be examining the binary codes of these designs; in fact, computation with Magma [11] shows that the codes over some other primes, in particular, $p = 3$, might be interesting, but here we consider only the binary codes. Thus, denoting the block set of $\mathcal{D}_i(n)$ by $\mathcal{B}_i(n)$ we will write

$$C_i(n) = C_2(\mathcal{D}_i(n)) = \langle v^B \mid B \in \mathcal{B}_i(n) \rangle,$$

where the span is taken over \mathbb{F}_2 . Notice that, since the blocks of the three designs do not overlap, we have, for any point $P = \{a, b, c\}$,

$$j = v^{\{a, b, c\}} + v_{\overline{\{a, b, c\}}_0} + v_{\overline{\{a, b, c\}}_1} + v_{\overline{\{a, b, c\}}_2}. \quad (9.4)$$

Now consider, for any given point $P = \{a, b, c\} \in \mathcal{P}$, the vector

$$w_P = \sum_{P \in B_i} v^{B_i}, \quad (9.5)$$

that is, the sum of all the incidence vectors of blocks of $\mathcal{D}_i(n)$ that contain P , for each $i = 0, 1, 2$. For any point Q of \mathcal{P} , $w_P(Q)$ (the coordinate of w_P at Q) is determined by four distinct cases, depending on the size of the intersection of the triples that define P and Q . We look at the various cases, writing B_i for a block of $\mathcal{D}_i(n)$:

- $i = 0$;

1. $P = Q$, $w_P(P) = |B_0| = \binom{n-3}{3}$;
2. $|P \cap Q| = 2$, $w_P(Q) = \binom{n-4}{3}$, and there are $3(n-3)$ such points;
3. $|P \cap Q| = 1$, $w_P(Q) = \binom{n-5}{3}$, and there are $3\binom{n-3}{2}$ such points;
4. $|P \cap Q| = 0$, $w_P(Q) = \binom{n-6}{3}$, and there are $\binom{n-3}{3}$ such points.

- $i = 1$;

1. $P = Q$, $w_P(P) = |B_1| = 3\binom{n-3}{2}$;
2. $|P \cap Q| = 2$, $w_P(Q) = 2\binom{n-4}{2} + (n-4)$, and there are $3(n-3)$ such points;
3. $|P \cap Q| = 1$, $w_P(Q) = \binom{n-5}{2} + 4(n-5)$, and there are $3\binom{n-3}{2}$ such points;
4. $|P \cap Q| = 0$, $w_P(Q) = 9(n-6)$, and there are $\binom{n-3}{3}$ such points.

- $i = 2$;

1. $P = Q$, $w_P(P) = |B_2| = 3(n-3)$;
2. $|P \cap Q| = 2$, $w_P(Q) = (n-4)$, and there are $3(n-3)$ such points;
3. $|P \cap Q| = 1$, $w_P(Q) = 0$, and there are $3\binom{n-3}{2}$ such points;
4. $|P \cap Q| = 0$, $w_P(Q) = 0$, and there are $\binom{n-3}{3}$ such points.

Congruences modulo 4 give different properties of the binary codes of the designs, as the lemmas to follow will show.

As a direct consequence of the observations above for w_P we have:

Lemma 9.2.1 *With notation as defined above, $P = \{a, b, c\} \in \mathcal{P}$,*

1. $n \equiv 0 \pmod{4}$:

- (a) for $i = 0$, $w_P = v^{\overline{\{a,b,c\}}_1}$, so $C_1(n) \subseteq C_0(n)$;
- (b) for $i = 1$, $w_P = v^{\overline{\{a,b,c\}}_1}$;
- (c) for $i = 2$, $w_P = v^P$, so $C_2(n) = \mathbb{F}_2^{\binom{n}{2}}$.
2. $n \equiv 2 \pmod{4}$: for $i = 0, 1, 2$, $w_P = v^P$, so $C_i(n) = \mathbb{F}_2^{\binom{n}{3}}$.
3. $n \equiv 1 \pmod{4}$:
- (a) for $i = 0$, $w_P = v^{\overline{\{a,b,c\}}_0}$;
- (b) for $i = 1$, $w_P = v^{\{a,b,c\}} + v^{\overline{\{a,b,c\}}_0} + v^{\overline{\{a,b,c\}}_2}$, and $\mathbf{j} \in C_1(n)$;
- (c) for $i = 2$, $w_P = v^{\overline{\{a,b,c\}}_2}$.
4. $n \equiv 3 \pmod{4}$:
- (a) for $i = 0$, $w_P = v^{\overline{\{a,b,c\}}_2}$, so $C_2(n) \subseteq C_0(n)$;
- (b) for $i = 1$, $w_P = v^{\overline{\{a,b,c\}}_0} + v^{\overline{\{a,b,c\}}_1} + v^{\overline{\{a,b,c\}}_2}$, $w_P = \mathbf{j} + v^{\{a,b,c\}}$;
- (c) for $i = 2$, $w_P = v^{\overline{\{a,b,c\}}_2}$.

Proof: Follows directly from the observations and Equation (9.4) ■ .

Proposition 9.2.2 For $n \geq 7$ and odd, $C_2(n)$ is a $[(\binom{n}{3}, \binom{n-1}{3}, 4)]_2$ code and $C_2(n)^\perp$ is a $[(\binom{n}{3}, \binom{n-1}{2}, n-2)]_2$ code. There are $\binom{n}{4}$ words of weight 4 in $C_2(n)$ and they span the code; there are $\binom{n}{2}$ words of weight $n-2$ in $C_2(n)^\perp$ and they span the code. Furthermore, $C_2(n) \cap C_2(n)^\perp = \{0\}$.

For n odd $\text{Aut}(C_2(n)) = S_n$. For n even, $\text{Aut}(C_2(n)) = S_{\binom{n}{3}}$.

Proof: Since we deal exclusively with $i = 2$ in this proof, we will denote a block of $\mathcal{D}_2(n)$ by $\overline{\{a,b,c\}}$, and write $C = C_2(n)$.

For $\Delta = \{a,b,c,d\}$ any subset of Ω of four elements, let

$$w(a,b,c,d) = v^{\{a,b,c\}} + v^{\{a,b,d\}} + v^{\{a,c,d\}} + v^{\{b,c,d\}}. \quad (9.6)$$

We claim that

$$w(a, b, c, d) = v(\overline{a,b,c}) + v(\overline{a,b,d}) + v(\overline{a,c,d}) + v(\overline{b,c,d}).$$

Because

$$\begin{aligned} v(\overline{a,b,c}) &= \sum_{x \neq c} v\{a,b,x\} + \sum_{x \neq b} v\{a,c,x\} + \sum_{x \neq a} v\{b,c,x\} \\ v(\overline{a,b,d}) &= \sum_{x \neq d} v\{a,b,x\} + \sum_{x \neq b} v\{a,d,x\} + \sum_{x \neq a} v\{b,d,x\} \\ v(\overline{a,c,d}) &= \sum_{x \neq d} v\{a,c,x\} + \sum_{x \neq c} v\{a,d,x\} + \sum_{x \neq a} v\{c,d,x\} \\ v(\overline{b,c,d}) &= \sum_{x \neq d} v\{b,c,x\} + \sum_{x \neq c} v\{b,d,x\} + \sum_{x \neq b} v\{c,d,x\}, \end{aligned}$$

and so $v(\overline{a,b,c}) + v(\overline{a,b,d}) + v(\overline{a,c,d}) + v(\overline{b,c,d}) = v\{a,b,d\} + v\{a,c,d\} + v\{b,c,d\} + v\{a,b,c\} + v\{a,c,d\} + v\{b,c,d\} + v\{a,b,c\} + v\{a,b,d\} + v\{b,c,d\} + v\{a,b,c\} + v\{a,b,d\} + v\{a,c,d\} = v\{a,b,c\} + v\{a,b,d\} + v\{a,c,d\} + v\{b,c,d\} = w(a, b, c, d)$ and hence $w(a, b, c, d) \in C$.

Clearly there are $\binom{n}{4}$ of such words, and the minimum weight of C is at most 4.

Furthermore,

$$\begin{aligned} \sum_{x \in \Omega \setminus \{a,b,c\}} w(a, b, c, x) &= \sum_{x \in \Omega \setminus \{a,b,c\}} v\{a,b,c\} + \sum_{x \neq c} v\{a,b,x\} + \sum_{x \neq b} v\{a,c,x\} \\ &\quad + \sum_{x \neq a} v\{b,c,x\} \\ &= (n-3) v\{a,b,c\} + v(\overline{a,b,c}) \\ &= 0 + v(\overline{a,b,c}), \end{aligned}$$

and thus $C = \langle w(a, b, c, d) \mid a, b, c, d \in \Omega \rangle$.

Now we consider the dual code C^\perp . For any pair of elements $a, b \in \Omega$, define

$$w(a, b) = \sum_{x \in \Omega \setminus \{a,b\}} v\{a,b,x\}. \quad (9.7)$$

The weight of $w(a, b)$ is clearly $n - 2$; we show it is in C^\perp . For any $\overline{\{x, y, z\}} \in \mathcal{B}_2$, writing $w = w(a, b)$,

$$(w, \overline{v^{\{x, y, z\}}}) = (w, \sum_{c \neq x, y, z} v^{\{x, y, c\}}) + (w, \sum_{c \neq x, y, z} v^{\{x, z, c\}}) + (w, \sum_{c \neq x, y, z} v^{\{y, z, c\}}).$$

If $a, b \notin \{x, y, z\}$ then all three terms are 0; if $x = a$ and $b \notin \{x, y, z\}$, the first and second terms are 1, the last term is 0, and hence the sum is 0; if $a, b \in \{x, y, z\}$, then the first term is $n - 3 = 0$, and the other two terms are 0, so the sum is 0 again. Thus $w(a, b) \in C^\perp$, and clearly there are $\binom{n}{2}$ vectors of this type.

Now we show that this is the minimum weight of C^\perp and that these are the minimum-weight vectors. Suppose $w \in C^\perp$, and suppose that $v^{\{a, b, c\}}$ is in the support of w . Since $(w, w(a, b, c, d)) = 0$ for all choices of $d \in \Omega \setminus \{a, b, c\}$, and $w(a, b, c, d)$ and $w(a, b, c, e)$ have only $v^{\{a, b, c\}}$ in common in their supports, for each $d \in \Omega \setminus \{a, b, c\}$ we get another term in w , and thus its weight is at least $1 + (n - 3) = n - 2$.

To show that any vector in C^\perp of weight $n - 2$ has this form, suppose $w \in C^\perp$ has weight $n - 2$. Then $(w, w(a, b, c, d)) = 0$ implies that $w = v^{\{a, b, c\}} + v^{\{a, b, d\}} + \dots$. Since $(w, w(a, b, c, x)) = 0$ for all choices of $x \in \Omega \setminus \{a, b, c, d\}$, w has another element from $w(a, b, c, x)$ for each such x , so

$$w = v^{\{a, b, c\}} + v^{\{a, b, d\}} + \begin{cases} v^{\{a, b, e\}} + v^{\{a, b, f\}} + \dots + v^{\{a, b, n\}} \\ v^{\{b, c, e\}} + v^{\{b, c, f\}} + \dots + v^{\{b, c, n\}} \\ v^{\{a, c, e\}} + v^{\{a, c, f\}} + \dots + v^{\{a, c, n\}} \end{cases}$$

for one of these cases. The top case is $w(a, b)$; if one of the other cases hold then $v^{\{a, b, x\}}$ is not in the support for some x , which will give a contradiction unless the weight is greater than $n - 2$.

To show that 4 is the minimum weight of C , notice that the block size for $\mathcal{D}_2(n)$ is $3(n - 3)$, which is even; thus $\mathbf{j} \in C^\perp$ and hence all words of C have even weight. We need then to show that C does not have words of weight 2. Suppose

$w = v^{\{a,b,c\}} + v^{\{d,e,f\}}$; then since $(w, w(a, b)) = 0$, we must have $\{a, b\} \subset \{d, e, f\}$, and $w = v^{\{a,b,c\}} + v^{\{a,b,d\}}$, where $d \neq c$. But then $(w, w(a, c)) \neq 0$, so we have a contradiction, and C cannot have vectors of weight 2. Now suppose C has a vector w of weight 4 that is not of the form $w(a, b, c, d)$. If $w = v^{\{a,b,c\}} + \dots$ then $(w, w(a, b)) = 0$ implies that $w = v^{\{a,b,c\}} + v^{\{a,b,d\}} + \dots$. But we also have $(w, w(b, c)) = 0$, so $w = v^{\{a,b,c\}} + v^{\{a,b,d\}} + v^{\{b,c,e\}} + \dots$. Now similarly arguing that $(w, w(b, d)) = (w, w(a, c)) = 0$, and assuming the weight of w is 4, we find that $d = e$ and $w = w(a, b, c, d)$.

Now we show that the dimension of C is $\binom{n-1}{3}$. For this we construct a basis of words of weight 4. We introduce an ordering of the points and the spanning weight-4 vectors so that the generating matrix is in upper triangular form.

For the point order: $\{1, 2, 3\}, \{1, 2, 4\}, \dots, \{1, 2, n-1\}, \{1, 3, 4\}, \dots, \{1, 3, n-1\}, \dots, \{1, n-2, n-1\}, \{2, 3, 4\}, \dots, \{n-3, n-2, n-1\}$ (which will all be pivot positions), and followed by the remaining $\binom{n-1}{2}$ points $\{1, 2, n\}, \{1, 3, n\}, \dots, \{n-2, n-1, n\}$.

The weight-4 vectors for the basis will be ordered as follows:

$$\begin{aligned} &w(1, 2, 3, 4), w(1, 2, 4, 5), w(1, 2, 5, 6), \dots, w(1, 2, n-1, n), w(1, 3, 4, 5), \dots, \\ &w(1, 3, n-1, n), \dots, w(1, n-2, n-1, n), w(2, 3, 4, 5), w(2, 3, 5, 6), \dots, \\ &w(2, 3, n-1, n), \dots, w(n-3, n-2, n-1, n). \end{aligned}$$

Then it is simple to verify that with this ordering of points and spanning vectors we get an upper triangular matrix of rank $\binom{n-1}{3}$. Thus C has dimension at least $\binom{n-1}{3}$.

To prove that this is in fact the dimension, we look at C^\perp . We can keep the same ordering of the points but we will in fact get the pivot positions in the last $\binom{n-1}{2}$ positions. For the rows of the generating matrix $\bar{\mathcal{G}}$ we take the minimum vectors $w(1, 2), w(1, 3), \dots, w(1, n-1), w(2, 3), \dots, w(2, n-1), w(n-2, n-1)$; then $\bar{\mathcal{G}}$ has the form $[A|I_k]$ where $k = \binom{n-1}{2}$. Thus C^\perp has dimension at least

$\binom{n-1}{2} = \binom{n}{3} - \binom{n-1}{3}$, and the proposition is proved.

To show that $C \cap C^\perp = \{0\}$, we show that $C + C^\perp = \mathbb{F}_2^{\binom{n}{3}}$ by showing that every vector of weight 1 can be expressed as a sum of vectors from C and C^\perp . In fact, if $a, b, c \in \Omega$ are distinct, then

$$\begin{aligned} w(a, b) + w(a, c) + w(b, c) + v^{\overline{\{a, b, c\}}} &= \sum_{x \in \Omega \setminus \{a, b\}} v^{\{a, b, x\}} + \sum_{x \in \Omega \setminus \{a, c\}} v^{\{a, c, x\}} + \\ &\sum_{x \in \Omega \setminus \{b, c\}} v^{\{b, c, x\}} + \sum_{x \in \Omega \setminus \{a, b, c\}} v^{\{a, b, x\}} + \sum_{x \in \Omega \setminus \{a, b, c\}} v^{\{a, c, x\}} + \sum_{x \in \Omega \setminus \{a, b, c\}} v^{\{b, c, x\}} \\ &= v^{\{a, b, x\}} + v^{\{a, b, x\}} + v^{\{a, b, x\}} = v^{\{a, b, x\}}, \end{aligned}$$

which is what is required.

Finally we obtain the automorphism group of $C_2(n)$. It is not difficult to see that $\text{Aut}(A_2(n)) = S_n$ and $S_n \subseteq \text{Aut}(C_2(n))$. Let $g \in \text{Aut}(C_2(n))$. Then g maps triples to triples. Also since the words having the form $w(a, b) = \sum_{x \in \Omega \setminus \{a, b\}} v^{\{a, b, x\}}$ are the words of minimum weight $n - 2$ in $C_2(n)^\perp$, g maps pairs to pairs. We use these facts to show that $\text{Aut}(C_2(n)) = S_n$.

Let $x \in \Omega$. For arbitrary $a, b \in \Omega$ such that $x \in \Omega \setminus \{a, b\}$, suppose that $\{a, b\}^g = \{c, d\}$. Then $\{a, b, x\}^g = \{c, d, x^*\}$ where $x^* \notin \{c, d\}$. Without loss of generality we may assume that $\{a, x\}^g = \{c, x^*\}$. Then we must have $\{b, x\}^g = \{d, x^*\}$.

Now consider $e, f \in \Omega \setminus \{a, b, c, d, x\}$. Then $\{a, e, x\}^g = \{c, x^*, e^*\}$ where $e^* \notin \{c, x^*\}$. This provides two possible images for $\{e, x\}$, namely

$$\{e, x\}^g = \{c, e^*\} \text{ or } \{e, x\}^g = \{x^*, e^*\}$$

If $\{e, x\}^g = \{c, e^*\}$, then we must have $\{a, e\}^g = \{x^*, e^*\}$ which implies $\{b, e, x\}^g = \{c, x^*, e^*, d\}$, a contradiction. Hence we must have $\{e, x\}^g = \{x^*, e^*\}$ which implies $\{a, e\}^g = \{c, e^*\}$. Thus $\{b, e, x\}^g = \{d, x^*, e^*\}$ and we deduce that $\{b, e\}^g = \{d, e^*\}$. Hence $\{a, b, e\}^g = \{c, d, e^*\}$.

Now assume that $\{a, f, x\}^g = \{c, x^*, f^*\}$ where $f^* \notin \{c, x^*\}$. Then similarly to the above argument we get $\{a, f\}^g = \{c, f^*\}$ and $\{f, x\}^g = \{x^*, f^*\}$. Hence $\{b, f, x\}^g = \{d, x^*, f^*\}$ and $\{e, f, x\}^g = \{e^*, x^*, f^*\}$. Finally we deduce that $\{e, f\}^g = \{e^*, f^*\}$.

From the above we deduce that g is defined in S_n and $\text{Aut}(C_2(n)) = S_n$. For n even $C_2(n) = \mathbb{F}_2^{\binom{n}{3}}$ and hence the result. ■

Lemma 9.2.3 *For all $n \geq 7$ $C_0(n)$ has words of weight 8. If n is odd, $w(a, b) = \sum_{x \in \Omega \setminus \{a, b\}} v^{\{a, b, x\}} \in C_0(n)^\perp$, and $C_0(n) \subseteq C_2(n)$. If $n \equiv 3 \pmod{4}$, $C_0(n) = C_2(n)$.*

Proof: We first show how words of weight 8 can be constructed. In this lemma we use the notation $\overline{\{a, b, c\}}$ to denote a block of $\mathcal{D}_0(n)$.

Let $\Delta = \{a, b, c, d, e, f\}$ be a subset of Ω of six elements. For each partition of Δ into three disjoint 2-element subsets we will get a weight-8 vector. The set Δ will be the point set of a 1-(6, 3, 4) design with $\lambda_2 = 2$ or 0. We do this as follows: suppose we take the partition $\pi = \{\{a, b\}, \{c, d\}, \{e, f\}\}$ of Δ , then the rule for our design will be that points from the same 2-element subset will not be together in a block. The eight blocks will thus be:

$$B_1 = \{a, c, e\}, B_2 = \{a, c, f\}, B_3 = \{a, d, e\}, B_4 = \{a, d, f\}$$

and their complements

$$B_5 = \{b, d, f\}, B_6 = \{b, d, e\}, B_7 = \{b, c, f\}, B_8 = \{b, c, e\}.$$

It is then a direct matter to prove that

$$w(\pi) = \sum_{i=1}^8 v^{B_i} = \sum_{i=1}^8 v^{\overline{B_i}}, \quad (9.8)$$

thus giving a vector of weight 8 in $C_0(n)$.

Now take n to be odd, and consider

$$(w(a, b), v^{\overline{\{x, y, z\}}}) = \left(\sum_{x \in \Omega \setminus \{a, b\}} v^{\{a, b, x\}}, \sum_{c, d, e \in \Omega \setminus \{x, y, z\}} v^{\{c, d, e\}} \right) = m.$$

Then

- $m = 0$ if $\{a, b\} \subseteq \{x, y, z\}$;
- $m = 0$ if $a \in \{x, y, z\}$ and $b \notin \{x, y, z\}$;
- if $\{a, b\} \cap \{x, y, z\} = \emptyset$, then $v^{\{a, b, c\}}$ is in the support of $v^{\overline{\{x, y, z\}}}$ except for $c = x, y, z$. Thus they meet in $n - 2 - 3 = n - 5$ positions, so that $m = 0$ for n odd.

Since from Proposition 9.2.2 we have that $C_2(n)^\perp = \langle w(a, b) \mid a, b \in \Omega \rangle$, we have now shown that $C_2(n)^\perp \subseteq C_0(n)^\perp$ for n odd, and thus $C_0(n) \subseteq C_2(n)$ for n odd. That equality holds here if $n \equiv 3 \pmod{4}$ follows from Lemma 9.2.1(4a). ■

Lemma 9.2.4 *For $n \geq 7$, $C_1(n)$ has words of weight 4. If $n \equiv 0 \pmod{4}$ then $C_0(n)$ has words of weight 4.*

Proof: We define two types of words of $\mathbb{F}_2^{\binom{n}{3}}$ of weight 4 and show that they are in $C_1(n)$ for any $n \geq 7$.

Let $\Delta = \{a, b, c, d, e, f\} \subseteq \Omega$ of size 6, and let $\Delta^* = [a, b, c, d, e, f]$ be a sequence of the elements of Δ . Let

$$w(\Delta^*) = v^{\{a, b, c\}} + v^{\{a, b, d\}} + v^{\{c, e, f\}} + v^{\{d, e, f\}}. \quad (9.9)$$

We claim that

$$w(\Delta^*) = v^{\overline{\{a, b, c\}}} + v^{\overline{\{a, b, d\}}} + v^{\overline{\{c, e, f\}}} + v^{\overline{\{d, e, f\}}}.$$

Because

$$\begin{aligned}
 v^{\overline{\{a,b,c\}}} &= \sum_{x,y \in \Omega \setminus \{a,b,c\}} v^{\{a,x,y\}} + \sum_{x,y \in \Omega \setminus \{a,b,c\}} v^{\{b,x,y\}} + \sum_{x,y \in \Omega \setminus \{a,b,c\}} v^{\{c,x,y\}} \\
 v^{\overline{\{a,b,d\}}} &= \sum_{x,y \in \Omega \setminus \{a,b,d\}} v^{\{a,x,y\}} + \sum_{x,y \in \Omega \setminus \{a,b,d\}} v^{\{b,x,y\}} + \sum_{x,y \in \Omega \setminus \{a,b,d\}} v^{\{d,x,y\}} \\
 v^{\overline{\{c,e,f\}}} &= \sum_{x,y \in \Omega \setminus \{c,e,f\}} v^{\{c,x,y\}} + \sum_{x,y \in \Omega \setminus \{c,e,f\}} v^{\{e,x,y\}} + \sum_{x,y \in \Omega \setminus \{c,e,f\}} v^{\{f,x,y\}} \\
 v^{\overline{\{d,e,f\}}} &= \sum_{x,y \in \Omega \setminus \{d,e,f\}} v^{\{d,x,y\}} + \sum_{x,y \in \Omega \setminus \{d,e,f\}} v^{\{e,x,y\}} + \sum_{x,y \in \Omega \setminus \{d,e,f\}} v^{\{f,x,y\}}
 \end{aligned}$$

and so $v^{\overline{\{a,b,c\}}} + v^{\overline{\{a,b,d\}}} + v^{\overline{\{c,e,f\}}} + v^{\overline{\{d,e,f\}}} = v^{\{a,d,e\}} + v^{\{a,d,f\}} + v^{\{a,e,f\}} + v^{\{b,d,e\}} + v^{\{b,d,f\}} + v^{\{b,e,f\}} + v^{\{c,d,e\}} + v^{\{c,d,f\}} + v^{\{c,e,f\}} + v^{\{a,c,e\}} + v^{\{a,c,f\}} + v^{\{a,e,f\}} + v^{\{b,c,e\}} + v^{\{b,c,f\}} + v^{\{b,e,f\}} + v^{\{d,c,e\}} + v^{\{d,c,f\}} + v^{\{d,e,f\}} + v^{\{c,a,b\}} + v^{\{c,a,d\}} + v^{\{c,b,d\}} + v^{\{e,a,b\}} + v^{\{e,a,d\}} + v^{\{e,b,d\}} + v^{\{f,a,b\}} + v^{\{f,a,d\}} + v^{\{f,b,d\}} + v^{\{d,a,b\}} + v^{\{d,a,c\}} + v^{\{d,b,c\}} + v^{\{e,a,b\}} + v^{\{e,a,c\}} + v^{\{e,b,c\}} + v^{\{f,a,b\}} + v^{\{f,a,c\}} + v^{\{f,b,c\}} = v^{\{a,b,c\}} + v^{\{a,b,d\}} + v^{\{c,e,f\}} + v^{\{d,e,f\}} = w(\Delta^*)$, where our notation is for blocks of $\mathcal{D}_1(n)$ in this lemma.

Similarly, let $\Delta = \{a, b, c, d, e\} \subseteq \Omega$ of size 5, and let $\Delta^* = [a, b, c, d, e]$ be a sequence of the elements of Δ . Let

$$u(\Delta^*) = v^{\{a,b,c\}} + v^{\{a,b,d\}} + v^{\{a,c,e\}} + v^{\{a,d,e\}}. \quad (9.10)$$

Then we can show as above that

$$u(\Delta^*) = v^{\overline{\{a,b,c\}}} + v^{\overline{\{a,b,d\}}} + v^{\overline{\{a,c,e\}}} + v^{\overline{\{a,d,e\}}},$$

thus illustrating two different types of words of weight 4 in $C_1(n)$ for any n .

Since $C_1(n) \subseteq C_0(n)$ when $n \equiv 0 \pmod{4}$ (by Lemma 9.2.1 (1a)), $C_0(n)$ also has words of weight 4 in this case. ■

Note 9.2.5 *If we take the sequence $\Delta' = [a, f, c, d, e, b]$ in the first construction of Lemma 9.2.4, then*

$$w(\Delta^*) + w(\Delta') = w(\pi),$$

where $\pi = \{\{a, e\}, \{b, f\}, \{c, d\}\}$ is the partition of the set Δ as used in the construction of the weight-8 words in $C_0(n)$ in Lemma 9.2.3, and $w(\pi)$ is as defined in Equation (9.8).

Lemma 9.2.6 For $n \equiv 0 \pmod{4}$, $C_1(n)^\perp$ has n words of weight $\binom{n-1}{2}$ given, for each $a \in \Omega$, by

$$w(a) = \sum_{x,y \in \Omega \setminus \{a\}} v^{\{a,x,y\}}. \quad (9.11)$$

The same is true for $C_0(n)^\perp$ for $n \equiv 0 \pmod{4}$ and for $n \equiv 1 \pmod{4}$.

For any n , the n vectors $w(a)$ are linearly independent and $\mathbf{j} = \sum_{a \in \Omega} w(a)$; if $n \equiv 1 \pmod{4}$ then

$$S = \langle \mathbf{j} + w(a) \mid a \in \Omega \rangle \subseteq C_1(n)^\perp$$

and has dimension $n - 1$.

Proof: Let $w(a)$ be as defined, and consider first $C_1(n)^\perp$. Taking an arbitrary block of $\mathcal{D}_1(n)$, consider $(w(a), v^{\overline{\{b,c,d\}}_1}) = m$. Then we have the following two cases:

(i) Suppose that $a \notin \{b, c, d\}$. Then we have that

$$\begin{aligned} m &= \left(\sum_{x,y \neq a} v^{\{a,x,y\}}, \sum_{x,y \in \Omega \setminus \{b,c,d\}} v^{\{b,x,y\}} + \sum_{x,y \in \Omega \setminus \{b,c,d\}} v^{\{c,x,y\}} + \sum_{x,y \in \Omega \setminus \{b,c,d\}} v^{\{d,x,y\}} \right) \\ &= \left(\sum_{x,y \neq a} v^{\{a,x,y\}}, \sum_{x,y \in \Omega \setminus \{b,c,d\}} v^{\{b,x,y\}} \right) + \left(\sum_{x,y \neq a} v^{\{a,x,y\}}, \sum_{x,y \in \Omega \setminus \{b,c,d\}} v^{\{c,x,y\}} \right) \\ &\quad + \left(\sum_{x,y \neq a} v^{\{a,x,y\}}, \sum_{x,y \in \Omega \setminus \{b,c,d\}} v^{\{d,x,y\}} \right) = r + s + t, \end{aligned}$$

where

$$r = \left(\sum_{x,y \neq a} v^{\{a,x,y\}}, \sum_{x,y \in \Omega \setminus \{b,c,d\}} v^{\{b,x,y\}} \right), \quad s = \left(\sum_{x,y \neq a} v^{\{a,x,y\}}, \sum_{x,y \in \Omega \setminus \{b,c,d\}} v^{\{c,x,y\}} \right)$$

and

$$t = \left(\sum_{x,y \neq a} v^{\{a,x,y\}}, \sum_{x,y \in \Omega \setminus \{b,c,d\}} v^{\{d,x,y\}} \right), \quad \text{respectively.}$$

Now

$$\begin{aligned}
 r &= \left(\sum_{x,y \neq a} v^{\{a,x,y\}}, \sum_{x,y \in \Omega \setminus \{b,c,d\}} v^{\{b,x,y\}} \right) \\
 &= \left(\sum_{x,y \neq a} v^{\{a,x,y\}} + \sum_{x \neq a,b} v^{\{a,b,x\}}, \sum_{x,y \in \Omega \setminus \{a,b,c,d\}} v^{\{b,x,y\}} + \sum_{x \neq a,b,c,d} v^{\{a,b,x\}} \right) \\
 &= \left(\sum_{x,y \neq a} v^{\{a,x,y\}}, \sum_{x,y \in \Omega \setminus \{b,c,d\}} v^{\{b,x,y\}} \right) + \left(\sum_{x,y \neq a} v^{\{a,x,y\}}, \sum_{x,y \in \Omega \setminus \{a,b,c,d\}} v^{\{a,b,x\}} \right) \\
 &\quad + \left(\sum_{x \neq a,b} v^{\{a,b,x\}}, \sum_{x,y \in \Omega \setminus \{a,b,c,d\}} v^{\{b,x,y\}} \right) + \left(\sum_{x \neq a,b} v^{\{a,b,x\}}, \sum_{x \in \Omega \setminus \{a,b,c,d\}} v^{\{a,b,x\}} \right) \\
 &= \left(\sum_{x,y \neq a,b} v^{\{a,b,x\}}, \sum_{x \in \Omega \setminus \{a,b,c,d\}} v^{\{a,b,x\}} \right) = n - 4.
 \end{aligned}$$

Similarly we get that $s = t = n - 4$, so $m = 3(n - 4)$.

(ii) Suppose that $a \in \{b, c, d\}$ and without loss of generality assume that $a = d$.

Then

$$\begin{aligned}
 m &= \left(\sum_{x,y \neq a} v^{\{a,x,y\}}, \sum_{x,y \in \Omega \setminus \{a,b,c\}} v^{\{a,x,y\}} + \sum_{x,y \in \Omega \setminus \{a,b,c\}} v^{\{b,x,y\}} + \sum_{x,y \in \Omega \setminus \{a,b,c\}} v^{\{c,x,y\}} \right) \\
 &= \left(\sum_{x,y \neq a} v^{\{a,x,y\}}, \sum_{x,y \in \Omega \setminus \{a,b,c\}} v^{\{a,x,y\}} \right) + \left(\sum_{x,y \neq a} v^{\{a,x,y\}}, \sum_{x,y \in \Omega \setminus \{a,b,c\}} v^{\{b,x,y\}} \right) \\
 &\quad + \left(\sum_{x,y \neq a} v^{\{a,x,y\}}, \sum_{x,y \in \Omega \setminus \{a,b,c\}} v^{\{c,x,y\}} \right) = \binom{n-3}{2} = \frac{(n-3)(n-4)}{2}.
 \end{aligned}$$

Now cases (i) and (ii) imply that if $n \equiv 0 \pmod{4}$, then $m \equiv 0 \pmod{2}$ and $w(a) \in C_1(n)^\perp$. Notice that if $n \equiv 1 \pmod{4}$ then $m = 1$ for all blocks, and since the block size is odd in this case, it follows that $(j, v^{\overline{\{b,c,d\}}_1}) = 1$ and hence that $j + w(a) \in C_1(n)^\perp$.

Now consider $C_0(n)^\perp$ and let $m = (w(a), \overline{v^{b,c,d}}_0)$. Suppose that $a \notin \{b, c, d\}$, it follows that

$$\begin{aligned} m &= \left(\sum_{x,y \neq a} v^{\{a,x,y\}}, \sum_{x,y,z \in \Omega \setminus \{b,c,d\}} v^{\{x,y,z\}} \right) \\ &= \binom{n-4}{2} = \frac{(n-4)(n-5)}{2}. \end{aligned}$$

Now suppose that $a \in \{b, c, d\}$ and without loss of generality assume that $a = d$. Then we have that

$$m = \left(\sum_{x,y \neq a} v^{\{a,x,y\}}, \sum_{x,y,z \in \Omega \setminus \{a,b,c\}} v^{\{x,y,z\}} \right) = 0.$$

Thus if $n \equiv 0 \pmod{4}$ or if $n \equiv 1 \pmod{4}$, we will have $m \equiv 0 \pmod{2}$ and $w(a) \in C_0(n)^\perp$.

Clearly there are n words of this type. We now show that they are linearly independent: suppose

$$\sum_{i=1}^n a_i w(i) = 0 = \sum_{i=1}^n a_i \sum_{j,k \in \Omega \setminus \{i\}} v^{\{i,j,k\}}.$$

The coefficient of $v^{\{i,j,k\}}$ is $a_i + a_j + a_k = 0$ for every choice of the triple $\{i, j, k\}$. It follows easily that $a_i = 0$ for all i .

That $\mathbf{j} = \sum_{a \in \Omega} w(a)$ follows from the observation that each vector $v^{\{a,b,c\}}$ will occur exactly three times in the sum. For n odd then it also follows that $\sum_{a \in \Omega} (\mathbf{j} + w(a)) = 0$, completing the proof. ■

Lemma 9.2.7 *For $n \equiv 0 \pmod{4}$, $C_1(n) = C_0(n)$ and has minimum weight 4. For $n \equiv 1 \pmod{4}$, $C_0(n) \subset C_1(n)$.*

Proof: First show that the minimum weight of $C_1(n)$ is 4. Notice that the block size is $3\binom{n-3}{2}$, which is even for $n \equiv 0 \pmod{4}$, and thus $\mathbf{j} \in C_1(n)^\perp$ and all

vectors in $C_1(n)$ have even weight. We need thus only show that there are no vectors of weight 2. Suppose that $w = v^{\{a,b,c\}} + v^{\{d,e,f\}} \in C_1(n)$. Considering cases, and with $w(a)$ as in Equation 9.11,:

- if $\{a, b, c\} \cap \{d, e, f\} = \emptyset$ then $(w(a), w) = 1$;
- if $\{a, b, c\} \cap \{d, e, f\} = \{a\}$ where $a = d$, then $(w(b), w) = 1$;
- if $\{a, b, c\} \cap \{d, e, f\} = \{a, b\}$ where $a = d, e = b$, then $(w(c), w) = 1$.

This gives a contradiction for all choices of w of weight 2, so the minimum weight is 4.

To show that $C_0(n) = C_1(n)$ for $n \equiv 0 \pmod{4}$, we form the sum

$$w = \sum_{\Delta^*} w(\Delta^*)$$

of the words $w(\Delta^*)$ of Equation (9.9) over sequences from $\Delta = \{a, b, c, d, e, f\}$ where a, b, c are fixed, and d, e, f vary over the remaining triples, and $w(\Delta^*)$ has $v^{\{a,b,c\}}$ in its support. The number of sets Δ containing a, b, c is $\binom{n-3}{3}$ and each Δ gives nine distinct words $w(\Delta^*)$ with $v^{\{a,b,c\}}$ in the support. In the sum, $v^{\{a,b,c\}}$ will occur $9\binom{n-3}{3} \equiv 0 \pmod{2}$ times; each $v^{\{d,e,f\}}$, where $\{d, e, f\}$ is disjoint from $\{a, b, c\}$, will occur $9 \equiv 1 \pmod{2}$ times; each $v^{\{a,b,d\}}, v^{\{a,c,d\}}, v^{\{b,c,d\}}$ will occur once for each $\Delta \ni d$, and thus $\binom{n-4}{2} \equiv 0 \pmod{2}$ times. Each $v^{\{a,d,e\}}, v^{\{b,d,e\}}, v^{\{c,d,e\}}$ will occur once whenever $\{d, e\} \subseteq \Delta$, that is $(n-5) \equiv 1 \pmod{2}$ times. Thus the sum $w \in C_1(n)$ is

$$\sum_{d,e,f \in \Omega \setminus \{a,b,c\}} v^{\{d,e,f\}} + \sum_{d,e \in \Omega \setminus \{a,b,c\}} v^{\{a,d,e\}} + \sum_{d,e \in \Omega \setminus \{a,b,c\}} v^{\{b,d,e\}} + \sum_{d,e \in \Omega \setminus \{a,b,c\}} v^{\{c,d,e\}},$$

that is

$$w = \sum_{\Delta^*} w(\Delta^*) = v^{\overline{\{a,b,c\}}_0} + v^{\overline{\{a,b,c\}}_1},$$

which shows that $C_0(n) \subseteq C_1(n)$, and, since $C_1(n) \subseteq C_0(n)$ for $n \equiv 0 \pmod{4}$ by Lemma 9.2.1 (1a), hence they are equal.

In the case $n \equiv 1 \pmod{4}$, looking at the vector w above, all the congruences modulo 2 remain the same apart from $n - 5 \equiv 0 \pmod{2}$. Thus we get

$$w = \sum_{\Delta^*} w(\Delta^*) = v^{\overline{\{a,b,c\}}_0},$$

and hence $C_0(n) \subseteq C_1(n)$. Now by Lemma 9.2.1 (3b), $\mathbf{j} \in C_1(n)$, and by Proposition 9.2.2, $\mathbf{j} \in C_2(n)^\perp$ and hence not in $C_2(n)$, and thus not in $C_0(n)$, since by Lemma 9.2.3 $C_0(n) \subseteq C_2(n)$. Thus the containment is proper. ■

Lemma 9.2.8 *If $w(a)$ is defined as in Equation (9.11), then the full weight enumerator for*

$$S = \langle \mathbf{j} + w(a) \mid a \in \Omega \rangle$$

for $n \equiv 1 \pmod{4} \geq 9$ is given as follows: for $r = 1$ to $\frac{n-1}{2}$, S has $\binom{n}{r}$ vectors of weight

1. $r \binom{n-r}{2} + \binom{r}{3}$ if r is even;
2. $\binom{n}{3} - r \binom{n-r}{2} - \binom{r}{3}$ if r is odd.

In each case such a word has the form $\sum_{i=1}^r (\mathbf{j} + w(a_i))$ where $\Delta = \{a_1, a_2, \dots, a_r\}$ has size r . The minimum weight of S is $2 \binom{n-2}{2}$ for $n > 9$, and 38 for $n = 9$.

Proof: For Δ as in the statement of the lemma, consider

$$\begin{aligned}
 w &= \sum_{i=1}^r (\mathbf{j} + w(a_i)) \\
 &= r\mathbf{j} + \sum_{i=1}^r \sum_{x,y \neq a_i} v^{\{a_i, x, y\}} \\
 &= r\mathbf{j} + \sum_{i=1}^r \left(\sum_{x,y \in \Omega \setminus \Delta} v^{\{a_i, x, y\}} + \sum_{j \neq i} \sum_{x \in \Omega \setminus \Delta} v^{\{a_i, a_j, x\}} + \sum_{j,k \neq i} v^{\{a_i, a_j, a_k\}} \right) \\
 &= r\mathbf{j} + \sum_{i=1}^r \sum_{x,y \in \Omega \setminus \Delta} v^{\{a_i, x, y\}} + 0 + 3 \sum_{a_i, a_j, a_k \in \Delta} v^{\{a_i, a_j, a_k\}}.
 \end{aligned}$$

The formulae given now follow, where $\binom{r}{3} = 0$ if $r = 1$ or 2 .

The smallest weight occurs when $r = 2$ except when $n = 9$ when it occurs at $r = 3$. ■

Lemma 9.2.9 For $n \equiv 0 \pmod{4} \geq 8$

$$T = \langle w(a) \mid a \in \Omega \rangle \subseteq C_1(n)^\perp$$

and has weight enumerator as given in Lemma 9.2.8 together with the complements of all the words. T is a $[(\binom{n}{3}, n, \binom{n-1}{2})_2$ code.

Proof: The proof is clear from Lemma 9.2.8 and Lemma 9.2.6. ■

Lemma 9.2.10 If $D = \langle u(\Delta^*) \mid \Delta \subset \Omega \rangle$, where $u(\Delta^*)$ is given in Equation (9.10), then D has dimension at least $\binom{n}{3} - n$.

Proof: We order the points of \mathcal{P} and a specific set of the words $u(\Delta^*)$ so that the generating matrix is in upper triangular form. The point order is as follows: $\{1, 2, 3\}, \{1, 2, 4\}, \dots, \{1, 2, n\}, \{1, 3, 4\}, \dots, \{1, 3, n\}, \dots, \{1, n-2, n\}, \{2, 3, 4\}, \dots, \{2, n-2, n\}, \dots, \{n-4, n-2, n-1\}, \{n-4, n-2, n\}$, giving $\binom{n}{3} -$

n positions, followed by the remaining n points: $\{1, n-1, n\}, \{2, n-1, n\}, \dots, \{n-4, n-1, n\}, \{n-3, n-1, n\}, \{n-2, n-1, n\}, \{n-3, n-2, n-1\}, \{n-3, n-2, n\}$.

The words $u(\Delta^*)$ are ordered according to sequences of elements of Ω of five elements, and writing here, for simplicity, the sequence $[a, b, c, d, e]$ to denote the word $u([a, b, c, d, e]) = v^{\overline{\{a,b,c\}}} + v^{\overline{\{a,b,d\}}} + v^{\overline{\{a,c,e\}}} + v^{\overline{\{a,d,e\}}}$. The ordering is as follows: $[1, 2, 3, n-1, n], \dots, [1, 2, n-2, n-1, n], [n-1, 1, 2, n, n-2], [n, 1, 2, n-1, n-2], \dots, [1, n-3, n-2, n-1, n], [n-1, 1, n-3, n, n-2], [n, 1, n-3, n-1, n-2], [n-1, 1, n-2, n, n-3], [n, 1, n-2, n-1, n-3]$ giving the first $\binom{n-1}{2} - 1$ vectors; $[2, 3, 4, n-1, n], \dots, [n, 2, n-2, n-1, n-3]$ giving the next $\binom{n-2}{2} - 1$ vectors; carry on in this way until $[n-4, n-3, n-2, n-1, n], [n-1, n-4, n-3, n, n-2], [n, n-4, n-3, n-1, n-2], [n-1, n-4, n-2, n, n-3], [n, n-4, n-2, n-1, n-3]$ giving $\binom{n-(n-4)}{2} - 1 = 5$ vectors. The total number of vectors is $\sum_{i=1}^{n-4} (\binom{n-i}{2} - 1) = \binom{n}{3} - n$.

If a matrix of codewords is now formed with the points in the order given, and the rows the words $u(\Delta^*)$ in the order given, then this matrix is in upper triangular form, with $\binom{n}{3} - n$ pivot positions in the first $\binom{n}{3} - n$ positions. Thus D has at least this dimension, for any $n \geq 7$. ■

Proposition 9.2.11 1. For $n \equiv 0 \pmod{4} \geq 8$, $C_0(n) = C_1(n)$ is a $[(\binom{n}{3}), (\binom{n}{3}) - n, 4]_2$ code, and $C_0(n)^\perp = C_1(n)^\perp$ is a $[(\binom{n}{3}), n, (\binom{n-1}{2})]_2$ code with weight enumerator given in Lemma 9.2.9.

2. For $n \equiv 1 \pmod{4} \geq 13$, $C_1(n)$ is a $[(\binom{n}{3}), (\binom{n}{3}) - n + 1, 4]_2$ code, and $C_1(n)^\perp$ is a $[(\binom{n}{3}), n-1, 2\binom{n-2}{2}]_2$ code with weight enumerator given in Lemma 9.2.8. For $n = 9$, $C_1(9)$ is a $[84, 76, 3]_2$ code and $C_1(9)^\perp$ is a $[84, 8, 38]_2$ code.

For all $n \geq 7$, $C_1(n) \cap C_1(n)^\perp = \{0\}$. For $n \equiv 0 \pmod{4}$ or $n \equiv 1 \pmod{4}$, $\text{Aut}(C_1(n)) = S_n$, and for $n \equiv 2 \pmod{4}$ or $n \equiv 3 \pmod{4}$, $\text{Aut}(C_1(n)) = S_{\binom{n}{3}}$.

Proof: First take $n \equiv 0 \pmod{4}$. Then by Lemma 9.2.9, $C_1(n)^\perp$ has dimension at least n , so $C_1(n)$ has dimension at most $\binom{n}{3} - n$. From Lemma 9.2.10, we have

$D \subset C_1(n)$ of dimension at least $\binom{n}{3} - n$, and thus equality holds. The facts about the minimum weight of $C_1(n)$ and its dual then follow from Lemma 9.2.7 and Lemma 9.2.9. That $C_1(n) = C_0(n)$ was proved in Lemma 9.2.7.

Now take $n \equiv 1 \pmod{4}$. Then $\mathbf{j} \in C_1(n)$ but $\mathbf{j} \notin C_1(n)^\perp$. Clearly $\mathbf{j} \in D^\perp$, and so $D^\perp \supset C_1(n)^\perp$, and $D \subset C_1(n)$. Now the $\dim(C_1(n)^\perp) \geq \dim(S) = n - 1$, and so $\dim(C_1(n)) \leq \binom{n}{3} - n + 1$. Since $\dim(D) \geq \binom{n}{3} - n$, we have $\dim(C_1(n)) = \binom{n}{3} - n + 1$ and $C_1(n) = \langle D, \mathbf{j} \rangle$. This establishes the dimension of the code.

We have already noted the minimum weight of the dual code, since we have just proved that $S = C_1(n)^\perp$ and we can thus use Lemma 9.2.8. We need to show that the minimum weight of $C_1(n)$ is 4 unless $n = 9$, in which case we will show that it is 3. Suppose first that $w = v^{\{a,b,c\}} + v^{\{d,e,f\}} \in C_1(n)$. Then $(w, \mathbf{j} + w(i)) = 0$ for all $i \in \Omega$. Notice that $\mathbf{j} + w(i) = \mathbf{j} + \sum_{x,y \neq i} v^{\{i,x,y\}} = \sum_{x,y,z \neq i} v^{\{x,y,z\}}$. Since w is to have weight 2, there is some element a , say, not in $\{d, e, f\}$. Then $(w, \mathbf{j} + w(a)) = 1$, giving a contradiction. So there are no elements of weight 2.

Suppose $w = v^{\{a,b,c\}} + v^{\{d,e,f\}} + v^{\{g,h,i\}} \in C_1(n)$. If there is some element $j \in \Omega$ such that $j \notin \{a, b, c, d, e, f, g, h, i\}$, then $(w, \mathbf{j} + w(i)) = 3$ and we have a contradiction. This shows that 4 is the minimum weight if $n > 9$. Consider now the case $n = 9$. We show that if $\Omega = \{a, b, c, d, e, f, g, h, i\}$, then $w \in C_1(9)$. Recall from Lemma 9.2.1 (3b), that $w_P = v^{\{a,b,c\}} + v^{\overline{\{a,b,c\}}_0} + v^{\overline{\{a,b,c\}}_2}$ where w_P is the sum of all the incidence vectors of blocks of $\mathcal{D}_1(n)$ containing the point $P = \{a, b, c\}$. If we form the vector $u = w_{\{a,b,c\}} + w_{\{d,e,f\}} + w_{\{g,h,i\}}$, it is quite direct to show that $u = w$. Thus the minimum weight is 3 when $n = 9$.

Now we show that $C_1(n) + C_1(n)^\perp = \mathbb{F}_2^{\binom{n}{3}}$ for $n \equiv 0 \pmod{4}$ and $n \equiv 1 \pmod{4}$ since it already follows for other n . For this, let $P = \{a, b, c\}$ be any point and consider $w = w(a) + w(b) + w(c) + v^{\overline{\{a,b,c\}}_1} \in C_1(n) + C_1(n)^\perp$ for $n \equiv 0 \pmod{4}$, and $u = (\mathbf{j} + w(a)) + (\mathbf{j} + w(b)) + (\mathbf{j} + w(c)) + (\mathbf{j} + v^{\overline{\{a,b,c\}}_1}) \in C_1(n) + C_1(n)^\perp$ for $n \equiv 1 \pmod{4}$. It is immediate that $w = u = v^{\{a,b,c\}}$, which

establishes the result.

To prove the stated results about the automorphism groups, if $n \equiv 0 \pmod{4}$, then by Lemma 9.2.6, $\{w(a) \mid a \in \Omega\}$ is the set of words of weight $\binom{n-1}{2}$ in $C_1(n)^\perp$. Hence if $\alpha \in \text{Aut}(C_1(n)^\perp)$, then $\alpha(w(a)) = w(b)$ and since $w(a) = w(b)$ if and only if $a = b$, we deduce that α is defined in S_n and hence $\text{Aut}(C_1(n)) = S_n$.

Now assume that $n \equiv 1 \pmod{4}$. Then for $n \geq 13$, $C_1(n)^\perp$ has minimum weight $2\binom{n-1}{2}$. The set

$$\{j + w(a) + j + w(b) \mid a, b \in \Omega, a \neq b\} = \{w(a) + w(b) \mid a, b \in \Omega, a \neq b\}$$

is the set of all vectors of minimum weight (this follows from Lemma 9.2.8 and the fact that $S = C_1(n)^\perp$). Using the definition of $w(a)$, it is easy to see that

$$w(a) + w(b) = \sum_{x, y \in \Omega \setminus \{a, b\}} (v^{\{a, x, y\}} + v^{\{b, x, y\}}).$$

Now it is clear that $w(a) + w(b) = w(c) + w(d)$ if and only if $\{a, b\} = \{c, d\}$. So we deduce that if $\alpha \in \text{Aut}(C_1(n))$, then α maps pairs to pairs. Now the proof follows similarly to the proof in Proposition 9.2.2. For $n = 9$, direct computations with Magma show that $\text{Aut}(C_1(9)) = S_9$.

For $n \equiv 2 \pmod{4}$, $C_1(n) = \mathbb{F}_2^{\binom{n}{3}}$ and hence the result. For $n \equiv 3 \pmod{4}$, we can easily see that $\text{Aut}(C_1(n)) = S_{\binom{n}{3}}$, because $C_1(n) = \langle v^P + j \mid P \in \mathcal{P} \rangle$ and for any $g \in S_{\binom{n}{3}}$ we have $g(v^P + j) = v^Q + j$. ■

Lemma 9.2.12 *For $n \equiv 1 \pmod{4}$, $C_1(n) + C_2(n) = \mathbb{F}_2^{\binom{n}{3}}$ and $C_2(n)^\perp \cap T = \langle j \rangle$ where T is as defined in Lemma 9.2.9.*

Proof: From Lemma 9.2.1 (3b), we have $v^{\{a, b, c\}} = w_{\{a, b, c\}} + u$, where $w_{\{a, b, c\}} \in C_1(n)$ and $u \in C_2(n)$, since $C_0(n) \subseteq C_2(n)$ by Lemma 9.2.3, and thus $C_1(n) + C_2(n) = \mathbb{F}_2^{\binom{n}{3}}$. It follows that $C_1(n)^\perp \cap C_2(n)^\perp = \{0\}$, that is $S \cap C_2(n)^\perp = \{0\}$,

where S is defined in Lemma 9.2.6. Suppose that $u \in C_2(n)^\perp \cap T$. Then $u = \sum_a w(a)$. Either $u = \sum_a (j + w(a))$ or $u + j = \sum_a (j + w(a))$. Recalling that $j \in C_2(n)^\perp$, we see that either $u = 0$ or $u = j$, which proves the assertion. ■

Note 9.2.13 From Lemma 9.2.12 and earlier results we see that, for $n \equiv 1 \pmod{4}$,

1. $C_0(n) \subset C_2(n)$;
2. $C_0(n) \subseteq C_1(n) \cap C_2(n)$;
3. $\dim(C_0(n)) \leq \binom{n}{3} - \binom{n}{2}$.

Lemma 9.2.14 If $E = \langle w(\pi) \mid \pi \rangle$ where $w(\pi)$ is defined in Equation (9.8) and π ranges over all partitions of all six element subsets Δ of Ω , then $\dim(E) \geq \binom{n}{3} - \binom{n}{2}$.

If $n \equiv 1 \pmod{4}$, $C_0(n) = E$ and has dimension $\binom{n}{3} - \binom{n}{2}$. Furthermore, $C_0(n) = C_1(n) \cap C_2(n)$.

Proof: The proof follows similar ideas to those in Lemma 9.2.10. Thus we order the points of \mathcal{P} and a specific set of the words $w(\pi)$ so that the generating matrix is in upper triangular form. The point order is as follows: $\{1, 2, 3\}, \{1, 2, 4\}, \dots, \{1, 2, n-1\}, \{1, 3, 4\}, \dots, \{1, 3, n-1\}, \dots, \{1, n-3, n-2\}, \{1, n-3, n-1\}, \{2, 3, 4\}, \dots, \{2, n-3, n-1\}, \dots, \{n-5, n-3, n-2\}, \{n-5, n-3, n-1\}$, giving $\binom{n}{3} - \binom{n}{2}$ positions, followed by the remaining points in arbitrary order.

The words $w(\pi)$ are ordered according to partitions of subsets of Ω of six elements; write here, for simplicity, the sequence $[a, b, c, d, e, f]$ to denote the word $w(\pi)$ with partition $\pi = \{\{a, b\}, \{c, d\}, \{e, f\}\}$. Thus $w(\pi)$ is the vector

$$v^{\{a,c,e\}} + v^{\{a,c,f\}} + v^{\{a,d,e\}} + v^{\{a,d,f\}} + v^{\{b,c,e\}} + v^{\{b,c,f\}} + v^{\{b,d,e\}} + v^{\{b,d,f\}}.$$

We will refer to the term in the support of $w(\pi)$ that is earliest in the ordering of the points as given above, as the leading term of $w(\pi)$. We will choose our π so that the leading terms will be the pivot positions in the generating matrix.

The ordering is as follows: $[1, n-2, 2, n-1, 3, n], [1, n-2, 2, n-1, 4, n], \dots, [1, n-2, 2, n-1, n-3, n], [1, n-3, 2, n-1, n-2, n], [1, n-3, 2, n-2, n-1, n], [1, n-2, 3, n-1, 4, n], \dots, [1, n-3, 3, n-2, n-1, n], \dots, [1, n-3, n-4, n-2, n-1, n]$ and $[1, n-4, n-3, n-1, n-2, n], [1, n-4, n-3, n-2, n-1, n]$ for the first $\binom{n-2}{2} - 1$ vectors, with leading terms the points $\{1, 2, 3\}, \dots, \{1, n-3, n-1\}$. The next vectors are $[2, n-2, 3, n-1, 4, n], \dots, [2, n-4, n-3, n-2, n-1, n]$ giving another $\binom{n-3}{2} - 1$ vectors with leading terms the points $\{2, 3, 4\}, \dots, \{2, n-3, n-1\}$. Continue in this way up to the last set of five vectors: $[n-5, n-2, n-4, n-1, n-3, n], [n-5, n-3, n-4, n-1, n-2, n], [n-5, n-3, n-4, n-2, n-1, n], [n-5, n-4, n-3, n-1, n-2, n], [n-5, n-4, n-3, n-2, n-1, n]$, with leading terms $\{n-5, n-4, n-3\}, \{n-5, n-4, n-2\}, \{n-5, n-4, n-1\}, \{n-5, n-3, n-2\}, \{n-5, n-3, n-1\}$. The number of terms is the sum of these which is again easily seen to be $\binom{n}{3} - \binom{n}{2}$.

If a matrix of codewords is now formed with the points in the order given, and the rows the words $w(\pi)$ in the order given, then this matrix is in upper triangular form, with $\binom{n}{3} - \binom{n}{2}$ pivot positions in the first $\binom{n}{3} - \binom{n}{2}$ positions. Thus E has at least this dimension, for any $n \geq 7$.

If $n \equiv 1 \pmod{4}$, then $\dim(C_0(n)) \leq \binom{n}{3} - \binom{n}{2}$, as noted above. Since $E \subseteq C_0(n)$, we have equality, and since this is also the dimension of $C_1(n) \cap C_2(n)$, this completes the proof. ■

Note 9.2.15 In the Appendix F we list the ordering of the vectors in the case $n = 9$.

Proposition 9.2.16 *For $n \equiv 1 \pmod{4} \geq 9$, $C_0(n)$ is a $[(\binom{n}{3}, \binom{n}{3} - \binom{n}{2}), 8]_2$ code, and $C_0(n)^\perp$ is a $[(\binom{n}{3}, \binom{n}{2}), n - 2]_2$ code. Further, $C_0(n) \cap C_0(n)^\perp = \{0\}$. For all $n \not\equiv 2 \pmod{4}$, $\text{Aut}(C_0(n)) = S_n$ and for $n \equiv 2 \pmod{4}$, $\text{Aut}(C_0(n)) = S_{\binom{n}{3}}$.*

Proof: Since $C_0(n) \subset C_2(n)$, its minimum weight is at least 4, and a vector of weight 4 would be of the form $w(a, b, c, d) \in C_2(n)$, as shown in Proposition 9.2.2. Since these words span $C_2(n)$ and since $\text{Aut}(C_0(n)) \supseteq S_n$, which is transitive on 4-tuples, if $C_0(n)$ contained one word of weight 4 it would contain all those in $C_2(n)$ and hence $C_0(n) = C_2(n)$, which is a contradiction for $n \equiv 1 \pmod{4}$. Thus its minimum weight is 6 or 8. If it contained a word of weight 6 then such a word would be in both $C_2(n)$ and $C_1(n)$, and $w = w(a, b, c, d) + w(a, b, c, e)$ would be a candidate. Consider the vector $u = u([a, b, d, e, c]) = v^{\{a, b, d\}} + v^{\{a, b, e\}} + v^{\{a, d, c\}} + v^{\{a, e, c\}} \in C_1(n)$. Then $w + u \in C_1(n)$ and has weight 2, which is a contradiction. Thus we need only show that the words of weight 6 in $C_2(n)$ have the form of w , in which case it will follow that $C_0(n)$ will have minimum weight 8. For this, we use the words $w(a, b) \in C_2(n)^\perp$, as defined in Equation (9.7). Suppose u is a word of weight 6 in $C_2(n)$. Any $w(a, b)$ must meet the support of u evenly: clearly six times is impossible, since if $\{a, b, c\}$ is in the support, then $(w(b, c), u) = 1$. Four times is also easily seen to be impossible for the same reason, so any $w(a, b)$ can meet the support of u twice or not at all. Thus u must be such that if $\{a, b, c\}$ is in its support, each pair $\{a, b\}$, $\{a, c\}$ and $\{b, c\}$ must occur again in a point in the support of u . Consideration of the possibilities leads only to a word of the form $w = w(a, b, c, d) + w(a, b, c, e)$. Thus the minimum weight of $C_0(n)$ is 8. That the minimum weight of $C_0(n)^\perp$ is $n - 2$ follows by a similar argument to that given in Proposition 9.2.2.

To show that $C_0(n) \cap C_0(n)^\perp = \{0\}$, again we show that $C_0(n) + C_0(n)^\perp = \mathbb{F}_2^{\binom{n}{3}}$. Recall that $w(a)$ and $w(a, b)$ are in $C_0(n)^\perp$, where $w(a)$ is as defined in Equation (9.11). Then, for any $\{a, b, c\}$, $w(a) + w(b) + w(c) + w(a, b) + w(a, c) +$

$w(b, c) + \mathbf{j} + v^{\overline{\{a, b, c\}}_0} = (w(a) + w(b) + w(c) + v^{\overline{\{a, b, c\}}_1}) + (w(a, b) + w(a, c) + w(b, c) + v^{\overline{\{a, b, c\}}_2}) + v^{\{a, b, c\}} = v^{\{a, b, c\}}$, as we observed before (and using Equation (9.4)), and hence $C_0(n) + C_0(n)^\perp = \mathbb{F}_2^{\binom{n}{3}}$.

For the automorphism groups, if $n \equiv 0 \pmod{4}$, then $C_0(n) = C_1(n)$ and hence $\text{Aut}(C_0(n)) = \text{Aut}(C_1(n)) = S_n$ by Proposition 9.2.11. If $n \equiv 1 \pmod{4}$, then by Lemma 9.2.8, $\{w(a) \mid a \in \Omega\}$ is the set of words of weight $\binom{n-1}{2}$ for $C_0(n)^\perp$. Now the proof is similar to the proof in Proposition 9.2.11. If $n \equiv 3 \pmod{4}$, then $C_0(n) = C_2(n)$ and the result follows from Proposition 9.2.2. For $n \equiv 2 \pmod{4}$, $C_2(n) = \mathbb{F}_2^{\binom{n}{3}}$ and the result follows. ■

Chapter 10

Permutation Decoding

10.1 Introduction

In Section 3.5 we have introduced the concept of permutation decoding sets and described the algorithm through which these sets are constructed. This chapter has a two fold methodological aim. The first aim is to present the theory as richly as possible with examples. This is done by using this decoding method in obtaining explicit PD-sets for some of the codes presented in Chapters 8 and 9, that is the binary codes of the triangular graphs and the codes obtained from the graphs on triples. The success of decoding came about by ordering the points in such a way that the nature of the information symbols was known and the action of the automorphism group apparent. The second aim is to illustrate with particular examples how computational methods could be applied in the cases where the minimum distance is reasonably small. Using Magma [11] we have obtained such sets for the $[15, 4, 8]_2$ code of the $2-(15, 8, 4)$ design described in Proposition 6.3.1, which is the dual code of the Hamming code of length 15, and for the binary codes of the Chang graphs.

We have developed two programmes in Magma (see Appendices C and H) which deal with computations. The first programme (Appendix C) computes the PD-sets of t -error-correcting codes, for small t , with $t \leq 7$. The second programme (Appendix H) is used for constructing the Chang graphs and their codes.

10.2 Codes of the triangular graphs

In this section we describe specific PD-sets for the binary codes obtained from the triangular graphs. For decoding purposes we order the points in such a way that the nature of the information symbols is known and the action of the automorphism group apparent. These codes were constructed in Chapter 8 and their properties were given in Lemma 8.2.3. In Lemma 8.2.7 we showed that by ordering the points in the following way:

$$\{1, 2\}, \{1, 3\}, \dots, \{1, n-1\}, \{2, 3\}, \dots, \{2, n-1\}, \dots, \{n-2, n-1\}, \quad (10.1)$$

followed by the remaining points

$$\{1, n\}, \{2, n\}, \dots, \{n-1, n\} \quad (10.2)$$

we get the generator matrix of C^\perp in upper triangular form.

The generator matrix obtained in Lemma 8.2.7 for C^\perp with the above ordering can be reduced to the form $[I_k | A]$ where k is the dimension of C^\perp . If the points are re-ordered with the first k put at the end, then the matrix is $[A | I_k]$. This is now standard form for the code C , and the corresponding generator matrix for C has the form $[I_{n-k} | A^T]$, where here we are using n for the length of the code.

In order to get the generator matrix into standard form, as described above, we order the point set \mathcal{P} by taking the set from Equation (10.2), that is

$$P_1 = \{1, n\}, P_2 = \{2, n\}, \dots, P_{n-1} = \{n-1, n\}, \quad (10.3)$$

first, followed by the set from Equation (10.1), that is

$$P_n = \{1, 2\}, P_{n+1} = \{1, 3\}, \dots, P_{2n-2} = \{2, 3\}, \dots, P_{\binom{n}{2}} = \{n-2, n-1\}. \quad (10.4)$$

The generator matrix for C^\perp , using the words of weight 3 (with \mathbf{j} if n is even), is then a check matrix for C in standard form. The generator matrix for C will then also be in standard form, with the first $n-1$ coordinates the information symbols for n odd, and the first $n-2$ for n even. Using the fact that the group of the code is S_n , we can find PD-sets for the code C .

Proposition 10.2.1 *For $n \geq 5$ odd, a PD-set of n elements can be found for C . If the points are ordered as given in Equations (10.3) and (10.4), the set*

$$\mathcal{S} = \{1_G\} \cup \{(i, n) \mid 1 \leq i \leq n-1\}$$

of permutations in S_n in the natural action on the points \mathcal{P} forms a PD-set of n elements for C .

Proof: Order the points of the coordinate set \mathcal{P} as described in Equations (10.3) and (10.4) so that the first $n-1$ points are in the information positions.

Now C can correct $t = \frac{n-3}{2}$ errors. We need a set \mathcal{S} of elements of $G = S_n = \text{Aut}(C)$ such that every t -set of elements of \mathcal{P} is moved by some element of \mathcal{S} into the check positions. If the $s \leq t$ positions are all in the check positions, then we can use the identity element, 1_G , to keep these in the check positions.

Suppose the $s \leq t$ positions occur at

$$\{a_1, n\}, \{a_2, n\}, \dots, \{a_r, n\},$$

distinct points in the information positions, and at

$$\{b_1, c_1\}, \{b_2, c_2\}, \dots, \{b_m, c_m\},$$

distinct points in the check positions, where $r + m = s \leq t$. The number of elements of Ω in the set

$$\mathcal{T} = \{a_1, \dots, a_r\} \cup \{b_1, \dots, b_m\} \cup \{c_1, \dots, c_m\} \subseteq \Omega \setminus \{n\}$$

is at most $r + 2m$. Since $r + m \leq t = (n - 3)/2$, we have $2r + 2m \leq n - 3$, and thus $r + 2m \leq n - 3$. Thus there are elements other than n in Ω that are not in \mathcal{T} ; let d be one of these. The transposition $\sigma = (d, n)$ will map the r elements

$$\{a_1, n\}, \{a_2, n\}, \dots, \{a_r, n\}$$

out of the information positions, as required, and fix the m elements already in the check positions.

It follows that the given set

$$\mathcal{S} = \{1_G\} \cup \{(i, n) \mid 1 \leq i \leq n - 1\} \quad (10.5)$$

forms a PD-set of n group elements for the code. ■

In this case the Gordon bound (see Theorem 3.5.5) has an explicit form:

Lemma 10.2.2 *For $n \geq 5$ odd, the Gordon bound for C is $\frac{n-1}{2}$.*

Proof: The length of the code is $\binom{n}{2}$ and the redundancy is $r = \binom{n}{2} - n + 1$. With $t = \frac{n-3}{2}$, we have

$$\frac{\binom{n}{2} - t + 1}{\binom{n}{2} - n + 1 - t + 1} = \frac{n^2 - 2n + 5}{n^2 - 4n + 7}$$

for the innermost term. In fact the Gordon bound is

$$\left\lceil \frac{n^2 - n}{n^2 - 3n + 2} \left\lceil \cdots \left\lceil \frac{n^2 - 2n + 7}{n^2 - 4n + 9} \left\lceil \frac{n^2 - 2n + 5}{n^2 - 4n + 7} \right\rceil \cdots \right\rceil \right\rceil \right\rceil.$$

It is not hard to show that this is equal to $\frac{n-1}{2}$ for $n \geq 5$ and odd. ■

Proposition 10.2.3 *For $n \geq 6$ and even, a PD-set of $n^2 - 2n + 2$ elements can be found for C . If the points are ordered as given in Equations (10.3) and (10.4), the set*

$$\mathcal{S} = \{1_G\} \cup \{(i, n) \mid 1 \leq i \leq n-1\} \cup \{[(i, n-1)(j, n)]^{\pm 1} \mid 1 \leq i, j \leq n-2\}$$

of permutations in S_n in the natural action on the points \mathcal{P} is a PD-set for C .

Proof: Again we order the points as in Equations (10.3) and (10.4) so that now the points P_1, P_2, \dots, P_{n-2} are in the information positions, \mathcal{I} , and the remaining points of \mathcal{P} , starting with $P_{n-1} = \{n-1, n\}$, then followed by $P_n, \dots, P_{\binom{n}{2}}$, are in the check positions, \mathcal{E} . In this case we need to correct $t = n-3$ errors, since the minimum weight is $2(n-2)$.

We claim that

$$\mathcal{S} = \{1_G\} \cup \{(i, n) \mid 1 \leq i \leq n-1\} \cup \{[(i, n-1)(j, n)]^{\pm 1} \mid 1 \leq i, j \leq n-2\}$$

is a PD-set for C . Note that $|\mathcal{S}| = 1 + n - 1 + 2(n-2) + (n-2)(n-3) = n^2 - 2n + 2$.

We need to show that every t -tuple T of points of \mathcal{P} can be moved into the check positions \mathcal{E} by some member of \mathcal{S} . Consider the various cases for the members of T :

- (i): if all the t positions are in \mathcal{E} then 1_G will do;
- (ii): if all the t positions are in \mathcal{I} then $(n-1, n)$ will do;
- (iii): if some $a \in \Omega \setminus \{n\}$ does not occur in any member of T then (a, n) will do.

We can thus restrict our attention to those sets T for which every $a \in \Omega$ appears in some duad in T . We show that if $\{a, b\} \in T$ and a does not occur again in any element of T , then an element of \mathcal{S} can be found to map T into \mathcal{E} . Consider the possible cases:

- (iv): $a = n$ and $b = n-1$, then 1_G will do; if $b \neq n-1$, then $(b, n-1)$ will do;
- (v): $a \neq n$ and $b = n$ then if $a = n-1$, $(n, n-1)$ will do and if $a \neq n-1$ then

$(a, n, n-1) = (a, n)(a, n-1)$ will do;

(vi): $a \neq n$ and $b \neq n$ then if $a = n-1$, $(b, n-1)(b, n)$ will do; if $a \neq n-1$, then if $b = n-1$, (a, n) will do and if $b \neq n-1$, $(a, n)(b, n-1)$ will do.

So if there is a duad $\{a, b\} \in T$ such that a occurs only once, our set of permutations will form a PD-set. Now every $a \in \Omega$ occurs and if every element appears more than once we would have $2n$ elements to place in $2t = 2(n-3)$ positions, which is impossible. ■

Remark 10.2.4 (i) The code C^\perp has minimum weight 3, so can only be used for single-error correction. Thus syndrome decoding would be the usual method employed. However notice that PD-sets can be found easily for this code too, using the ordering of the points given in Lemma 8.2.7, where the set \mathcal{S} of n permutations given in Equation (10.5) will form a PD-set for C^\perp for $n \geq 5$ odd or even. The Gordon bound is less than this number.

(ii) The permutations given in the set \mathcal{S} need to be written as permutations on the points $P_1, P_2, \dots, P_{\binom{n}{2}}$. Thus, for example, if $n = 6$, then with the ordering of the points as given in Equations (10.3) and (10.4),

$$\begin{aligned} (1, 6) &\equiv (P_2, P_6)(P_3, P_7)(P_4, P_8)(P_9, P_5) \\ (1, 5)(1, 6) &\equiv (P_1, P_9, P_5)(P_2, P_6, P_{12})(P_3, P_7, P_{14})(P_4, P_8, P_{15}) \\ (1, 5)(2, 6) &\equiv (P_1, P_{12})(P_3, P_{10})(P_4, P_{11})(P_6, P_5)(P_7, P_{14})(P_8, P_{15}) \end{aligned}$$

(iii) For n even the Gordon bound becomes

$$\left\lceil \frac{n^2 - n}{n^2 - 3n + 4} \left\lceil \frac{n^2 - n - 2}{n^2 - 3n + 2} \left\lceil \cdots \left\lceil \frac{n^2 - 3n + 8}{n^2 - 5n + 12} \right\rceil \cdots \right\rceil \right\rceil \right\rceil.$$

An exact formula for this, in contrast to the odd case, does not seem evident, but from computations (using Magma [11]) up to a large value of n , the following formula appears to hold for this bound for $n \geq 18$ (smaller values of n seem

to be unrepresentative of the general rule): writing $n = 2k + 18$, $k_1 = k \pmod{6} \in \{0, 1, 2, 3, 4, 5\}$, $k \geq 0$, the Gordon bound for n is

$$n + 8 + 10 \left\lfloor \frac{k}{6} \right\rfloor + k_1 + \left\lfloor \frac{k_1}{2} \right\rfloor.$$

For n even the size of the PD-sets we have found are of the order of n^2 , a lot bigger than the Gordon bound, which gives the order of n ; the Magma output in Appendix E, illustrates this. However, we show also the size of the automorphism group in comparison to illustrate that our sets are a lot better than trying to use the whole group.

10.3 Codes of the graphs on triples

In this section using the results established in Chapter 9 we determine PD-sets, for some of the binary codes obtained from the adjacency matrix of the graphs on $\binom{n}{3}$ vertices, for $n \geq 7$, with adjacency defined by the vertices as 3-sets being adjacent if they have zero, one or two elements in common, respectively. In Proposition 9.2.2 we showed that the points $\{1, 2, n\}, \{1, 3, n\}, \dots, \{n-2, n-1, n\}$ can be taken to be the information positions for the code $C_2(n)^\perp$ for $n \geq 7$ odd. We now replace the point $\{n-2, n-1, n\}$ with $\{n-3, n-2, n-1\}$; that this can be done is easily seen by looking at the last basis word for $C_2(n)$, that is $w(n-3, n-2, n-1, n)$. With this ordering of points, the generator matrix for $C_2(n)^\perp$ is in standard form and we have the following:

Theorem 10.3.1 *Let $D = C_2(n)^\perp$ be the $[(\binom{n}{3}), (\binom{n-1}{2}), n-2]_2$ code from the design $\mathcal{D}_2(n)$ when $n \geq 7$ is odd. Taking the points $\{1, 2, n\}, \{1, 3, n\}, \dots, \{n-2, n-1, n\}$ as information symbols, but replacing the point $\{n-2, n-1, n\}$ by $\{n-3, n-2, n-1\}$, then D has a PD-set in S_n given by the following elements of S_n in their natural action on triples of elements of $\Omega = \{1, 2, \dots, n\}$:*

$$S = \{(n, i)(n-1, j)(n-2, k) \mid 1 \leq i \leq n, 1 \leq j \leq n-1, 1 \leq k \leq n-2\}.$$

We note that the notation includes the convention $(i, i) = 1$, the identity element of S_n .

Proof: That the information symbols can be taken as given above follows from Proposition 9.2.2. Let \mathcal{I} denote the information positions, and \mathcal{E} the check positions. Thus

$$\mathcal{I} = \{\{i, j, n\} \mid 1 \leq i < j < n\} \cup \{\{n-3, n-2, n-1\}\} \setminus \{\{n-2, n-1, n\}\}.$$

Let $P = \{n-3, n-2, n-1\} \in \mathcal{I}$ and $Q = \{n-2, n-1, n\} \in \mathcal{E}$. Notice that the code D will correct $t = \frac{n-3}{2}$ errors.

Take a set \mathcal{T} of t points of \mathcal{P} and let $T = \bigcup_{\{a,b,c\} \in \mathcal{T}} \{a, b, c\}$. We need to exhibit an element $\sigma \in S$ such that $T\sigma \subseteq \mathcal{E}$. For this we need to consider the different types of composition of \mathcal{T} , so the proof goes through a number of cases. Notice that if $\mathcal{T} \subseteq \mathcal{E}$ then the identity 1 will do. Thus suppose $\mathcal{T} \not\subseteq \mathcal{E}$.

Case (I): $\mathcal{T} \subseteq \mathcal{I}$. Then at least $t-1$ members of \mathcal{T} contain n .

(i) $P \notin \mathcal{T}$: then $|T| \leq 2t+1 = n-2$, so there are at least two elements a and b in Ω , not equal to n , that are not in T . If $a \leq n-3$ then $\sigma = (n, a)$ will satisfy $T\sigma \subseteq \mathcal{E}$. If $\{a, b\} = \{n-2, n-1\}$ then again (n, a) will do.

(ii) $P \in \mathcal{T}$: then $|T| \leq 2(t-1) + 1 + 3 = n-1$, so there is at least one element $a \in \Omega$ such that $a \notin T$. Clearly $a \leq n-4$. If $|T| = n-1$, then $n-3, n-2, n-1$ appear only in P and in no other element of \mathcal{T} . Thus $(n, n-3)$ will do. If $|T| < n-1$ then there are at least two elements $a, b \notin T$ with $a, b \leq n-4$. Then $T(n, a)(n-1, b) \subseteq \mathcal{E}$.

Case (II): suppose \mathcal{T} meets both \mathcal{I} and \mathcal{E} non-trivially.

(i) Suppose first that there is an element $a \in \Omega$ such that $a \notin T$.

1. If $a \leq n-4$ then if $P \notin \mathcal{T}$, $g = (n, a)$ will do. If $P \in \mathcal{T}$ then the number of points of the form $\{i, n-2, n-3\}$ with $i \neq n, n-1$, a is $n-5 > t-1$ for $n \geq 7$, so there is an element $b \leq n-4$ such that $b \neq a$ and $\{b, n-2, n-3\} \notin \mathcal{T}$.

Then $\mathcal{T}(n, a)(n - 1, b) \subseteq \mathcal{E}$.

2. If $a = n - 3$ then $P \notin \mathcal{T}$. If $Q \notin \mathcal{T}$ then $(n, n - 3)$ will do. If $Q \in \mathcal{T}$ then $\mathcal{T}(n, n - 3)(n - 1, b) \subseteq \mathcal{E}$ for any $b \leq n - 4$.
3. If $a = n - 2$ then $P, Q \notin \mathcal{T}$. If $\{n - 3, n - 1, n\} \notin \mathcal{T}$ then $(n, n - 2)$ will do, and if $\{n - 3, n - 1, n\} \in \mathcal{T}$, then $(n, n - 2)(n - 1, b)$ for some $b \leq n - 4$ will do.
4. If $a = n - 1$ then $P, Q \notin \mathcal{T}$. If $\{n - 3, n - 2, n\} \notin \mathcal{T}$ then $(n, n - 1)$ will do, and if $\{n - 3, n - 2, n\} \in \mathcal{T}$, then $(n, n - 1)(n - 2, b)$ for some $b \leq n - 4$ will do.
5. If $a = n$, then $\mathcal{T} \cap \mathcal{I} = \{\{n - 3, n - 2, n - 1\}\}$. The number of points of the form $\{i, n - 2, n - 3\}$ with $i \neq n, n - 1$ is $n - 4 > t - 1$ for $n \geq 7$, so there is an element $b \leq n - 4$ such that $\{b, n - 2, n - 3\} \notin \mathcal{T}$. Then $\mathcal{T}(b, n - 1) \subseteq \mathcal{E}$.

(ii) Now suppose that $T = \Omega$. For $a \in \Omega$, let x_a denote the number of times a appears in points in \mathcal{T} . So $1 \leq x_a \leq t$ for each $a \in \Omega$ and $3t = \sum_{i=1}^n x_i$. For $1 \leq i \leq t$ let $k_i = |\{a \in \Omega \mid x_a = i\}|$. Thus

$$3t = x_1 + x_2 + \cdots + x_n = k_1 + 2k_2 + \cdots + tk_t.$$

For any $a \in \Omega$, $x_a = 3t - \sum_{b \neq a} x_b \leq 3t - (n - 1) = t - 2$, and so $k_i = 0$ for $i \geq t - 1$.

We will now show that we can find a point $\{a, b, c\} \in \mathcal{T}$ such that $x_a = x_b = 1$, $a, b \leq n - 4$, and $c \neq n$. Suppose $x_n = m$, where $1 < m \leq t - 2$. Then

$$3t = k_1 + m + \sum_{x_a \geq 2, a \neq n} \geq k_1 + m + 2(n - 1 - k_1),$$

which simplifies to $k_1 \geq t + 4 + m$. If $m = 1$ then this inequality still applies if we take k_1 to be the number of elements with $x_a = 1$ excluding n . Suppose that

as many pairs with $x_a = 1$ as possible occur as part of a triple with n in \mathcal{T} . This uses $2m$ elements, leaving $k_1 - 2m \geq t + 4 - m$ elements with $x_a = 1$ (always excluding n from the count). We want to exclude $n - 3, n - 2, n - 1$, which still leaves at least $k_1 - 2m - 3 \geq t + m - 1$ elements. The number of points available is $t - m$ so we must have at least one point $X = \{a, b, c\}$ with two elements a and b with $x_a = x_b = 1$, $a, b \leq n - 4$, and $c \neq n$.

Finally we show how this point $X = \{a, b, c\}$ can be used to define group elements that will map \mathcal{T} into \mathcal{E} . We need to look at the various possibilities for c .

1. $c \leq n - 4$: then $\sigma = (n, a)(n - 1, b)(n - 2, c)$ will satisfy $\mathcal{T}\sigma \subseteq \mathcal{E}$, since $\{d, e, n\}\sigma \in \mathcal{E}$, $\{a, b, c\}\sigma = \{n, n - 1, n - 2\} \in \mathcal{E}$, and $\{n - 3, n - 2, n - 1\}\sigma^{-1} = \{b, c, n - 3\} \notin \mathcal{T}$, since $x_b = 1$ and $a \neq n - 3$.
2. $c = n - 1$: then $\sigma = (n, a)(b, n - 2)$ will work as above, noting that $\{n - 3, n - 2, n - 1\}\sigma^{-1} = \{b, n - 1, n - 3\} \notin \mathcal{T}$, since $x_b = 1$ and $a \neq n - 3$.
3. $c = n - 2$: then $\sigma = (n, a)(b, n - 1)$ will work as in the previous case.
4. $c = n - 3$: then $\{a, b, c\} = \{a, b, n - 3\}$ and take $\sigma = (n, a)(b, n - 1)(n - 2, n - 3)$. Then $\{a, b, c\}g = \{n, n - 1, n - 2\} \in \mathcal{E}$, and $\{n - 3, n - 2, n - 1\}\sigma^{-1} = \{b, n - 2, n - 3\} \notin \mathcal{T}$, since $x_b = 1$ and $a \neq n - 2$.

We have shown that every t -tuple, and hence every s -tuple for $s \leq t$ can be moved by an element of S into the error positions. Thus S is a PD-set for D . ■

Next we looked at the code $C_0(n)$ for $n \equiv 1 \pmod{4} \geq 9$, with minimum weight 8 and thus 3-error-correcting. This code has been obtained in Proposition 9.2.16. Note first that from Lemma 9.2.14 we can take as the $\binom{n}{2}$ check positions the points $\{i, j, n\}$ for $1 \leq i, j \leq n - 1$, $\{i, n - 2, n - 1\}$ for $1 \leq i \leq n - 3$ and two extra points: $\{n - 4, n - 3, n - 1\}$ and $\{n - 5, n - 4, n - 3\}$,

where again we have switched the last point with $\{n-4, n-3, n-2\}$ in order to be able to construct a PD-set.

Theorem 10.3.2 *Let $C = C_0(n)$ be the $[(\binom{n}{3}, \binom{n}{3} - \binom{n}{2}), 8]_2$ code from the design $\mathcal{D}_0(n)$ when $n \equiv 1 \pmod{4} \geq 9$. With information and check positions defined as above, C has a PD-set in S_n given by the following elements of S_n in their natural action on triples of elements of $\Omega = \{1, 2, \dots, n\}$:*

$$S = \{(n, i_0)(n-1, i_1)(n-2, i_2)(n-3, i_3)(n-4, i_4)(n-5, i_5) \mid 1 \leq i_j \leq n-j, 0 \leq j \leq 5\},$$

where (i, i) denotes the identity element of S_n .

Proof: Let \mathcal{I} denote the information positions and \mathcal{E} the check position. Thus, writing $P = \{n-4, n-3, n-1\}$ and $Q = \{n-5, n-4, n-3\}$, let

$$\mathcal{E}_1 = \{\{i, j, n\} \mid 1 \leq i, j \leq n-1\},$$

$$\mathcal{E}_2 = \{\{i, n-2, n-1\} \mid 1 \leq i \leq n-3\},$$

and $\mathcal{E}_3 = \{P, Q\}$, then

$$\mathcal{E} = \mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3.$$

The code C corrects three errors, so for any given set \mathcal{T} of three points of \mathcal{P} , we need to exhibit an element $\sigma \in S$ such that $\mathcal{T}\sigma \subseteq \mathcal{E}$. For this we need to consider the different types of composition of \mathcal{T} , depending on the number of points from \mathcal{T} in \mathcal{I} . Notice that if $\mathcal{T} \subseteq \mathcal{E}$ then the identity 1 will do, which is included in S . Thus suppose $\mathcal{T} \not\subseteq \mathcal{E}$.

Case (I): $\mathcal{T} \subseteq \mathcal{I}$. Let $\mathcal{T} = \{P_1, P_2, P_3\}$. If there is an element $a \in P_i$ for $i = 1, 2, 3$, then (n, a) will do. If there is an element $a \in P_1, P_2$, and $a \notin P_3$, then if $P_3 = \{g, h, i\}$, where $g < h < i \leq n-1$, then $(n, a)(n-1, i)(n-2, h)$ will map \mathcal{T} to \mathcal{E} .

Now we can suppose the P_i are disjoint, where $P_1 = \{a, b, c\}$ and $a < b < c \leq n - 1$, and $P_2 = \{d, e, f\}$ where $d < e < f \leq n - 1$. Since these are disjoint, their images must be disjoint, so we need $\sigma \in S$ such that $P_1\sigma \in \mathcal{E}_1$, $P_2\sigma \in \mathcal{E}_2$ and $P_3\sigma = Q$. Consideration of the cases involved easily yields that some element of the form

$$\sigma = (n, a_1)(n - 1, a_2)(n - 2, a_3)(n - 3, a_4)(n - 4, a_5)(n - 5, a_6)$$

where $a_i \leq n - i + 1$, will work in all cases, as required.

Case (II): $\mathcal{T} \cap \mathcal{I} = \{P_1, P_2\}$. We consider possibilities for $P_3 \in \mathcal{E}$.

1. $P_3 \in \mathcal{E}_1$, that is $P_3 = \{n, h, i\}$:

- (a) if $P_1 \cap P_2 = \emptyset$, then $(n - 1, a)(n - 2, b)(n - 3, d)(n - 4, e)(n - 5, f)$ will map \mathcal{T} into \mathcal{E} ;
- (b) if $P_1 \cap P_2 = \{a\}$, where $a = d$, then $(n, a)(h, n - 1)(i, n - 2)$ will do;
- (c) if $P_1 \cap P_2 = \{a, b\}$, then $(n - 1, a)(n - 2, b)$ will do.

2. $P_3 \in \mathcal{E}_2$, that is $P_3 = \{n - 1, n - 2, i\}$:

- (a) if $P_1 \cap P_2 \cap P_3 = \emptyset$, or if $P_1 \cap P_2 = \emptyset$ and neither $n - 1$ nor $n - 2$ are in $P_1 \cup P_2$, then $(n, a)(n - 3, d)(n - 4, e)(n - 5, f)$ will map \mathcal{T} into \mathcal{E} ; if $n - 1 = a$ or $n - 2 = a$, then $(n, a)(n - 3, d)(n - 4, e)(n - 5, f)$ will still do;
- (b) if $P_1 \cap P_2 = \{a\}$, where $a = d$, then (n, a) will do;
- (c) if $P_1 \cap P_2 = \{a, b\}$, then $(n, i)(n - 1, a)(n - 2, b)$ will do.

3. $P_3 \in \mathcal{E}_3$, that is $P_3 = P$ or Q :

- (a) if $a \in P_1 \cap P_2$, then (n, a) will do;

- (b) if P_1 and P_2 are disjoint then they must map to disjoint elements in \mathcal{E} while P_3 must also stay in \mathcal{E} ; this can be done by mapping P_3 to an element in \mathcal{E}_1 , P_1 to an element in \mathcal{E}_2 and P_2 to P or Q . This can be achieved with an element σ of S . Note that the transpositions in σ need not commute.

Case (III): $\mathcal{T} \cap \mathcal{I} = \{P_1\}$.

1. If $n \notin P_2$ or P_3 , then (n, a) will map \mathcal{T} into \mathcal{E} .
2. If $n \in P_2 \cap P_3$ then we can map P_1 into \mathcal{E}_2 and keep P_2 and P_3 in \mathcal{E}_1 by an element of the form $(n-1, b)(n-2, c)$ or $(n-1, c)(n-2, b)$ (where we still use the convention that $a < b < c$).
3. If $P_2 \in \mathcal{E}_1$ and $P_3 \in \mathcal{E}_2$ then if $n-1, n-2 \notin P_1$, the element $(n-3, c)(n-4, b)(n-5, a)$ will map P_1 to Q and keep P_2 in \mathcal{E}_1 , and P_3 in \mathcal{E}_2 ; if $c = n-1$ then $(n-3, b)(n-4, a)$ maps P_1 to P , and if $c = n-2$ then $(n-1, n-2)(n-3, b)(n-4, a)$ will map P_1 to P , and the others will stay in the same class.
4. If $P_2 \in \mathcal{E}_1$ and $P_3 \in \mathcal{E}_3$, then $P_3 = P$ or Q . Taking $P_3 = Q$ first, if none of $n-i$ for $i \in \{1, 2, 3, 4, 5\}$ are in P_1 , then $(n-1, a)(n-2, b)$ will do. If some of the $n-i$ are in P_1 then a case by case analysis shows that we can keep P_2 in \mathcal{E}_1 and map P_1 and P_3 into \mathcal{E}_2 or \mathcal{E}_3 . The same is true for $P_3 = P$; we leave these details for the reader to check.

Thus in all cases we have shown that an element of S can be found to move the triple into the check positions, so S is a PD-set for the code. ■

10.4 PD-sets through computation

For small t , PD-sets can be found computationally. Using Magma we have designed a programme (see Appendix C) which could be used to determine the PD-sets with small t and $t \leq 7$. We used the programme and determined the PD-sets for the $[15, 4, 8]_2$ code of the 2 -(15, 8, 4) design, and the binary codes of the Chang graphs. This programme was also used for the PD-sets of codes related to A_9 (see discussion in Section 6.3.2). A list of these codes and corresponding PD-sets can be found at the website:

<http://www.ces.clemson.edu/~keyj>

under the list of PD-sets.

In [60] Key, examined the Hermitian and Ree unitals on 28 points, both of whose codes are only single-error correcting, but nevertheless PD-sets were found. Key also looked at some codes from desarguesian projective planes; these codes are cyclic, so PD-sets were found in the normalizer of a regular cyclic subgroup of the automorphism group.

10.4.1 Codes from A_6 and A_9

As an illustration of permutation decoding, we obtained a PD-set for the binary code of the 2 -(15, 8, 4) design: the code is the simplex code of length 15, that is a $[15, 4, 8]$ code, which is the dual to the binary Hamming code of length 15. A generator matrix in standard form is

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


From Lemma 6.3.1 we have that the automorphism group of this code is the group $PGL_4(2)$. The group $PGL_4(2)$ contains Singer cycles, and hence the code is cyclic. According to the bound mentioned in Theorem 3.5.5, at least five permutations are needed for a PD-set. In addition, according to the analysis in MacWilliams [79], a PD-set might be found in a Singer group. Using the programme listed in Appendix C we found the following seven elements that form a PD-set for this code in a Singer group in $PGL_4(2)$:

Id,

$(1, 13, 10, 9, 8)(2, 5, 14, 7, 6)(3, 11, 15, 12, 4),$
 $(1, 15, 2, 13, 12, 5, 10, 4, 14, 9, 3, 7, 8, 11, 6),$
 $(1, 2, 12, 10, 14, 3, 8, 6, 15, 13, 5, 4, 9, 7, 11),$
 $(1, 11, 7, 9, 4, 5, 13, 15, 6, 8, 3, 14, 10, 12, 2),$
 $(1, 8, 9, 10, 13)(2, 6, 7, 14, 5)(3, 4, 12, 15, 11),$
 $(1, 6, 11, 8, 7, 3, 9, 14, 4, 10, 5, 12, 13, 2, 15).$

This gives an algorithm for correcting three errors. The minimum size of a PD-set for this code is 5.

We now list some of the codes with interesting parameters obtained from the designs resulting from the action of A_9 (see Section 6.3.2) on two different designs on 126 points:

- The binary code C of the 1-(126, 20, 20) design is a $[126, 56, 6]_2$ with dual a $[126, 70, 5]_2$ code. For C the minimum size of a PD-set is 4, and we found one of size 17; for C^\perp the minimum size is 7 and we found one of size 32.
- The binary code C of the 1-(126, 40, 40) design is a $[126, 48, 16]_2$ and its dual is a $[126, 78, 5]_2$ code. We found a PD-set of size 43 for C^\perp , the minimum size being 8.

10.4.2 Binary codes of the Chang graphs

There exist four non-isomorphic strongly regular graphs of the type $(28, 12, 6, 4)$, being $T(8)$ and the three Chang graphs. All these graphs are switching equivalent.

Definition 10.4.1 [22] *The operation of **switching** a graph Γ with respect to a set Y of vertices replaces Γ by the graph Γ' such that $\{a, b\}$ is an edge of Γ' if and only if both or neither of the following conditions occur:*

- (i) $|\{a, b\} \cap Y| = 0$ or 2 .
- (ii) $\{a, b\}$ is an edge of Γ .

In other words switching replaces all edges between Y and its complement with non-edges and vice versa, leaving edges within Y and outside Y unaltered.

The vertex set of $T(8)$ is the set of duads of $\{1, 2, \dots, 8\}$. So a subset of the vertex set can be regarded as the edge set of a graph with eight vertices. Here we take a set of eight elements $\{a, b, c, d, e, f, g, h\}$ as vertices for $T(8)$. The three **Chang graphs** can be obtained by switching $T(8)$ with respect to:

- (1) four disjoint edges, that is $\{a, b\}, \{c, d\}, \{e, f\}, \{g, h\}$;
- (2) an octagon, that is $\{a, b\}, \{b, c\}, \{c, d\}, \{d, e\}, \{e, f\}, \{f, g\}, \{g, h\}, \{h, a\}$;
- (3) the disjoint union of a pentagon and a triangle, that is $\{a, b\}, \{b, c\}, \{c, a\}, \{d, e\}, \{e, f\}, \{f, g\}, \{g, h\}, \{h, d\}$.

Each graph obtained is a strongly regular graph with parameters as those of $T(8)$, that is $(28, 12, 6, 4)$. Additional information on the Chang graphs can be found in [22, Chapter 4] and [87].

By making use of the notion of switching as given above we have developed a programme in Magma (see Appendix H), which we used to construct the Chang graphs from $T(8)$, and to determine their respective binary codes.

In Table 10.1 we list the codes from the Chang graphs and $T(8)$ respectively. The first column gives the names of the graphs which we adopted as the names

of their respective codes, the second the dimension, and the remaining the weight enumerator of each of the codes. We will call the binary codes from the Chang graphs, Chang 1, Chang 2 and Chang 3 codes, respectively. From Lemma 8.2.3 we have that $T(8)$ produces a binary code of dimension 6 and from Table 10.1 we deduce that each Chang code has dimension 8. Now if C is any of the Chang codes, it follows from [50, Theorem 5.1] that $\mathbf{j} \in C$. In addition observe that the Chang 1 and Chang 2 codes, have the same weight enumerator, and they are 3-error-correcting codes. Using the notion of **invariant multisets** on the codewords of weight 8, it is shown in [50] that the Chang 1 and Chang 2 codes are non-isomorphic.

Name	Dim	0	4	8	12	16	20	24	28
$T(8)$	6	1			28	35			1
Chang 1	8	1		6	121	121	6		1
Chang 2	8	1		6	121	121	6		1
Chang 3	8	1	1	3	121	128	3	1	1

Table 10.1: Weight enumerator of the codes of the graphs of type $(28, 12, 6, 4)$

Using the programme given in Appendix C we determined PD-sets associated with the Chang codes.

In the following we only list the a PD-set for the Chang 1 code. Note that according to the Gordon bound the minimum size for a PD-set for the Chang 1 code is 5, and the PD-set presented below has 16 elements. The PD-set for the Chang 2 code is given in Appendix I. Notice that the Chang 3 code is a single-error correcting code, so a PD-set for this code could be found using syndrome decoding.

$(1, 23)(2, 22)(3, 25)(4, 21)(5, 12)(6, 17)(8, 27)(9, 19)(11, 15)(13, 26)(14, 20)(24, 28),$
 $(1, 7, 23, 20, 11, 6, 22, 18, 2, 17, 15, 14)(3, 12, 5, 25, 26, 27, 24, 19, 9, 28, 8, 13)(4, 21, 10),$

$(1, 22)(2, 19)(3, 15)(4, 10)(6, 26)(7, 25)(8, 14)(11, 24)(12, 23)(16, 21)(17, 20)(18, 28),$
 $(1, 8)(2, 13)(3, 28)(5, 6)(9, 14)(10, 16)(11, 15)(12, 17)(19, 20)(22, 26)(23, 27)(24, 25),$
 $(1, 8, 24, 20, 12, 28, 22, 26, 3, 17, 19, 25)(2, 15, 27, 14, 7, 9, 23, 11, 13, 6, 18, 5)(4, 16, 10),$
 $(1, 7)(2, 6)(3, 5)(8, 26)(9, 24)(10, 21)(11, 17)(13, 25)(14, 23)(15, 20)(18, 22)(27, 28),$
 $(1, 20)(2, 18)(3, 26)(4, 10)(6, 15)(7, 23)(8, 24)(11, 14)(12, 25)(13, 27)(17, 22)(19, 28),$
 $(1, 7, 8, 22, 18, 26)(2, 5, 28, 23, 9, 25)(3, 6, 13, 24, 14, 27)(10, 21, 16)(11, 12, 17, 15, 19, 20),$
 $(1, 27)(2, 26)(3, 24)(4, 21)(5, 17)(6, 12)(8, 23)(9, 20)(10, 16)(13, 22)(14, 19)(25, 28),$
 $(1, 23, 9, 12, 22, 2, 5, 19)(3, 15, 28, 7, 24, 11, 25, 18)(4, 10, 21, 16)(6, 27, 26, 20, 14, 13, 8, 17),$
 $(1, 7, 27, 25, 22, 18, 13, 28)(2, 12, 6, 26, 23, 19, 14, 8)(3, 17, 11, 5, 24, 20, 15, 9)(4, 21, 16, 10),$
 $(1, 23, 28, 20, 6, 3, 22, 2, 25, 17, 14, 24)(4, 21, 16)(5, 8, 18, 27, 12, 15, 9, 26, 7, 13, 19, 11),$
 $(1, 27, 22, 13)(2, 6, 23, 14)(3, 11, 24, 15)(4, 16)(5, 20, 9, 17)(7, 25, 18, 28)(8, 12, 26, 19)(10, 21),$
 $(1, 23, 11, 22, 2, 15)(3, 5, 26, 24, 9, 8)(4, 10, 21)(6, 18, 17, 14, 7, 20)(12, 25, 27, 19, 28, 13),$
 $(1, 27, 20, 5, 22, 13, 17, 9)(2, 11, 26, 25, 23, 15, 8, 28)(3, 6, 18, 12, 24, 14, 7, 19)(4, 16, 10, 21),$
 Id.

Appendix A

Programmes A1 and A2

We have included two main programmes written in Magma that were used in the construction of designs and codes from finite simple groups. All of our work was carried out on Sun workstations at the University of Natal and Clemson University with Magma versions 2.7 and 2.8. Here we first give a general purpose programme (Programme A1) used to find the designs and respective binary codes from primitive permutation representations of simple groups and then we list Programme A2 which was used to obtain the designs and codes from the alternating groups A_6 and A_9 , followed by the output of the respective designs and binary codes.

A.1 Programme A1

```
load simgps;
SetLogFile("G.out");
g:=SimGroup("G");
re:=SimRecord("G");
ma:=re'Max;
for k:=1 to #ma do
gk:=ma[k];
```

```

a1,a2,a3:=CosetAction(g,gk);
st:=Stabilizer(a2,1);
orbs:=Orbits(st);#orbs;
v:=Index(a2,st); v;
pr:=[divisors of order of G];
lo:=[#orbs[i]: i in [1..#orbs]];lo;
for j:=2 to #lo do
  "orbs no",j,"of length",#orbs[j];
  for l:=1 to #orbs do
    blox[l]:=Setseq(orbs[j]^a2);
    des[l]:=Design<1,v|blox[l]>; des[l];
    IsIsomorphic(des[l],des[l+1]);
    "des",des[l],"is isomorphic to",des[l+1];
    autdes:=AutomorphismGroup(des[l]);
    autdes; for i:=1 to #pr do
      p:=pr[i]; dc:=decode(v,blox,p);
      d1:=Dual(dc); d1:=Dim(dc);
      d2:=Dim(d1); d3:=Dim(dc meet d1);
      "p=",p,"dim=",d1,"dimdual=",d2,"hull=",d3;
    end for; end for; end for; end for;

```

A.2 Programme A2

```

//The program, where G=A6 or A9
load simgps;
g:=SimGroup('G');
re:=SimRecord('G');
ma:=re'Max;
'no. of prim. reps='',#ma;
for k:=1 to #ma do
k,'th prim. rep.';
gk:=ma[k];
a1,a2,a3:=CosetAction(g,gk);
st:=Stabilizer(a2,1);
orbs:=Orbits(st);
'no. of orbits='',#orbs;
v:=Index(a2,st);
'degree='',v;
pr:=[2,3,5,7];
lo:=[#orbs[i]: i in [1..#orbs]];
'seq. of orbit lengths='',lo;
for j:=2 to #lo do
'orbs no'',j,'of length'',#orbs[j];
blox:=Setseq(orbs[j]^a2);
des:=Design<1,v|blox>;des;
autdes:=AutomorphismGroup(des);
'autgp of order'',Order(autdes);
for i:=1 to #pr do
p:=pr[i];
dc:=LinearCode(des,GF(p));
d1:=Dual(dc); d1:=Dim(dc);
d2:=Dim(d1); d3:=Dim(dc meet d1);
'p='',p,'dim='',d1,'dimdual='',
d2,'hull='',d3;
if not ({d1,d2} subset {0,1,v-1,v})
then if i in {1} then
cau:=PermutationGroup(dc);
'perm gp of order'',Order(cau);
end if;end if;
end for; '-----';
end for; '.....';
end for;

//omiting the trivial designs and

```

```

//the natural representations
//Results for G=A6, of order 360
.....
$4 th prim. rep.
no. of orbits= 3
degree= 15
seq. of orbit lengths= [ 1, 6, 8 ]
orbs no 2 of length 6
1-(15, 6, 6) Design with 15 blocks
autgp of order 720
p= 2 dim= 14 dimdual= 1 hull= 0
p= 3 dim= 9 dimdual= 6 hull= 0
perm gp of order 720
p= 5 dim= 15 dimdual= 0 hull= 0
-----
orbs no 3 of length 8
1-(15, 8, 8) Design with 15 blocks
autgp of order 20160
p= 2 dim= 4 dimdual= 11 hull= 4
perm gp of order 20160
p= 3 dim= 15 dimdual= 0 hull= 0
p= 5 dim= 15 dimdual= 0 hull= 0
-----
.....
5 th prim. rep.
no. of orbits= 3
degree= 15
seq. of orbit lengths= [ 1, 6, 8 ]
orbs no 2 of length 6
1-(15, 6, 6) Design with 15 blocks
autgp of order 720
p= 2 dim= 14 dimdual= 1 hull= 0
p= 3 dim= 9 dimdual= 6 hull= 0
perm gp of order 720
p= 5 dim= 15 dimdual= 0 hull= 0
-----
orbs no 3 of length 8
1-(15, 8, 8) Design with 15 blocks
autgp of order 20160
p= 2 dim= 4 dimdual= 11 hull= 4
perm gp of order 20160
p= 3 dim= 15 dimdual= 0 hull= 0
p= 5 dim= 15 dimdual= 0 hull= 0

```

```

-----
//Results for G=A9 of order 181440
//omiting trivial designs
no. of prim. reps= 8
.....
2 th prim. rep.
no. of orbits= 3
degree= 36
seq. of orbit lengths= [ 1, 14, 21 ]
orbs no 2 of length 14
1-(36, 14, 14) Design with 36 blocks
autgp of order 362880
p= 2 dim= 8 dimdual= 28 hull= 0
perm gp of order 362880
p= 3 dim= 36 dimdual= 0 hull= 0
p= 5 dim= 28 dimdual= 8 hull= 0
p= 7 dim= 35 dimdual= 1 hull= 0
-----
orbs no 3 of length 21
1-(36, 21, 21) Design with 36 blocks
autgp of order 362880
p= 2 dim= 28 dimdual= 8 hull= 0
perm gp of order 362880
p= 3 dim= 27 dimdual= 9 hull= 0
p= 5 dim= 36 dimdual= 0 hull= 0
p= 7 dim= 35 dimdual= 1 hull= 0
-----
.....
3 th prim. rep.
no. of orbits= 4
degree= 84
seq. of orbit lengths= [ 1, 18, 20, 45 ]
orbs no 2 of length 18
1-(84, 18, 18) Design with 84 blocks
autgp of order 362880
p= 2 dim= 56 dimdual= 28 hull= 0
perm gp of order 362880
p= 3 dim= 34 dimdual= 50 hull= 7
p= 5 dim= 84 dimdual= 0 hull= 0
p= 7 dim= 84 dimdual= 0 hull= 0
-----
orbs no 3 of length 20

1-(84, 20, 20) Design with 84 blocks
autgp of order 362880
p= 2 dim= 48 dimdual= 36 hull= 0
perm gp of order 362880
p= 3 dim= 84 dimdual= 0 hull= 0
p= 5 dim= 75 dimdual= 9 hull= 0
p= 7 dim= 84 dimdual= 0 hull= 0
-----
orbs no 4 of length 45
1-(84, 45, 45) Design with 84 blocks
autgp of order 362880
p= 2 dim= 76 dimdual= 8 hull= 0
perm gp of order 362880
p= 3 dim= 34 dimdual= 50 hull= 7
p= 5 dim= 75 dimdual= 9 hull= 0
p= 7 dim= 57 dimdual= 27 hull= 8
-----
.....
4 th prim. rep.
no. of orbits= 3
degree= 120
seq. of orbit lengths= [ 1, 56, 63 ]
orbs no 2 of length 56
1-(120, 56, 56) Design with 120 blocks
autgp of order 348364800
p= 2 dim= 8 dimdual= 112 hull= 8
perm gp of order 348364800
p= 3 dim= 120 dimdual= 0 hull= 0
p= 5 dim= 120 dimdual= 0 hull= 0
p= 7 dim= 119 dimdual= 1 hull= 0
-----
orbs no 3 of length 63
1-(120, 63, 63) Design with 120 blocks
autgp of order 348364800
p= 2 dim= 120 dimdual= 0 hull= 0
p= 3 dim= 36 dimdual= 84 hull= 36
p= 5 dim= 120 dimdual= 0 hull= 0
p= 7 dim= 119 dimdual= 1 hull= 0
-----
.....
5 th prim. rep.
no. of orbits= 3
degree= 120

```

```

seq. of orbit lengths= [ 1, 56, 63 ]
orbs no 2 of length 56
1-(120, 56, 56) Design with 120 blocks
autgp of order 348364800
p= 2 dim= 8 dimdual= 112 hull= 8
perm gp of order 348364800
p= 3 dim= 120 dimdual= 0 hull= 0
p= 5 dim= 120 dimdual= 0 hull= 0
p= 7 dim= 119 dimdual= 1 hull= 0
-----
orbs no 3 of length 63
1-(120, 63, 63) Design with 120 blocks
autgp of order 348364800
p= 2 dim= 120 dimdual= 0 hull= 0
p= 3 dim= 36 dimdual= 84 hull= 36
p= 5 dim= 120 dimdual= 0 hull= 0
p= 7 dim= 119 dimdual= 1 hull= 0
-----
.....
6 th prim. rep.
no. of orbits= 5
degree= 126
seq. of orbit lengths=
[ 1, 5, 20, 40, 60 ]
orbs no 2 of length 5
1-(126, 5, 5) Design with 126 blocks
autgp of order 362880
p= 2 dim= 70 dimdual= 56 hull= 0
perm gp of order 362880
p= 3 dim= 99 dimdual= 27 hull= 0
p= 5 dim= 125 dimdual= 1 hull= 0
p= 7 dim= 126 dimdual= 0 hull= 0
-----
orbs no 3 of length 20
1-(126, 20, 20) Design with 126 blocks
autgp of order 362880
p= 2 dim= 56 dimdual= 70 hull= 0
perm gp of order 362880
p= 3 dim= 126 dimdual= 0 hull= 0
p= 5 dim= 125 dimdual= 1 hull= 0
p= 7 dim= 126 dimdual= 0 hull= 0
-----
orbs no 4 of length 40
1-(126, 40, 40) Design with 126 blocks
autgp of order 362880
p= 2 dim= 48 dimdual= 78 hull= 0
p= 3 dim= 99 dimdual= 27 hull= 0
p= 5 dim= 77 dimdual= 49 hull= 27
p= 7 dim= 99 dimdual= 27 hull= 8
-----
orbs no 5 of length 60
1-(126, 60, 60) Design with 126 blocks
autgp of order 362880
p= 2 dim= 74 dimdual= 52 hull= 26
p= 3 dim= 27 dimdual= 99 hull= 0
p= 5 dim= 125 dimdual= 1 hull= 0
p= 7 dim= 126 dimdual= 0 hull= 0
-----
.....
7 th prim. rep.
no. of orbits= 5
degree= 280
seq. of orbit lengths=
[ 1, 27, 36, 54, 162 ]
orbs no 2 of length 27
1-(280, 27, 27) Design with 280 blocks
autgp of order 362880
p= 2 dim= 232 dimdual= 48 hull= 0
p= 3 dim= 68 dimdual= 212 hull= 41
p= 5 dim= 280 dimdual= 0 hull= 0
p= 7 dim= 280 dimdual= 0 hull= 0
-----
orbs no 3 of length 36
1-(280, 36, 36) Design with 280 blocks
autgp of order 362880
p= 2 dim= 42 dimdual= 238 hull= 42
p= 3 dim= 252 dimdual= 28 hull= 0
p= 5 dim= 280 dimdual= 0 hull= 0
p= 7 dim= 280 dimdual= 0 hull= 0
-----
orbs no 4 of length 54
1-(280, 54, 54) Design with 280 blocks
autgp of order 362880
p= 2 dim= 48 dimdual= 232 hull= 0
p= 3 dim= 125 dimdual= 155 hull= 84
p= 5 dim= 280 dimdual= 0 hull= 0

```



```

p= 7 dim= 280 dimdual= 0 hull= 0
-----
orbs no 5 of length 162
1-(280, 162, 162) Design with 280 blocks
autgp of order 362880
p= 2 dim= 68 dimdual= 212 hull= 68
p= 3 dim= 41 dimdual= 239 hull= 41
p= 5 dim= 280 dimdual= 0 hull= 0
p= 7 dim= 280 dimdual= 0 hull= 0
-----
.....
8 th prim. rep.
no. of orbits= 12
degree= 840
seq. of orbit lengths=
[ 1, 8, 24, 24, 27, 36, 72, 72, 72, 72,
216, 216 ]
orbs no 2 of length 8
1-(840, 8, 8) Design with 840 blocks
autgp of order 362880
p= 2 dim= 530 dimdual= 310 hull= 112
p= 3 dim= 624 dimdual= 216 hull= 189
p= 5 dim= 651 dimdual= 189 hull= 56
p= 7 dim= 651 dimdual= 189 hull= 0
-----
orbs no 3 of length 24
1-(840, 24, 24) Design with 840 blocks
autgp of order 181440
p= 2 dim= 322 dimdual= 518 hull= 224
p= 3 dim= 699 dimdual= 141 hull= 21
p= 5 dim= 840 dimdual= 0 hull= 0
p= 7 dim= 840 dimdual= 0 hull= 0
-----
orbs no 4 of length 24
1-(840, 24, 24) Design with 840 blocks
autgp of order 181440
p= 2 dim= 322 dimdual= 518 hull= 224
p= 3 dim= 699 dimdual= 141 hull= 21
p= 5 dim= 840 dimdual= 0 hull= 0
p= 7 dim= 840 dimdual= 0 hull= 0
-----
orbs no 5 of length 27
1-(840, 27, 27) Design with 840 blocks

```

```

autgp of order 362880
p= 2 dim= 616 dimdual= 224 hull= 48
p= 3 dim= 446 dimdual= 394 hull= 41
p= 5 dim= 651 dimdual= 189 hull= 56
p= 7 dim= 784 dimdual= 56 hull= 0
-----
orbs no 6 of length 36
1-(840, 36, 36) Design with 840 blocks
autgp of order 362880
p= 2 dim= 608 dimdual= 232 hull= 190
p= 3 dim= 482 dimdual= 358 hull= 77
p= 5 dim= 771 dimdual= 69 hull= 21
p= 7 dim= 798 dimdual= 42 hull= 0
-----
orbs no 7 of length 72
1-(840, 72, 72) Design with 840 blocks
autgp of order 181440
p= 2 dim= 258 dimdual= 582 hull= 160
p= 3 dim= 182 dimdual= 658 hull= 141
p= 5 dim= 258 dimdual= 582 hull= 83
p= 7 dim= 259 dimdual= 581 hull= 0
-----
orbs no 8 of length 72
1-(840, 72, 72) Design with 840 blocks
autgp of order 181440
p= 2 dim= 546 dimdual= 294 hull= 176
p= 3 dim= 587 dimdual= 253 hull= 141
p= 5 dim= 840 dimdual= 0 hull= 0
p= 7 dim= 840 dimdual= 0 hull= 0
-----
orbs no 9 of length 72
1-(840, 72, 72) Design with 840 blocks
autgp of order 181440
p= 2 dim= 546 dimdual= 294 hull= 176
p= 3 dim= 587 dimdual= 253 hull= 141
p= 5 dim= 840 dimdual= 0 hull= 0
p= 7 dim= 840 dimdual= 0 hull= 0
-----
orbs no 10 of length 72
1-(840, 72, 72) Design with 840 blocks
autgp of order 181440
p= 2 dim= 258 dimdual= 582 hull= 160
p= 3 dim= 182 dimdual= 658 hull= 141

```

```
p= 5 dim= 258 dimdual= 582 hull= 83
p= 7 dim= 259 dimdual= 581 hull= 0
-----
orbs no 11 of length 216
1-(840, 216, 216) Design with 840 blocks
autgp of order 362880
p= 2 dim= 306 dimdual= 534 hull= 160
p= 3 dim= 230 dimdual= 610 hull= 230
p= 5 dim= 595 dimdual= 245 hull= 0
p= 7 dim= 595 dimdual= 245 hull= 0
-----
orbs no 12 of length 216
1-(840, 216, 216) Design with 840 blocks
autgp of order 362880
p= 2 dim= 418 dimdual= 422 hull= 98
p= 3 dim= 446 dimdual= 394 hull= 41
p= 5 dim= 554 dimdual= 286 hull= 104
p= 7 dim= 714 dimdual= 126 hull= 0
```

Appendix B

Generators for $O_8^+(2) : 2$

a = (1,2)(5,93)(6,89)(7,11)(8,65)
 (10,100)(12,63)(13,116)(14,53)
 (16,34)(17,40)(18,21)(19,38)(20,30)
 (22,111)(24,46)(25,45)(26,115)(27,52)
 (28,101)(29,69)(31,43)(32,97)(33,60)
 (35,88)(36,50)(37,44)(39,104)(41,99)
 (42,81)(47,94)(48,105)(49,95)(51,108)
 (54,118)(56,73)(57,120)(58,112)(59,62)
 (61,64)(66,113)(67,83)(70,87)(71,79)
 (75,102)(76,84)(78,91)(80,103)(82,110)
 (85,119)(92,98)(107,114), order 2;

b = (2,3)(5,93)(6,29)(7,60)(8,70)
 (10,58)(11,66)(12,30)(13,100)(14,53)
 (15,104)(16,21)(17,40)(18,19)(20,98)
 (22,111)(24,109)(25,45)(26,115)(27,78)
 (28,101)(32,97)(33,113)(34,38)(35,57)
 (36,44)(37,85)(41,99)(42,73)(43,74)
 (48,52)(50,119)(51,69)(54,118)(56,67)
 (59,106)(61,64)(63,92)(65,82)(68,95)
 (71,79)(72,94)(75,102)(76,120)(80,103)
 (81,83)(84,88)(87,110)(89,108)(91,105)
 (112,116)(114,117), order 2;

c = (3,29)(4,97)(6,24)(7,76)(8,93)
 (10,50)(11,62)(13,16)(14,103)(15,26)
 (17,74)(18,52)(19,95)(21,49)(22,90)
 (23,55)(25,77)(27,107)(28,113)(30,82)
 (31,100)(33,57)(34,61)(35,101)(36,47)
 (37,64)(38,105)(39,84)(40,79)(42,92)

(43,58)(44,78)(45,111)(46,108)(48,114)
 (53,68)(54,91)(59,60)(63,87)(65,99)
 (67,70)(71,72)(73,110)(75,115)(80,117)
 (81,96)(85,112)(86,98)(94,119)(102,106)
 (104,120)(116,118), order 2;

d = (5,41,93,99)(6,82,51,70)(7,76,60,
 120)(8,29,65,69)(10,50,58,119)(11,84,33,
 57)(12,67,30,56)(13,44,116,37)(14,80,53,
 103)(15,106)(16,78,34,91)(17,79,40,71)
 (18,52,19,48)(20,73,63,83)(21,27,38,105)
 (22,54,111,118)(23,55)(25,64,45,61)(26,
 102,115,75)(28,97,101,32)(31,47)(35,66,
 88,113)(36,112,85,100)(39,62)(42,92,81,
 98)(43,94)(49,107)(59,104)(68,117)(72,
 74)(77,90)(86,96)(87,89,110,108)(95,114),
 order 4;

e = (5,115)(7,56)(11,73)(12,76)(20,57)
 (22,45)(23,77)(25,111)(26,93)(30,120)(31,
 47)(33,83)(35,98)(41,75)(42,66)(43,94)(49,
 107)(54,61)(55,90)(60,67)(63,84)(64,118)
 (68,117)(72,74)(81,113)(88,92)(95,114)
 (99,102), order 2;

f = (8,106)(10,50)(11,63)(13,44)(14,103)
 (15,65)(16,78)(18,52)(22,90)(23,111)
 (25,77)(26,99)(28,86)(30,60)(35,81)
 (38,105)(39,110)(40,79)(45,55)(59,82)
 (62,87)(67,120)(70,104)(73,84)(85,112)

$(93, 102)(96, 101)(98, 113),$

order 2;

$g = (4, 77)(7, 10)(9, 55)(11, 100)(13, 66)$

$(15, 72)(17, 102)(22, 97)(26, 80)(27, 84)$

$(28, 61)(32, 111)(33, 112)(35, 91)(39, 47)$

$(40, 75)(48, 120)(49, 62)(52, 76)(57, 105)$

$(58, 60)(59, 95)(64, 101)(68, 106)$

$(78, 88)(94, 104)(103, 115)(113, 116),$

order 2;

$h = (10, 18)(13, 16)(14, 40)(17, 53)(19, 58)$

$(21, 100)(22, 25)(23, 55)(27, 36)(31, 49)$

$(34, 116)(37, 91)(38, 112)(43, 95)(44, 78)$

$(45, 111)(47, 107)(48, 119)(50, 52)(54, 64)$

$(61, 118)(68, 74)(71, 80)(72, 117)(77, 90)$

$(79, 103)(85, 105)(94, 114),$ order 2.

Appendix C

PD-sets Through Computation

Here we list a general programme which was used to obtain the PD-sets through computations for a t -error-correcting code, for small t , obtained from designs or graphs. For this we require the length of the code, the dimension, the minimum weight, and the automorphism group. Note that given a generator matrix for C the automorphism group can be obtained by using Magma.

```
qudecodeR.m
p=p-ary code
//C= code,
pdset=PD set for code
IV:=func< v, block,p|CharacteristicVector
(VectorSpace(GF(p),v), block) > ;
ba1:=Basis(C);
seq:=[];
d:=Dimension(C);
v:=Length(C);
for j:=1 to d do
b:=ba1[j];
seq:=seq cat [b[k]: k in [d+1..v]];
end for;
ma:=KMatrixSpace(GF(p),d,v-d);
sm:=ma!seq;
smt:=-Transpose(sm);
```

```

z:=[0:j in [1..v-d]];
seqn:=[];
for j:=1 to v-d do
r:=[smt[j][i]:i in [1..d]];
zj:=z;
zj[j]:=1;
rc:=r cat zj;
seqn:=seqn cat rc;
end for;
cseq:=&cat[Eltseq(ba1[i]):i in [1..d]];
man:=KMatrixSpace(GF(p),v-d,v);
ma1:=KMatrixSpace(GF(p),1,d);
ma2:=KMatrixSpace(GF(p),d,v);
ma3:=KMatrixSpace(GF(p),1,v-d);
hsmt:=man!seqn;
"check matrix";
H:=hsmt;
cs:=ma2!cseq;
f:=GF(p);
kset:={};
for i:=1 to 5 do
bb:=Random(C);
ers:=[];
for i:=1 to t do
ni:={Random({1..v})};
ai:=Random(f);
cc:=IV(v,ni,p);
ers:=Append(ers,ai*cc);
end for;
b:=bb + &+[ers[i]:i in [1..t]];
"sent....",bb;
"received.",b;
for k:=1 to #pdset do
e:=PDset[k];
seq1:=[];
for i:=1 to v-d do
seq1:=Append(seq1, InnerProduct(b^e,hsmt[i]));
end for;
s:={i:i in [1..v-d]|seq1[i] ne 0};
if #s le t then
k,"th pdset elt";
e;
#s,"errors";
kset:=kset join {k};
bee:=b^e;
aseq:=[bee[i]:i in [1..d]];
vv:=ma1!aseq;
r:=C!(vv*cs);
"corrected",r^(e^-1);
"It is",r^(e^-1) eq bb,
"that the corrected vector is the sent word";
break k;
end if;
end for;
"-----";
end for;

```

Appendix D

Minimum Weights

The output for computations of the minimum weights for the codes obtained from the rank-3 permutation representations of the symplectic groups $PSp_4(3)$ and $PSp_4(5)$ respectively. By using Programme A1 we have obtained the designs and codes from the rank-3 primitive permutation representations of $PSp_4(3)$ and $PSp_4(5)$ of degrees 40 and 156 respectively. The first items of the output refer to the number of orbits of a point stabilizer in the action of the groups and the second is the degree of the representation. The remaining items are self explanatory. These computations were used to deduce the bounds given in Theorem 7.2.11.

```
3
40
design:=Design<1,v|blocks>;
1-(40, 12, 12) Design with 40 blocks
Permutation group au acting on a set of cardinality 40
Order = 51840 = 2^7 * 3^4 * 5
p= 2 dim= 16 dimdual= 24 hull= 16
code:=LinearCode(design,GF(2));;
> wd:=WeightDistribution(code);
> wd;
[ <0, 1>, <8, 45>, <12, 1120>, <16, 15570>, <20, 32064>, <24, 15570>, <28,
1120>, <32, 45>, <40, 1> ]
> dual:=Dual(code);
```

```

> wdual:=WeightDistribution(dual);
> wdual;
[ <0, 1>, <6, 240>, <8, 2205>, <10, 23760>, <12, 182560>, <14, 664560>, <16,
2035170>, <18, 3243600>, <20, 4473024>, <22, 3243600>, <24, 2035170>, <26,
664560>, <28, 182560>, <30, 23760>, <32, 2205>, <34, 240>, <40, 1> ]
> quit;
Total time: 1.859 seconds
=====

3
156
design:=Design<1,v|blocks>;
1-(156, 30, 30) Design with 156 blocks
Permutation group au acting on a set of cardinality 156
Order = 9360000 = 2^7 * 3^2 * 5^4 * 13
p= 2 dim= 66 dimdual= 90 hull= 66
code:=LinearCode(design,GF(2));
> mdcode:=MinimumDistance(code);
> md;
12
Total time: 56091.750 seconds
=====

3
156
design:=Design<1,v|blocks>;
1-(156, 30, 30) Design with 156 blocks
Permutation group au acting on a set of cardinality 156
Order = 9360000 = 2^7 * 3^2 * 5^4 * 13
p= 2 dim= 66 dimdual= 90 hull= 66
code:=LinearCode(design,GF(2));
> dual:=Dual(code);
> mdual:=MinimumDistance(dual);
> mdual;
10
Total time: 115125.059 seconds

```


Appendix E

Gordon Bound

Here we give the Gordon bound for the PD-sets obtained for the codes from the triangular graph $T(n)$ for $n \geq 6$ and even. The first column gives the value of n , with n an even integer, the second the code length, the third the number of errors corrected, the fourth the value of the Gordon bound, the fifth the size of the PD-set we constructed, and the last column gives the order of S_n .

n,	length,	n-3,	Gordon,	PDset,	S_n
6	15	3	5	26	720
8	28	5	8	50	40320
10	45	7	11	82	3628800
12	66	9	15	122	479001600
14	91	11	18	170	87178291200
16	120	13	22	226	20922789888000
18	153	15	26	290	6402373705728000
20	190	17	29	362	2432902008176640000
22	231	19	33	442	1124000727777607680000
24	276	21	36	530	620448401733239439360000
26	325	23	40	626	403291461126605635584000000
28	378	25	43	730	304888344611713860501504000000
30	435	27	48	842	265252859812191058636308480000000
32	496	29	51	962	263130836933693530167218012160000000
34	561	31	55	1090	295232799039604140847618609643520000000
36	630	33	58	1226	371993326789901217467999448150835200000000
38	703	35	62	1370	523022617466601111760007224100074291200000000

40 780 37 65 1522 815915283247897734345611269596115894272000000000

Appendix F

$w(\pi)$ for Lemma 9.2.14

The table below shows the ordering of the vectors $w(\pi)$ as given in Lemma 9.2.14, in the case $n = 9$. Read down the successive columns. The leading terms, corresponding to pivot positions, can be read from the first, third and fifth elements in each block: thus the block $[1\ 7\ 2\ 8\ 5\ 9]$ has leading term $\{1, 2, 5\}$.

1	7	2	8	3	9		2	7	3	8	4	9		3	7	4	8	5	9
1	7	2	8	4	9		2	7	3	8	5	9		3	7	4	8	6	9
1	7	2	8	5	9		2	7	3	8	6	9		3	6	4	8	7	9
1	7	2	8	6	9		2	6	3	8	7	9		3	6	4	7	8	9
1	6	2	8	7	9		2	6	3	7	8	9		3	7	5	8	6	9
1	6	2	7	8	9		2	7	4	8	5	9		3	6	5	8	7	9
1	7	3	8	4	9		2	7	4	8	6	9		3	6	5	7	8	9
1	7	3	8	5	9		2	6	4	8	7	9		3	5	6	8	7	9
1	7	3	8	6	9		2	6	4	7	8	9		3	5	6	7	8	9
1	6	3	8	7	9		2	7	5	8	6	9		4	7	5	8	6	9
1	6	3	7	8	9		2	6	5	8	7	9		4	6	5	8	7	9
1	7	4	8	5	9		2	6	5	7	8	9		4	6	5	7	8	9
1	7	4	8	6	9		2	5	6	8	7	9		4	5	6	8	7	9
1	6	4	8	7	9		2	5	6	7	8	9		4	5	6	7	8	9
1	6	4	7	8	9														
1	7	5	8	6	9														
1	6	5	8	7	9														
1	6	5	7	8	9														
1	5	6	8	7	9														
1	5	6	7	8	9														

Appendix G

Construction of codes from graphs

The programme that follows was used to construct the graphs on triples and their respective codes. With appropriate changes it can be used to construct the triangular graph and its code.

```
SetLogFile{"duads_out"};
//give value to n
pts=[];
for i:=1 to n-3 do
for j:=i+1 to n-2 do
for k:=j+1 to n-1 do
for l:=k+1 to n do
pts:=Append(pts,{i,j,k,l});
end for;
end for;
end for;
end for;
v:=#pts;
blox0=[];
blox1=[];
blox2=[];
blox3=[];
for i:=1 to v do
```

```

    bl:={};bla:={};
    blc:={};bld:={};
    for j:=1 to v do
        ss:=pts[j];
    if #(pts[i] meet ss) eq 0 then
        bl:=bl join {j};
    elif #(pts[i] meet ss) eq 1 then
        bla:=bla join {j};
    end if;
    if #(pts[i] meet ss) eq 2 then
        blc:=blc join {j};
    elif #(pts[i] meet ss) eq 3 then
        bld:=bld join {j};
    end if;
    end for;
    blox0:=Append(blox0,bl);
    blox1:=Append(blox1,bla);
    blox2:=Append(blox2,blc);
    blox3:=Append(blox3,bld);
    end for;
p:=2;

//blox;
des:=Design<1,v|blox0>;des;
au:=AutomorphismGroup(des);au;
co:=LinearCode(des,GF(2));
cod:=Dual(co);
d1:=Dim(co);d2:=Dim(cod);
d3:=Dim(co meet cod);
"p=",p,"dim=",d1,"dimdual=",d2,"hull=",d3;
mco:=MD(co);mco;
mcod:=MD(cod);mcod;
dse:=Design<1,v|blox1>;dse;
aut:=AutomorphismGroup(dse);aut;
c1:=LinearCode(dse,GF(2));
c1d:=Dual(c1);
d11:=Dim(c1);d22:=Dim(c1d);
d33:=Dim(c1 meet c1d);
"p=",p,"dim=",d11,"dimdual=",d22,"hull=",d33;
mc1:=MD(c1);mc1;
mc1d:=MD(c1d);mc1d;
dsc:=Design<1,v|blox2>;dsc;
autdes:=AutomorphismGroup(dsc);autdes;

```

```

c2:=LinearCode(dsc,GF(2));
c2d:=Dual(c2);
d12:=Dim(c2);d21:=Dim(c2d);
d31:=Dim(c2 meet c2d);
"p=",p,"dim=",d12,"dimdual=",d21,"hull=",d31;
mc2:=MD(c2);mc2;
mc2d:=MD(c2d);mc2d;

dsd:=Design<1,v|blox3>;dsd;
autd:=AutomorphismGroup(dsd);autd;
c3:=LinearCode(dsd,GF(2));
c3d:=Dual(c3);
d32:=Dim(c3);d34:=Dim(c3d);
d35:=Dim(c3 meet c3d);
"p=",p,"dim=",d32,"dimdual=",d34,"hull=",d35;
mc3:=MD(c3);mc3;
mc3d:=MD(c3d);mc3d;

```

Appendix H

Constructing the Chang codes

Here we give the programme which was used to construct the Chang graphs from $T(8)$ by using the notion of switching as given in Definition 10.4.1. Also by using this programme we were able to construct the binary codes associated with each of the three Chang graphs. Notice that the notations mset1, mset2 and mset3 in the programme correspond to disjoint edges, an octagon, and a disjoint union of a pentagon and a triangle (see Section 10.4.2).

```
pts:={{1,2},{1,3},{1,4},{1,5},{1,6},
{1,7},{1,8},{2,3},{2,4},{2,5},{2,6},
{2,7},{2,8},{3,4},{3,5},{3,6},{3,7},
{3,8},{4,5},{4,6},{4,7},{4,8},{5,6},
{5,7},{5,8},{6,7},{6,8},{7,8}};
```

```
mat:=MatrixRing(Integers(),28);
sj:=[1:j in [1..28*28]];
jmat:=mat!sj;
maq:=MatrixRing(Rationals(),28);
oblox:=[];
for i:=1 to 28 do
  bl:={};
  for j:=1 to 28 do
    s:=pts[j];
    if #(pts[i] meet s) eq 1 then
```

```

bl:=bl join {j};
end if; end for;
oblox:=Append(oblox,bl); end for;
oblox;
ndes:=Design<1,28|oblox>;
ma:=IncidenceMatrix(ndes);
a1:=ma;
b1:=jmat-a1;
c1:=b1-a1;
mset1:={1,14,23,28};
mset2:={1,7,8,14,19,23,26,28};
mset3:={2,14,3,10,23,26,28,13};
ch1:=c1;
for i:=1 to 28 do
bl:=ch1[i];
for x in mset do
bl[x]:=bl[x]*(-1);
end for;
ch1[i]:=bl; end for;
for x in mset do
ch1[x]:=(-1)*ch1[x]; end for;
ch1;
ch2:=(-1)*ch1;
cha:=ch2+jmat;
cha3:=(1/2)*cha;
des1:=Design<1,28|cha3>;
descha3;
cod:=LinearCode(descha3,GF(2));

```


Appendix I

A PD-set for the Chang 2 code

Here we give the output of the computations for a PD-set for the Chang 2 code. The computations were carried out using the programmes listed in Appendices H and C respectively.

(1,20,4,21,14,9,5,19,6,2)(3,8,16,15,17)(7,22)(10,25,23,27,26)(11,28,13,24,12),
(1,18,9,7,8,22)(2,5,3,20,14,16)(4,15,19)(6,17,21)(10,12)(11,27)(13,24)(25,28),
(1,18,20,4,3,9,7,16,19,14,8,22,5,15,2)(6,17,21)(10,13,24,12,23)(11,26,27,28,25),
(1,9,8)(2,18,14,22,3,7)(4,20,15,5,19,16)(6,21,17)(10,24)(11,26)(12,23)(25,27),
(1,18,4,8,7,15)(2,20,21)(3,5,17,14,16,6)(9,22,19)(10,24,11)(12,27,13)(23,25,28),
(1,4)(2,21)(3,17)(6,14)(8,15)(9,19)(10,27)(11,13)(12,24)(23,25),
(1,18,14,8,7,3)(2,9,22)(4,16,6,15,5,17)(10,24,28)(11,23,25)(12,26,27)(19,20,21),
(1,21)(2,14)(4,20)(5,19)(6,9)(7,22)(8,17)(10,26)(11,24)(13,28)(15,16)(25,27),
(1,20,18,4,21,8,5,22,15,6,9,16,7,19,17)(2,3,14)(10,26,13,23,28)(11,27,25,24,12),
(1,18,4,3,6,8,7,15,14,17)(2,21,9,22,19)(5,16)(10,28,27,13,11)(12,23,26,25,24),
(1,20,3)(2,8,5)(4,22,17)(6,19,18)(7,21,15)(9,16,14)(10,24,26)(12,28,27)(13,25,23),
(1,3,4,8,14,15)(2,19,9)(5,17,7,16,6,18)(11,24,26)(12,25,28)(13,23,27)(20,21,22),
(1,20,4,9,5,19)(2,6,22,14,21,7)(3,17,18)(8,16,15)(10,25,12)(11,13,26)(23,27,24),
(1,8,9)(2,6,18,19,5,3,21,7,15,20,14,17,22,4,16)(10,25,13,27,24)(11,12,23,26,28),
(1,20,8,5,9,16)(2,3,14)(4,19,15)(6,22,17,7,21,18)(10,23)(12,27)(13,26)(24,25),
(1,20)(2,4)(3,15)(5,9)(6,21)(7,22)(8,16)(10,23)(11,28)(12,13)(14,19)(26,27),
(2,17)(3,21)(5,7)(6,14)(8,9)(10,27)(11,23)(13,25)(15,19)(16,22)(18,20)(26,28),
(1,9)(2,14)(4,22)(5,21)(6,20)(7,19)(10,13)(11,12)(15,18)(16,17)(23,28)(24,27),
(1,20,3,7,19,8,5,2,18,4,9,16,14,22,15)(6,21,17)(10,24,23,13,12)(11,27,25,26,28),
(1,3,21)(2,6,8)(4,18,20)(5,15,22)(7,16,19)(9,14,17)(10,28,25)(11,24,23)(13,26,27),
(1,6,7)(2,20,19)(3,16,15)(4,14,5)(8,17,18)(9,21,22)(10,26,12)(11,13,25)(24,27,28),

$(1, 4, 6, 7, 14)(2, 9, 19, 21, 22)(3, 8, 15, 17, 18)(10, 27, 11, 28, 13)(12, 26, 24, 23, 25),$
 $(1, 18, 14, 17, 5, 8, 7, 3, 6, 16)(2, 21, 20, 9, 22)(4, 15)(10, 11, 23, 27, 12)(13, 28, 26, 25, 24),$
 $(1, 19, 6, 22, 14, 9, 4, 21, 7, 2)(3, 8, 15, 17, 18)(5, 20)(10, 27, 11, 28, 13)(12, 26, 24, 23, 25),$
 $(1, 3, 22, 6, 15, 9, 14, 18, 21, 4, 8, 2, 7, 17, 19)(5, 16, 20)(10, 13, 28, 11, 27)(12, 25, 23, 24, 26),$
 $(1, 14, 7)(2, 18, 9, 3, 22, 8)(4, 6, 5)(10, 28, 24)(11, 25, 23)(12, 27, 26)(15, 21, 16, 19, 17, 20),$
 $(1, 4, 7, 14, 5)(2, 20, 9, 19, 22)(3, 16, 8, 15, 18)(10, 12, 13, 23, 24)(11, 28, 26, 25, 27),$
 $(2, 17, 22, 15, 20, 3, 21, 18, 19, 16)(4, 5, 14, 6, 7)(8, 9)(10, 25, 13, 27, 24)(11, 12, 23, 26, 28),$
 $(1, 17, 7, 8, 6, 18)(2, 20, 19)(3, 5, 15, 14, 16, 4)(9, 21, 22)(10, 26, 12)(11, 13, 25)(24, 27, 28),$
 $(1, 4, 5)(2, 18, 21, 3, 22, 17)(6, 14, 7)(8, 19, 16, 9, 15, 20)(10, 12, 25)(11, 26, 13)(23, 24, 27),$
 $(1, 4)(2, 3)(5, 7)(8, 19)(9, 15)(11, 25)(12, 24)(13, 23)(16, 22)(17, 21)(18, 20)(26, 28),$
 $(1, 4, 6)(2, 18, 20, 3, 22, 16)(5, 14, 7)(8, 19, 17, 9, 15, 21)(10, 11, 25)(12, 26, 13)(23, 28, 24),$
 $(1, 18, 20)(2, 4, 17)(3, 19, 6)(5, 8, 22)(7, 16, 9)(10, 11, 26)(12, 25, 13)(14, 15, 21)(23, 27, 28),$
 $(1, 4, 14, 5, 6)(2, 20, 21, 9, 19)(3, 16, 17, 8, 15)(10, 23, 26, 25, 27)(11, 13, 12, 28, 24),$
 $(1, 14, 5, 7, 6)(2, 16, 22, 17, 9, 3, 20, 18, 21, 8)(10, 23, 12, 11, 27)(13, 26, 24, 28, 25)(15, 19),$
 $(1, 2, 15, 5, 22, 8, 14, 19, 16, 7, 9, 3, 4, 20, 18)(6, 21, 17)(10, 23, 12, 24, 13)(11, 25, 28, 27, 26),$
 $(1, 17, 14, 15, 7, 8, 6, 3, 4, 18)(2, 19, 22, 9, 21)(5, 16)(10, 11, 13, 27, 28)(12, 24, 25, 26, 23),$
 $\text{Id},$

Bibliography

- [1] E. Artin, *Geometric Algebra*, Wiley Interscience, New York, 1957.
- [2] M. Aschbacher, *Finite Group Theory*, Cambridge Studies in Advance Mathematics, vol. 10, Cambridge University Press, Cambridge, 1986.
- [3] E. F. Assmus, Jr. and J. D. Key, *Designs and their Codes*, Cambridge Tracts in Mathematics, vol. 103, Cambridge University Press, Cambridge, 1992, (Second printing with corrections, 1993).
- [4] E. F. Assmus, Jr. and J. D. Key, *Designs and codes: an update*, Des. Codes Cryptogr. **9** (1996), 7–27.
- [5] E. F. Assmus, Jr. and J. D. Key, *Polynomial Codes and Finite Geometries*, Handbook of Coding Theory (V. S. Pless and W. C. Huffman, eds.), vol. 2, Elsevier, 1998, Part 2, pp. 1269–1343.
- [6] B. Bagchi, *A regular two-graph admitting the Hall-Janko-Wales group*, Sankhyā, Ser. A **54** (1992), 35–45, Combinatorial mathematics and applications (Calcutta, 1988).
- [7] B. Bagchi, A. E. Brouwer and H. A. Wilbrink, *Notes on binary codes related to $O(5, q)$ generalized quadrangles for odd q* , Geom. Dedicata **39** (1991), 339–355.

- [8] M. K. Bennett, *Affine and projective geometry*, Wiley-Interscience, New York, 1995.
- [9] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Cambridge University Press, Cambridge, 1993.
- [10] N. L. Biggs and A. T. White, *Permutation Groups and Combinatorial Structures*, Cambridge University Press, London, Cambridge, 1979, London Math. Soc. Lecture Note Series 33.
- [11] W. Bosma and J. Cannon, *Handbook of Magma Functions*, Department of Mathematics, University of Sydney, November 1994.
- [12] P. L. H. Brooke, *On matrix representations and codes associated with the simple group of order 25920*, J. Algebra **91** (1984), 536–566.
- [13] P. L. H. Brooke, *On the Steiner system $S(2, 4, 28)$ and codes associated with the simple group of order 6048*, J. Algebra **97** (1985), 376–406.
- [14] A. E. Brouwer, *Strongly regular graphs*, The CRC Handbook of Combinatorial Designs (Charles J. Colbourn and Jeffrey H. Dinitz, eds.), CRC Press, Boca Raton, 1996, VI.5, pp. 667–685.
- [15] A. E. Brouwer and C. J. van Eijl, *On the p -rank of the adjacency matrices of strongly regular graphs*, J. Algebraic Combin. **1** (1992), 329–346.
- [16] A. E. Brouwer and J.H. van Lint, *Strongly regular graphs and partial geometries*, Enumeration and Design (D.M. Jackson and S.A. Vanstone, eds.), Academic Press, Toronto, 1984, Proc. Silver Jubilee Conf. on Combinatorics, Waterloo, 1982, pp. 85–122.
- [17] A. R. Calderbank and D. B. Wales, *A global code invariant under the Higman-Sims group*, J. Algebra **75** (1982), 233–260.

- [18] N. J. Calkin, J. D. Key and M. J. de Resmini, *Minimum weight and dimension formulas for some geometric codes*, Des. Codes Cryptogr. **17** (1999), 105–120.
- [19] P. J. Cameron, *Finite permutation groups and finite simple groups*, Bull. London Math. Soc. **13** (1981), 1–22.
- [20] P. J. Cameron, *Groups, Graph Connections* (Lowell W. Beineke and Robin J. Wilson, eds.), Clarendon Press, Oxford, 1997, Chapter 9, pp. 128–140.
- [21] P. J. Cameron, *Permutation Groups*, Cambridge University Press, Cambridge, 1999, London Math. Soc. Student Texts 45.
- [22] P. J. Cameron and J. H. van Lint, *Designs, Graphs, Codes and their Links*, Cambridge University Press, Cambridge, 1991, London Math. Soc. Student Texts 22.
- [23] R. W. Carter, *Simple Groups of Lie Type*, London and New York, Wiley-Interscience, 1972.
- [24] H. Chabanne, *Permutation decoding of abelian codes*, IEEE Trans. Inform. Theory **38** (1992), 1826–1829.
- [25] K. L. Clark, *Bounds for the minimum weight of the dual codes of some class of designs*, Ph.D. thesis, Clemson University, S. C., 2000.
- [26] K. L. Clark and J. D. Key, *Geometric codes over fields of odd prime power order*, Congr. Numer. **137** (1999), 177–186.
- [27] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of Finite Groups*, Oxford University Press, Oxford, 1985.
- [28] J.H. Conway and N. J. Sloane, *Sphere Packings, Lattices and Groups*, Springer Verlag, New York, 1988.

- [29] R. T. Curtis, *On graphs and codes*, Geom. Dedicata **41** (1992), no. 2, 127–134.
- [30] R. T. Curtis and T. R. Morris, *Codes, Graph Connections*, Oxford Lecture Ser. Math. Appl., vol. 5, Oxford University Press, New York, 1997, pp. 116–127.
- [31] P. Delsarte, *A geometric approach to a class of cyclic codes*, J. Combin. Theory **6** (1969), 340–358.
- [32] P. Delsarte, *On cyclic codes that are invariant under the general linear group*, IEEE Trans. Information Theory **16** (1970), 760–769.
- [33] P. Delsarte, *BCH bounds for a class of cyclic codes*, SIAM J. Appl. Math. **19** (1970), 420–429.
- [34] P. Delsarte, *Majority logic decodable codes derived from finite inversive planes*, Inform. and Control **18** (1971), 319–325.
- [35] P. Delsarte and J. M. Goethals, *On a class of majority-logic decodable cyclic codes*, IEEE Trans. Information Theory **14** (1968), 182–188.
- [36] P. Delsarte, J. M. Goethals and F. J. MacWilliams, *On the generalized Reed-Muller codes and their relatives*, Inform. and Control **16** (1970), 403–442.
- [37] P. Dembowski, *Finite Geometries*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44, Springer-Verlag, Berlin, Heidelberg, New York, 1968.
- [38] U. Dempwolff, *Primitive rank-3 groups on symmetric designs*, Des. Codes and Cryptogr. **22** (2001), 191–207.
- [39] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Dover Publications, New York, 1958, With an introduction by Wilhelm Magnus.

- [40] J. Dieudonné, *La Géométrie des Groupes Classiques*, Second ed., Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Band 5, Springer-Verlag, Berlin, Göttingen, Heidelberg, 1963.
- [41] J. Dieudonné, *Sur les Groupes Classiques*, Third ed., Actualités scientifiques et industrielles 1040, Hermann, Paris, 1973.
- [42] P. Ding and J. D. Key, *Minimum-weight codewords as generators of generalized Reed-Muller codes*, IEEE Trans. Inform. Theory **46** (2000), 2152–2158.
- [43] J. D. Dixon and B. Mortimer, *Permutation Groups*, Springer Verlag, New York, 1996.
- [44] L. Finkelstein and A. Rudvalis, *Maximal subgroups of the Hall-Janko-Wales group*, J. Algebra **24** (1977), 486–493.
- [45] S. Gao and J. D. Key, *Bases of minimum-weight vectors for codes from designs*, Finite Fields Appl. **4** (1998), 1–15.
- [46] D. M. Gordon, *Minimal permutation sets for decoding the binary Golay codes*, IEEE Trans. Inform. Theory **28** (1982), 541–543.
- [47] R. Gow, *Some characters of affine subgroups of classical groups*, J. London Math. Soc **2** (1976), 231–236.
- [48] R. M. Guralnick, K. Magaard, J. Saxl and P. H. Tiep, *Cross characteristic representations of odd characteristic symplectic groups and unitary groups*, J. Algebra, to appear.
- [49] W. H. Haemers, C. Parker, V. Pless and V. D. Tonchev, *A design and a code invariant under the simple group Co_3* , J. Combin. Theory, Ser. A **62** (1993), no. 2, 225–233.

- [50] W. H. Haemers, R. Peeters and J. M. van Rijkevorsel, *Binary codes of strongly regular graphs*, Des. Codes Cryptogr. **17** (1999), 187–209.
- [51] D. G. Higman, *Finite permutation groups of rank 3*, Math. Z. **86** (1964), 145–156.
- [52] R. Hill, *A First Course in Coding Theory*, Oxford Applied Mathematics and Computing Science Series, Oxford University Press, Oxford, 1986.
- [53] W. C. Huffman, *Codes and Groups*, Handbook of Coding Theory (V. S. Pless and W. C. Huffman, eds.), vol. 2, Elsevier, 1998, Part 2, pp. 1345–1440.
- [54] D. R. Hughes and F. C. Piper, *Design Theory*, Cambridge University Press, Cambridge, 1985.
- [55] B. Huppert, *Endliche Gruppen I*, Springer Verlag, Berlin, Heidelberg, 1967.
- [56] Z. Janko, *A new finite simple group with abelian Sylow subgroups and its characterization*, J. Algebra **32** (1996), 147–186.
- [57] W. M. Kantor, *Classification of 2-transitive symmetric designs*, Graphs and Combin. **1** (1985), 165–166.
- [58] W. M. Kantor and R. A. Liebler, *The rank-3 permutation representations of the finite classical groups*, Trans. American Math. Soc. **271** (1982), 1–71.
- [59] G. T. Kennedy and V. Pless, *A coding theoretic approach to extending designs*, Discrete Math. **142** (1995), 155–168.
- [60] J. D. Key, *Permutation decoding: an update*, <http://www.ces.clemson.edu/~keyj/Key/PDsets/PDupdate.pdf>, unpublished.
- [61] J. D. Key, *Codes and finite geometries*, Congress Num. **131** (1998), 85–89.

- [62] J. D. Key, *Some error-correcting codes and their applications*, Applied Mathematical Modeling: A Multidisciplinary Approach (D. R. Shier and K. T. Wallenius, eds.), CRC Press, Boca Raton, FL, 2000, pp. 291–314.
- [63] J. D. Key and M. J. de Resmini, *Codewords for a projective plane from sets of type (s, t)* , European J. Combin. **15** (1994), 259–268.
- [64] J. D. Key and M. J. de Resmini, *Small sets of even type and codewords*, J. Geom. **61** (1998), 83–104.
- [65] J. D. Key and M. J. de Resmini, *Ternary dual codes of the planes of order nine*, J. Statist. Plann. Inference **95** (2001), 229–236.
- [66] J. D. Key and J. Moori, *Designs, codes and graphs from the Janko groups J_1 and J_2* , J. Combin. Math and Combin. Comput. **40** (2002), 143–159.
- [67] J. D. Key, J. Moori and B. G. Rodrigues, *Binary codes from graphs on triples*, submitted.
- [68] J. D. Key, J. Moori and B. G. Rodrigues, *Binary codes of triangular graphs and permutation decoding*, submitted.
- [69] J. D. Key, J. Moori and B. G. Rodrigues, *On some designs and codes from primitive representations of some finite simple groups*, J. Combin. Math and Combin. Comput., to appear.
- [70] J. D. Key, J. Moori and B. G. Rodrigues, *Permutation decoding for binary codes from graphs on triples*, in preparation.
- [71] J. D. Key, J. Moori and B. G. Rodrigues, *Some binary codes from symplectic geometry of odd characteristic*, submitted.
- [72] J. D. Key and B. G. Rodrigues, *Permutation decoding and small unitals*, unpublished.

- [73] P. Kleidman and M. W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, Cambridge University Press, Cambridge, 1990, London Math. Soc. Lecture Notes, 129.
- [74] W. Knapp and P. Schmid, *Codes with prescribed permutation group*, J. Algebra **67** (1980), 415–435.
- [75] J. M. Lataille, P. Sin and P. H. Tiep, *The modulo 2 structure of rank 3 permutation modules for odd characteristic symplectic groups*, J. Algebra, to appear.
- [76] M. W. Liebeck, *The affine permutation groups of rank three*, Proc. London Math. Soc. **54** (1987), no. 3, 477–516.
- [77] M. W. Liebeck and J. Saxl, *The finite permutation groups of rank three*, Bull. London Math. Soc. **18** (1986), 165–172.
- [78] D. Livingstone and A. Wagner, *Transitivity of finite permutation groups on unordered sets*, Math. Z. **90** (1965), 393–403.
- [79] F. J. MacWilliams, *Permutation decoding of systematic codes*, Bell System Tech. J. **43** (1964), 485–505.
- [80] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1983.
- [81] J. L. Massey, *Threshold Decoding*, The M.I.T. Press, 1963.
- [82] V. Pless, *Introduction to the Theory of Error Correcting Codes*, Third ed., Wiley Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons Inc, New York, 1998.
- [83] C. E. Praeger and L. H. Soicher, *Low Rank Representations and Graphs for Sporadic Groups*, Cambridge University Press, Cambridge, 1997.

- [84] B. G. Rodrigues, *On the Theory and Examples of Group Extensions*, Master's thesis, University of Natal, Pietermaritzburg, 1999.
- [85] J. J. Rotman, *An Introduction to the Theory of Groups*, Fourth ed., Springer-Verlag, New York, Inc., 1995.
- [86] L. D. Rudolph, *A class of majority logic decodable codes*, IEEE Trans. Information Theory **13** (1967), 305–307.
- [87] J. J. Seidel, *Strongly regular graphs*, Surveys in Combinatorics, Proc. 7th Brit. Comb. Conf. (B. Bollobás, ed.), Cambridge, 1979, London Math. Soc. Lecture Note Series 38, pp. 157–180.
- [88] C. E. Shannon, *A mathematical theory of communication*, Bell System Tech. J. **27** (1948), 379–423, 623–656.
- [89] R. Steinberg, *Automorphisms of finite linear groups*, Canad. J. Math. **12** (1960), 606–615.
- [90] M. Suzuki, *Group Theory I*, Springer-Verlag, New York, 1982.
- [91] D. E. Taylor, *The Geometry of the Classical Groups*, Sigma Series in Pure Mathematics, vol. 9, Heldermann Verlag, Berlin, 1992.
- [92] V. D. Tonchev, *Combinatorial Configurations Designs, Codes, Graphs*, Pitman Monographs and Surveys in Pure and Applied Mathematics, No. 40, Longman, New York, 1988, Translated from the Bulgarian by Robert A. Melter.
- [93] T. Tsuzuku, *Finite Groups and Finite Geometries*, Cambridge Tracts in Mathematics, vol. 78, Cambridge University Press, 1982.
- [94] H. Whitney, *Congruent graphs and the connectivity of graphs*, Amer. J. Math. **54** (1932), 154–168.

- [95] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.
- [96] J. Wolfman, *A permutation decoding of the $(24, 12, 8)$ Golay code*, IEEE Trans. Inform. Theory **29** (1983), 748–750.

Index

- action on a set, 10
- blocks of imprimitivity, 14
- bound
 - Gordon, 44, 127, 130
 - Singleton, 26
- characteristic function, 49
- code
 - automorphism group, 28
 - automorphism of, 28
 - block, 25
 - cyclic, 45
 - doubly-even, 28
 - dual, 27
 - equivalent, 26
 - from graphs on triples, 99
 - from symplectic group, 78
 - from triangular graph, 91
 - Golay, 46
 - Hamming, 137
 - hull of, 28
 - isomorphic, 26
 - linear, 26
 - minimum weight, 26
 - of a design, 49
 - orthogonal, 27
 - p-rank, 49
 - self-orthogonal, 28
 - weight, 26
- codewords, 25
- collineation, 37
- decoding
 - majority logic, 40
 - nearest neighbour, 40
 - permutation, 42
 - syndrome, 40
- design, 29
 - automorphism group, 31
 - self-dual, 31
 - simple, 30
 - symmetric, 31
 - trivial, 30
- dimension
 - affine, 38
 - code, 26
 - projective, 36

distance

Hamming, 25

minimum, 25

duads, 22, 89

form

alternating, 17

bilinear, 17

non-degenerate, 18

symplectic, 17

fundamental theorem

affine geometry, 38

projective geometry, 37

geometry

affine, 38

projective, 36

graph, 33

automorphism group, 34

Chang, 139

complement, 33

complete, 34

line, 34

null, 34

rank-3, 35

regular, 33

strongly regular, 33

triangular, 34

valency, 33

vertex-transitive, 34

Grassman's identity, 36

group

J_1 , 61

J_2 , 61

k -transitive, 12

affine semilinear, 25

automorphism, 13

doubly transitive, 10

general linear, 25

imprimitive, 15

permutation, 9

primitive, 15

projective semilinear, 25

projective symplectic, 20

rank, 10

semilinear, 25

Singer, 37, 138

symmetric, 9

symplectic, 20

transitive, 9

hyperplanes, 36

incidence structure, 29

invariant

G , 14

multiset, 140

partitions, 14

isotropic

point, 21

- vectors, 19
- Janko groups, 61
- k-homogeneous, 22
- lines, 36
- matrix
 - adjacency, 34
 - check, 27
 - generator, 27
 - incidence, 30
 - inner product, 19
- maximal isotropic subspace, 21
- orbit, 9
- orbital, 10
 - digraph, 10
- orbitals, 10
- orthogonal
 - complement, 18
 - vectors, 18
- parallel r-flats, 38
- permutation
 - faithful representation, 11
 - representation, 10
- point
 - absolute, 21
 - totally isotropic, 21
- points, 36
- polarity, 20
- q-ary code, 25
- r-flat, 38
- radical, 18
- rank r , 34
- redundancy, 28
- replication number, 31
- semilinear transformation, 24
- Singer
 - cycle, 37
 - group, 37
- space
 - affine, 38
 - inner product, 17
 - projective, 36
 - symplectic, 18
- stabilizer, 10
- subdegrees, 10
- suborbits, 10
- subspace
 - isotropic, 21
 - non-isotropic, 21
 - totally isotropic, 21
- support set, 49
- switching, 139
- symbols
 - check, 27

- information, 27
- symmetric q -ary channel, 39
- syndrome, 27
- trivial partitions, 14
- vector
 - all-one, 28
 - constant, 28
 - incidence, 30
- weight
 - distribution, 26
 - enumerator, 26
- words, 25