Codes Related to and Derived from Hamming Graphs

by

Thifhelimbilu Ronald Muthivhi

Thesis submitted in fulfillment of the requirements
for the degree of
Master of Science in Mathematics
in the
Department of Mathematics and Applied Mathematics
University of the Western Cape

Supervisor: **Prof E.C. Mwambene**

Co-Supervisor: **Dr W. Fish**

February 2013

Keywords and phrases

Automorphism

Cayley graphs

Codes

Cubes

Designs

Dual codes

Hamming graphs

Permutation decoding
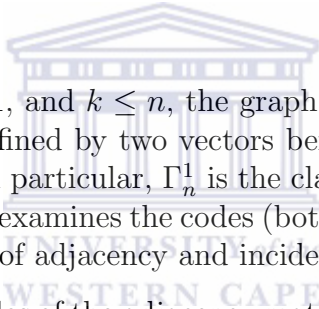
Ternary codes

Vertex-transitivity

Abstract

Codes Related to and Derived from Hamming Graphs

T.R Muthivhi

M.Sc thesis, Department of Mathematics, University of Western Cape

For integers $n, k \geq 1$, and $k \leq n$, the graph Γ_n^k has vertices the 2^n vectors of $\mathbb{F}_2^n$ and adjacency defined by two vectors being adjacent if they differ in k coordinate positions. In particular, Γ_n^1 is the classical n-cube, usually denoted by $H^1(n, 2)$. This study examines the codes (both binary and p-ary for p an odd prime) of the row span of adjacency and incidence matrices of these graphs.

We first examine codes of the adjacency matrices of the n-cube. These have been considered in [14]. We then consider codes generated by both incidence and adjacency matrices of the Hamming graphs $H^1(n, 3)$ [12]. We will also consider codes of the line graphs of the n-cube as in [13].

Further, the automorphism groups of the codes, designs and graphs will be examined, highlighting where there is an interplay. Where possible, suitable permutation decoding sets will be given.

February 2013

Declaration

declare that *Codes Related to and Derived from Hamming Graphs* is my work, that it has not been submitted before for any degree or examination in any other university, and that all the sources I have used or quoted have been indicated and acknowledged by complete references.

Thifhelimbilu Ronald Muthivhi   February 2013

Signed.....................................

List of symbols

Aut(C)   automorphism group of a linear code C

Aut($\mathcal{D}$)   automorphism group of a design $\mathcal{D}$

Aut(Γ)   automorphism group of a graph Γ

A_n adjacency matrix

$\mathcal{B}$ block set of a design

C linear code

$C^\perp$ dual code of C

$\dim(C)$ dimension of C

$\dim(C^\perp)$ dimension of $C^\perp$

$d(c, c')$ Hamming distance between c and c'

$d(u, v)$ minimum length of all paths between u and v

$d(x, y)$ Hamming distance between vectors x and y

$\mathcal{D}$ design

$E(\Gamma)$ Edge-set of a graph Γ

$\mathbb{F}_q$ finite field of order q where $q = p^t$, p a prime

$\mathbb{F}_q^n$ vector space of n-tuples over $\mathbb{F}_q$

G group

G_n incidence matrix

Γ graph

H parity-check matrix of C

$H^1(n, 2)$	the n-cube
$H^k(n, 2)$	the generalised cube
I	identity matrix
$L(H^1(n, 2))$	line graph of the n-cube
$L_n(2)$	incidence matrix of $L(H^1(n, 2))$
M	generator matrix
$\cong$	isomorphism of two structures
$\jmath$	all-one vector in a given code
$\jmath_n$	all-one vector of length n
$\mathcal{P}$	point set of a design
S_n	symmetric group on a set of n elements
$\mathrm{Stab}_G(v)$	stabiliser of a fixed vertex v in G
$S_2 \wr S_n$	wreath product of groups S_2 and S_n
$t - (v, k, \lambda)$	t-design for some non-negative integers t, v, k and λ
$V(\Gamma)$	vertex-set of a graph Γ
V_n	set of vectors of length n
$\mathrm{wt}(x)$	Hamming weight of a vector x
$(,)$	standard inner product
$\subseteq$	is a subset of
$\leq$	less than or equal to
$\in$	is an element of
$\cup$	the union of
$\cap$	the intersection of
Σ	the sum of
$[n, k, d]_q$	a q-ary code of length n, dimension k, and minimum weight d

v

Acknowledgements

I would like to thank my mother for giving me the gift of life in the first place and for providing me with support during the times when I needed it most. I am especially indebted to my elder brother Patrick who supported me financially from the first grade to tertiary level. I am fortunate to have such a giving and loving family, who made this achievement possible. They always believed in me and readily gave unconditional support for me to pursue my interests.

I also thank my supervisor Prof E.C. Mwambene for his ideas, guidance and patience throughout the past two years. Many thanks to my co-supervisor Dr W. Fish whose advice kept me on course.

Special thanks to Mukhethwa and Khumbo for their continuous encouragement throughout my research.

Contents

viii

List of Tables

UNIVERSITY *of the*

WESTERN CAPE

Chapter 1

Introduction

1.1 Introduction and historical background

Claude Shannon's 1948 paper "A Mathematical Theory of Communication" gave birth to the twin disciplines of information theory and coding theory. The basic goal of coding theory is efficient and reliable communication in an unstable environment. To be efficient, the transfer of information must not require a prohibitive amount of time and effort. To be reliable, the received data stream must resemble the transmitted stream to within narrow tolerances.

Coding theory is the branch of mathematics which studies methods of transmitting data as efficiently and accurately as possible across noisy channels. It solves the problem of how to make transmitted messages easy to decipher. This subject is totally different from cryptography, which is the branch of mathematics which makes messages hard to decipher.

Coding theory attempts to lessen these constraints by models which are constructed through mainly algebraic means. Shannon was primarily interested in an information theory. Shannon's colleague, Richard Hamming, had been labouring on error-correction for early computers even before Shannon's 1948 paper, and he made some of the first breakthroughs in coding theory. In the late 1940s, Claude Shannon was developing information theory and coding as a mathematical model for communication. At the same time, Richard Hamming found the need for error correction in his work on computers. Parity checking was already being used to detect errors in the calculations of the relay-based computers of the day, and Hamming realized that a more sophisticated pattern of parity checking allowed the correction of single errors along

with the detection of double errors. The codes that Hamming devised, the single-error-correcting binary Hamming codes and their single-error-correcting, double-error-detecting extended versions, marked the beginning of coding theory. These codes remain important to this day, for both theoretical and practical, as well as historical reasons.

Codes generated by incidence matrices of combinatorial designs have been studied rather extensively [1]; codes generated by the adjacency matrices of graphs have had less attention. In particular, for strongly regular graphs there is a strong relation with designs and therefore similar results may be expected. In this thesis we study binary codes from adjacency and incidence matrices of some classes of graphs, and apply the method of permutation decoding to these codes.

Permutation decoding was first developed by MacWilliams [24] and involves finding a set of automorphisms of a code called a PD-set. The method is described fully in MacWilliams and Sloane [25], Chapter 16, p.513 and Huffman [17], Section 8. It is most useful when the code has a fairly large group of automorphisms. Codes from strongly regular graphs (including triangular graphs), lattice graphs and graphs from triples, were shown to be good in [21], [22], [23].

Designs have their origin in statistics. They have been used to address the problem of designing certain types of experiments. There is an interesting chapter on designs and error-correcting codes in [2]. Designs have also been discussed in detail in [1] and [14]. The idea of a design can be illustrated in the following example which we have obtained from [14]. Suppose we wish to compare the effect of v varieties of fertilisers on different crops. We can do this by testing each crop with each variety of fertiliser applied to blocks of land (one for each crop) with each block having size v. This is not economical. We can use a design where each crop is tested with only k of the varieties so that each block now has k elements and any two varieties are used together on the same crop a constant number λ of times.

One of the first results in graph theory appeared in Leonhard Euler's paper on Seven Bridges, published in 1736. It is also regarded as one of the first topological results in geometry, that is, it does not depend on any measurements. In 1845 Gustav Kirchhoff published his circuit laws for calculating the voltage and current in electric circuits. In 1852 Francis Guthrie posed the four color problem which requires one to determine if it is possible to colour, using only four colours, any map of countries in such a way as to prevent two bordering countries from having the same colour. This problem was only solved a

2

century later in 1976 by Kenneth Appel and Wolfgang Haken. While trying to solve it, mathematicians invented many fundamental graph-theoretic terms and concepts. Graphs now have applications in various disciplines including computer science, engineering and the social sciences. In this thesis, we combine the theory from graphs and that from designs to generate codes which we examine extensively.

1.2 Overview of the thesis

In this section, we present an overall perspective of the thesis. We present the main contributions of each chapter of the thesis. In Chapter 2, we introduce preliminaries relating to codes, designs and graphs, necessary for the presentation of what follows in the latter chapters of the thesis. Chapter 3 describes the generalised cube $H^k(n, 2)$ and codes from the n-cube. We describe the iterative construction of the $H^k(n, 2)$ graph and we give $H^1(4, 2)$ as an example of such a graph. In Section 3.1 we describe the properties of $H^k(n, 2)$ and show that its automorphism group is given by $S_2 \wr S_n$. We also consider the distance transitivity of $H^1(n, 2)$. We also show that $H^k(n, 2)$ is isomorphic to $\mathrm{Cay}(\mathbb{F}_2^n, B_k)$, the Cayley graph defined on $\mathbb{F}_2^n$. Further, we discuss incidence and adjacency matrices of $H^1(n, 2)$ and the dimension and the minimum words of the codes generated by these matrices.

Chapter 4 describes the graph $H^1(n, 3)$ and designs $\mathcal{D}(n, 3)$ and $\mathcal{D}^*(n, 3)$. In this chapter we look at six issues; namely, the 2-rank of an adjacency matrix and the binary codes of $\mathcal{D}(n, 3)$ and $\mathcal{D}^*(n, 3)$, automorphism groups of $\mathcal{D}(n, 3)$ and $\mathcal{D}^*(n, 3)$, incidence matrices of $H^1(n, 3)$, and codes from an incidence matrix of $H^1(n, 3)$. Finally, we discuss permutation decoding for these codes.

Chapter 5 describes the binary codes from the line graph $L(H^1(n, 2))$ of the n-cube. We discuss the binary codes in Section 5.2. In Section 5.4, we describe codes from an incidence matrix of $L(H^1(n, 2))$. We describe the automorphism groups of $L(H^1(n, 2))$ and the hulls in Sections 5.5 and 5.6 respectively. Finally, we focus on permutation decoding for the codes.

Chapter 2

Preliminaries relating to codes, designs and graphs

In this chapter, we deal with introductory definitions and results relating to codes, designs and graphs which will be required in subsequent chapters. In addition, we introduce some general classical fundamental results that are useful for our discussion. As far as possible, we adhere to the commonly used notation and terminology. Most of the details can be found in [1]. General notation for graph theory is standard and can be found in [33].

2.1 Graphs

In this section we define graphs. For our purposes, the definition of a graph is made to reflect the pertinent characterisation of our discussion.

Definition 2.1.1. A **graph** $\Gamma = (V, E)$ consists of a **vertex-set V** and an **edge-set E**, where the edge, denoted by $[u, v]$, is an association of the vertices $u, v \in V$. If $[u, v] \in E$, then u and v are said to be **adjacent**, and are called the **endpoints** of $[u, v]$. The edge $[u, v]$ is said to be **incident** with u and v. A graph $\Gamma = (V, E)$ is **simple** if $[x, x] \notin E$ and E is a set. We adopt the usual notation $V(\Gamma)$ for the set of vertices of Γ and $E(\Gamma)$ for the set of edges.

A **path** between u and v is a sequence of distinct vertices $u_0 u_1 \cdots u_n$ where $u_0 = u, u_n = v$ and $[u_i, u_{i+1}]$ is an edge. The length of the path $u_0 u_1 \cdots u_n$ is n. A graph is **connected** if and only if any two vertices $u, v \in V$ are vertices of a path in Γ. Otherwise, Γ is **disconnected**. The **distance** between u and

v, denoted by $d(u, v)$, is the minimum length of all paths between u and v, if such paths exist. Otherwise, $d(u, v) = \infty$. The **diameter** of a graph is the maximum distance between any two vertices. Furthermore, the **degree** or the **valency** of a vertex v of Γ is the number of edges with which v is incident. If all the vertices of Γ are incident with the same number of edges, then Γ is said to be **regular**, and the common valency is the valency of the graph. We define the *i***th neighbourhood** of v as the set of all vertices that lie at a distance i from v.

The following proposition will be useful when determining the length of the code generated by incidence matrices.

Proposition 2.1.2. [32, Proposition 2.3.8.] *The sum of the degrees of all the vertices of a graph is equal to twice the number of edges of the graph.*

From the above proposition we deduce the following:

Corollary 2.1.3. [32, Corollary 2.3.10.] *A graph having n vertices and valency k has $\frac{nk}{2}$ edges.*

It is clear that the maximum valency that any graph having n vertices can have is $n - 1$, when every vertex is adjacent to every other vertex. Hence the maximum number of edges that such a graph can have is $\binom{n}{2}$. Such a graph is called a **complete** graph, and is denoted by K_n.

Definition 2.1.4. A graph Γ is **bipartite** if there are subsets A and B of the vertex set V such that

1. $A \cap B = \emptyset$;

2. $A \cup B = V$;

3. $A \neq \emptyset$ and $B \neq \emptyset$;

4. Every edge in Γ is incident with one vertex in A and one vertex in B.

A **line graph** of a graph $\Gamma = (V, E)$ is the graph $L(\Gamma)$ with vertex set E where $e, e' \in E$ are adjacent in $L(\Gamma)$ if and only if there exists $v \in V$ such that e and e' are commonly incident with v.

Let Γ and Γ' be two graphs. A map $f : V(\Gamma) \to V(\Gamma')$ is a **homomorphism** from Γ to Γ' if it preserves edges, that is, if $e = [x, y] \in E(\Gamma)$, then $[f(x), f(y)] \in E(\Gamma')$.

If a homomorphism is one to one, onto and its inverse preserves edges, it is called an isomorphism. Equivalently, we have the following.

Definition 2.1.5. Let Γ and $\Gamma^{'}$ be two graphs and consider a map $f : V(\Gamma) \longrightarrow V(\Gamma^{'})$. We say that f is an **isomorphism** if the following conditions are satisfied:
(i) f is a bijection;
(ii) f preserves edges, that is, if $[x, y] \in E(\Gamma)$, then $[f(x), f(y)] \in E(\Gamma^{'})$;
(iii) f^{-1} is a homomorphism.

If there is an isomorphism f from a graph Γ to another graph $\Gamma^{'}$, then Γ and $\Gamma^{'}$ are said to be isomorphic and we write $\Gamma \cong \Gamma^{'}$. The concept of an automorphism has been used extensively to distinguish and explore degrees of symmetry in graphs and is a key element in defining vertex-transitive graphs. An **automorphism** is an isomorphism from a graph Γ to itself. The set of automorphisms of Γ forms a group under composition, and is denoted by $\text{Aut}(\Gamma)$.

The important concept of vertex-transitivity is defined in terms of the automorphisms of a graph.

Definition 2.1.6. A graph Γ is said to be **vertex-transitive** if given any vertices u and v, there exists an automorphism $\alpha \in \text{Aut}(\Gamma)$ such that $\alpha(u) = v$.

A refinement of the concept of vertex-transitivity is that of distance-transitivity.

Definition 2.1.7. A graph $\Gamma = (V, E)$ is **distance-transitive** if, for vertices $u, v, w, x \in V(\Gamma)$ with $d(u, v) = d(w, x)$, there exists some $\alpha \in \text{Aut}(\Gamma)$ satisfying $\alpha(u) = w$ and $\alpha(v) = x$.

Let Γ be a graph and G a subgroup of $\text{Aut}(\Gamma)$. The stabiliser of a fixed vertex v in G is defined by $\text{Stab}_G(v) = \{\alpha \in G : \alpha(v) = v\}$.

Proposition 2.1.8. [3, Lemma 2.2.4] *Suppose Γ is connected and has* diam$(\Gamma) = d$ *and automorphism group Aut$(\Gamma) = G$. Then Γ is distance-transitive if and only if it is vertex-transitive and $\text{Stab}_G(v)$ is transitive on $\Gamma_i(v)$ for $i = 1, \cdots, d$ and for all $v \in V(\Gamma)$ where $\Gamma_i(v)$ is the subgraph of Γ with vertex-set $V(\Gamma_i(v)) = \{u \in V(\Gamma) : d(u, v) = i\}$.*

Proof. Suppose that Γ is distance-transitive. Then Γ is also vertex-transitive. Consider $u, u' \in \Gamma_i(v)$, *i.e.* $d(u, v) = d(u', v) = i$. Since Γ is distance-transitive,

there exists an automorphism $\alpha \in G$ such that $\alpha(v) = v$ and $\alpha(u) = u'$. Thus $\alpha \in \mathrm{Stab}_G(v)$, and $\mathrm{Stab}_G(v)$ is transitive on $\Gamma_i(v)$.

Conversely, suppose Γ is vertex-transitive and that $\mathrm{Stab}_G(v)$ is transitive on $\Gamma_i(v)$ for all $v \in V(\Gamma)$. Consider $u, w, u', w' \in V(\Gamma)$, such that $d(u, w) = d(u', w') = i$. Let $\alpha \in G$ be such that $\alpha(w) = w'$ and choose $\beta \in \mathrm{Stab}_G(w')$ so that $\beta(\alpha(u)) = u'$. Then for the composition $\beta o \alpha$, we get $(\beta\alpha)(u) = u'$ and $(\beta\alpha)(w) = \beta(w') = w'$. So $\beta\alpha$ is an automorphism of Γ mapping u, w to u', w'. Hence Γ is distance-transitive. $\qquad\square$

A crucial and extensively studied class of vertex-transitive graphs are the so-called Cayley graphs. We now give the definition of a Cayley set, which intrinsically defines a Cayley graph.

Definition 2.1.9. Let G be a group. A subset S of G is a **Cayley set** if it satisfies the following conditions:
(i) the identity element 1_G is not in S,
(ii) if $s \in S$ then so is s^{-1}.

Cayley graphs are a prototype of vertex-transitive graphs.

Definition 2.1.10. Let G be a group and S a Cayley set of G. The **Cayley graph** $\mathrm{Cay}(G, S)$ has the elements of G as vertices and $[x, y]$ is an edge, if there is $s \in S$ such that $y = x(s)$, for $x, y \in G$.

Throughout the thesis, we use graphs to generate codes. This is done through adjacency and incidence matrices which we now define.

Definition 2.1.11. An **adjacency matrix** $A = [a_{ij}]$ of Γ having vertex-set $V(\Gamma) = \{v_1, \cdots, v_n\}$, is an $n \times n$ matrix with $a_{ij} = 1$ if $[v_i, v_j] \in E(\Gamma)$, and $a_{ij} = 0$ otherwise.

Definition 2.1.12. An **incidence** matrix of Γ is an $n \times |E|$ matrix B with $b_{ij} = 1$ if v_i is incident on e_j, and $b_{ij} = 0$ otherwise.

An **adjacency** matrix is determined by a vertex ordering. Every adjacency matrix is symmetric ($a_{ij} = a_{ji}$ for all i, j). An adjacency matrix of a simple graph Γ has entries 0 or 1, with $0's$ on the diagonal. The degree of v is the sum of the entries in the row for v.

7

2.2 Designs

In this section, we summarize some of the basic concepts from the theory of designs. We first define a $t - (v, k, \lambda)$ design for some non-negative integers t, v, k and λ.

Definition 2.2.1. An incidence structure with point set $\mathcal{P}$ and block set $\mathcal{B}$, then $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is called a
$\boldsymbol{t - (v, k, \lambda)}$ design for some non-negative integers $\boldsymbol{t, v, k,}$ and $\boldsymbol{\lambda}$, if

1. $|\mathcal{P}| = \boldsymbol{v}$

2. every block $\boldsymbol{B}$ is incident with exactly $\boldsymbol{k}$ points; and

3. every $\boldsymbol{t}$ distinct points are together incident with exactly $\boldsymbol{\lambda}$ blocks.

   If $|\mathcal{B}| = |\mathcal{P}|$ then the design $\mathcal{D}$ is said to be symmetric.

   From a graph Γ we obtain an incidence design **neighbourhood**, if the adjacency matrix of Γ is interpreted as the incidence matrix of a design.

Definition 2.2.2. An **automorphism of a design** $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is a permutation σ of the points $\mathcal{P}$ which preserves the blocks $\mathcal{B}$.

   The automorphisms of $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ form a group under group composition, and induce a permutation on the block set $\mathcal{B}$. Linear codes will be constructed from the incidence matrices of the design, and their automorphism groups will be determined.

Lemma 2.2.3. [31, Lemma 2.1] *Let $\Gamma = (V, E)$ be a connected graph with incidence matrix B. Then*

1. $\mathrm{rank}_2(B) = |V| - 1$,

2. *if Γ is non-bipartite and p is any odd prime, then $\mathrm{rank}_p(B) = |V|$.*

Proof. 1. Let $r < |V|$. The sum of any r rows must contain at least one-zero entry, since otherwise there would be no edge connecting any of these r vertices, which would contradict the connectedness of Γ. Hence no r rows are linearly dependent if $r < |V|$. The sum of the $|V|$ rows is 0, so the rank is $|V| - 1$.

8

Conversely if $\text{rank}_2(B) = |V| - 1$, there are no $r < |V|$ rows which add up to the all-zero vector. So there are no r vertices which are not connected to the other $|V| - r$ vertices. Hence Γ is connected.

2. for p odd, let $w = \Sigma a_i r_i = 0$ be a sum of multiples of the rows r_i of Γ, where r_i corresponds to the vertex i. Taking a closed path $(i_1, i_2, \cdots, i_n)$ of odd length, $a_{i_0} = -a_{i_1} = \cdots = a_{i_n} = -a_{i_0}$ and thus $a_{i_0} = 0$.

Since the graph is connected, we get $a_i = 0$ for all i. $\qquad\square$

2.3 Codes

In this thesis we will be examining codes generated by the incidence and adjacency matrices of graphs.

Definition 2.3.1. Let F be a finite set, termed an **alphabet**, of q elements. A **q-ary** code C is a set of finite sequences of elements of F, called **codewords**. If all the sequences in C have the same length n, then C is called a **block code** of length n.

Let C be a q-ary code, and c and c' codewords in C. The **Hamming distance** between c and c', denoted by $d(c, c')$, is the number of coordinate positions in which they differ. The Hamming distance is usually referred to as the **distance** between two codewords. It defines a metric on the set of all sequences of length n over the alphabet F.

The **minimum distance** d of a code C is the minimum of the distance between any two distinct codewords in C, i.e.,

$$d(c) = \min\left\{ \mathrm{d}(\mathrm{c}, \mathrm{c}') : \mathrm{c}, \mathrm{c}' \in C, \mathrm{c} \neq \mathrm{c}' \right\}.$$

Only linear codes will be considered in this thesis.

Definition 2.3.2. A **linear code** of length n over the field $\mathbb{F}_q$ is a subspace of $\mathbb{F}_q^n$. If $\dim(C) = k$, and $d(c) = d$ then C is written $[n, k, d]_q$, or simply $[n, k, d]$ if $q = 2$. The information rate is $\frac{k}{n}$, and the redundancy is $n - k$.

Let C be an $[n, k, d]_q$ code. The **dual code** of C, denoted by $C^{\perp}$, is given by

$$C^{\perp} = \left\{ v \in \mathbb{F}_q^n : (v, c) = 0, \text{for all } \mathrm{c} \in \mathrm{C} \right\},$$

9

where $(,)$ denotes the standard inner product on $\mathbb{F}_q^n$. Furthermore, if $C \subseteq C^\perp$, then C is said to be **self-orthogonal**, and if $C = C^\perp$, then C is said to be **self-dual.**

Definition 2.3.3. Let C be an $[n, k, d]_q$ code. A **generator matrix** $\mathcal{G}$ for C is a $k \times n$ matrix obtained from any set of k linearly independent vectors in C.

Since the dual code $C^\perp$ is the null space of $\mathcal{G}$, the following result is deduced:

Proposition 2.3.4. [32, Proposition 2.1.13.] *Let C be an $[n, k, d]_q$ code. Then*

$$\dim(C) + \dim(C^\perp) = n.$$

Now if $\mathcal{G}$ is a generator matrix for C, then a generator matrix $\mathcal{H}$ for $C^\perp$ is an $(n - k) \times n$ matrix that satisfies $\mathcal{G}\mathcal{H}^T = 0$. The generator matrix for $C^\perp$ thus provides a mechanism of checking whether or not a codeword is in C.

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

Throughout the thesis, we consider codes generated by adjacency and incidence matrices of various classes of Hamming graphs. As mentioned in the introduction, codes constructed from designs have enriched the theory of designs in that new designs have been constructed, existing designs have been extended, and certain designs have been shown not to exist. Knowledge about the design from which a code was constructed could facilitate efficient encoding and decoding. On the other hand, not all codes yield designs, and the Assmus-Mattson Theorem (see [1], Theorem 2.11.2) gives criteria for determining whether the supports of the vectors of a certain weight yield a t-design. The step from a design to a code can be taken via the incidence matrix of the design.

Definition 2.3.5. Let $\mathcal{T} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be an incidence structure, F any field, and $F^\mathcal{P}$ the vector space of functions from $\mathcal{P}$ to F. For any $X \subseteq \mathcal{P}$, let v^X denote the characteristic function on X i.e. $v^X(p) = 1$ *if* $p \in X$, and $v^X(p) = 0$ *if* $p \notin X$. The standard basis for F^P is $\{v^p : p \in \mathcal{P}\}$. If no confusion arises, the accurate use of notation may be sacrificed for the sake of readability - the braces around the point p may be dropped as will be the case in this thesis, where the points are either k-subsets or m-tuples.

Definition 2.3.6. Let $\mathcal{T} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be an incidence structure, F any field, and $F^\mathcal{P}$ the vector space of functions from $\mathcal{P}$ to F. For a block $B \in \mathcal{B}$,

where $B \subseteq \mathcal{P}$, the **incidence vector** v^B is the vector associated with the characteristic function on B and will be written

$$v^B = \sum_{p:(p,B)\in\mathcal{I}} v^p.$$

Note that if the block B is not a subset of $\mathcal{P}$, then in order to define v^B, B first has to be identified with the set of points which are incident with it.

Definition 2.3.7. Let $\mathcal{T} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be an incidence structure. The **code** of $\mathcal{T}$ over a field F is the subspace of $F^{\mathcal{P}}$ generated by the incidence vectors associated with the blocks of $\mathcal{T}$, i.e.,

$$C_F(\mathcal{T}) = \text{span}\left\{v^B : B \in \mathcal{B}\right\}.$$

The above definition is not dependent on an ordering of the incidence vectors, since any ordering of the incidence vectors will generate codes that are isomorphic. If p is any prime and F is the field $\mathbb{F}_p$, then $C_F(\mathcal{T})$ can be written $C_p(\mathcal{T})$.

Definition 2.3.8. Let $\mathcal{T} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be an incidence structure, and $C_p(\mathcal{T})$ the code of $\mathcal{T}$ over $\mathbb{F}_p$. Then the **p-rank** of $\mathcal{T}$ is the dimension of $C_p(\mathcal{T})$ and is written

$$\text{rank}_p(\mathcal{T}) = \dim(C_p(\mathcal{T})).$$

With regard to automorphism groups, the automorphism group of an incidence structure will be contained in the automorphism group of the code generated by the incidence structure. Clearly, if the code generated is the full vector space or the dual of the code generated by the all-one vector $\jmath$, then the automorphism group of the code is the full symmetric group on the points $\mathcal{P}$. The converse is also true (see [20], Lemma 4).

As for codes generated by incidence matrices of connected graphs, we have the following result.

Lemma 2.3.9. [13, Lemma 7.] *Let Γ be a graph, G an incidence matrix for Γ, and (P,Q,R,S) a 4-cycle in Γ. For any prime p, if C is the code generated by G, then*

$$u = v^{[P,Q]} + v^{[R,S]} - v^{[P,S]} - v^{[Q,S]} \in C^{\perp}. \tag{2.1}$$

In particular, for p any prime, $m \geq 2$, then for $n \geq 2$, $C_p(G_n(m)^{\perp})$, the code of the incidence matrix of the Hamming graph $H(n,m)$, contains the weight-4 word

11

$$u(x, x + e, x + f) = v^{[x,x+e]} - v^{[x,x+f]} - v^{[x+e+f,x+e]} + v^{[x+e+f,x+f]}, \qquad (2.2)$$

where $x \in V_n$, $\mathrm{wt}(e) = \mathrm{wt}(f) = 1$, $e \neq f$. Further, $C_p(G_n(m))^\perp$ has minimum weight-4 for p odd, any m, and for $p = 2 = m$, $C_2(G_n(m)^\perp)$ has minimum weight-3 for $m \geq 3$.

We now give a formal definition of an automorphism and the automorphism group of a code mentioned previously.

Definition 2.3.10. Let C be an $[n, k, d]_q$ code. Then any isomorphism of C onto itself is called an **automorphism** of C. The set of all automorphisms of C form a group under composition, the automorphism group of C, denoted by $\mathrm{Aut}(C)$.

An automorphism of C is thus a permutation on the coordinate positions which maps codewords to codewords. Hence any automorphism of C preserves its weight classes, and this idea is useful in determining $\mathrm{Aut}(C)$ in the first place. With specific reference to the codes generated by an adjacency matrix of graphs as is the case in this thesis, the automorphism group of the graph is contained in the automorphism group of the code.

Even if the full automorphism group of the code has not been determined but the automorphism group of the graph is known, then permutations which map errors occurring at the information positions into the check positions may still be identified. The full automorphism group of the graph may not even need to be known. All that may be required are sets of automorphisms of the graph.

The concept of a permutation decoding set is defined next.

Definition 2.3.11. If C is a t-error-correcting code with information set $\mathcal{I}$ and check set $\mathcal{C}$, then a **PD**-set for C is a set S of automorphisms of C which is such that every t-set of coordinate positions is moved by at least one member of S into the check positions $\mathcal{C}$.

For $s \leq t$ an **s-PD**-set is a set S of automorphisms of C which is such that every s-set of coordinate positions is moved by at least one member of S into $\mathcal{C}$. Specifically, if $\mathcal{I} = \{1, \cdots, k\}$ are the information positions and $\mathcal{C} = \{k+1, \cdots, n\}$ the check positions, then every s-tuple from $\{1, \cdots, n\}$ can be moved by some element of S from $\mathcal{I}$ into $\mathcal{C}$.

The algorithm for permutation decoding is as follows: Suppose S is a PD-set for C, x is sent and y is received and at most t errors occur:

1. for $i = 1, \cdots, m$, compute $\sigma_i(y)$, where $\sigma_i \in S$, and the syndrome $s_i = H(\sigma_i(y))^T$ until an i is found such that the weight of s_i is t or less;

2. if $u = u_1 u_2 \cdots u_k$ are the information symbols of $\sigma_i(y)$, compute the codeword $c = uG$;

3. decode y as $\sigma_i^{-1}(c)$.

In the next chapter, we will discuss the generalised cubes $H^k(n, 2)$ and codes from $H^1(n, 2)$.

Chapter 3

The generalised cubes $H^k(n,2)$ and codes from $H^1(n,2)$

In this chapter we consider the generalised cubes $H^k(n,2)$ and codes from the row span of adjacency and incidence matrices of the n-cube $H^1(n,2)$. Some properties of the graphs including their automorphism group are presented in Section 3.1. We also show that the n-cube is distance-transitive and that it is a Cayley graph. In Section 3.2, we describe binary codes obtained from the row span of adjacency matrices of $H^1(n,2)$, giving their dimension and minimum words. We also describe codes of the row span of incidence matrices of $H^1(n,2)$. Finally, we discuss 3-PD-sets for these codes.

3.1 The generalised cubes $H^k(n,2)$

The n-cubes are a well-known and frequently studied class of graphs. They are in fact the Hamming graphs $H^1(n,2)$. Their vertices can be regarded as binary n-tuples, adjacent if their Hamming distance is 1. The more common alternative construction for $H^1(n,2)$ is given recursively as follows: starting with $H^1(1,2) \cong K_2$, take two copies of $H^1(n-1,2)$ which we will label $H^1(n-1,2)$ and $H^1(n-1,2)'$. Then for each vertex $v \in V(H^1(n-1,2))$, join it to the corresponding vertex $v' \in V(H^1(n-1,2)')$. Thus $H^1(2,2)$ is just the square, $H^1(3,2)$ is what would normally be referred to as the cube, and $H^1(4,2)$.

One easily sees that cubes can be extended in quite a natural way on the same set of vertices if one takes full advantage of the Hamming distance. The

generalised cubes $H^k(n, 2)$ are defined as follows.

Definition 3.1.1. The generalised cubes $H^k(n, 2)$ are graphs with vertex-set the set of all n-tuples over $\mathbb{F}_2$, and two n-tuples u and v are adjacent if and only if they differ in exactly k coordinate positions.

Let $v \in V(H^k(n, 2))$. It is clear that $\deg(v) = \binom{n}{k}$. By Corollary 2.1.3, $H^k(n, 2)$ has $2^{n-1}\binom{n}{k}$ edges.

For example, $H^1(4, 2)$ has 16 vertices. These are 0000, 1000, 0100, 1100, 0010, 1010, 0110, 1110, 0001, 1001, 0101, 1101, 0011, 1011, 0111, and 1111. It also has 32 edges.

We now consider the automorphism group of $H^k(n, 2)$. The lemma below was first presented in [3].

Lemma 3.1.2. [3, Lemma 5.2.1.] $S_2 \wr S_n \leq \operatorname{Aut}(H^k(n, 2))$.

Proof. Let $\sigma \in S_2^n$. Then $\sigma = (\sigma_1, \sigma_2, \cdots, \sigma_n)$ where $\sigma_i \in S_2$. For $x = (x_1, x_2, \cdots, x_n)$ and $y = (y_1, y_2, \cdots, y_n)$ such that $[x, y] \in E(H^k(n, 2))$, $\sigma[x, y] = [\sigma(x), \sigma(y)] \in E(H^k(n, 2))$ since if $x_i \neq y_i$ then $\sigma_i(x_i) \neq \sigma_i(y_i)$; the same holds for $x_i = y_i$.

Now, consider ρ a permutation on n symbols, permuting the n coordinates. So we have that $x_{\rho(i)} \neq y_{\rho(i)}$ whenever $x_i \neq y_i$. Similarly, it holds for $x_i = y_i$, so that ρ preserves adjacency. $\square$

$S_2 \wr S_n$ is in fact equal to $\operatorname{Aut}(H^k(n, 2))$. However, the permutation decoding which is discussed in Section 3 does not employ the entire group.

Proposition 3.1.3. [6] *The automorphism group of the Hamming graph $H^k(n, 2)$ is given by* $(S_2 \times S_2 \times S_2 \times \cdots \times S_2) \rtimes S_n$.

As for $H^k(n, 2)$ being Cayley, we have the following. Let B_k, $k \geq 1$, denote the set of vertices of $H^k(n, 2)$ of weight k. Since for each $x \in \mathbb{F}_2^n$, $x + x = 0$, it is clear that B_k is a Cayley set of the group $\mathbb{F}_2^n$. We show that $H^k(n, 2) \cong \operatorname{Cay}(\mathbb{F}_2^n, B_k)$.

Proposition 3.1.4. [6] $H^k(n, 2) \cong \operatorname{Cay}(\mathbb{F}_2^n, B_k)$.

Proof. Define a map $f : V(H^k(n, 2)) \longrightarrow \mathbb{F}_2^n$ by $f(u) = (u_1, u_2, \cdots, u_n)$. Clearly, f is a bijection. Let $[x, y] \in E(H^k(n, 2))$, so that $f(x) - f(y)$ has

weight k. Therefore we have that $b = f(x) - f(y) \in B_k$. $[f(x), f(y)]$ is an edge since $f(x) = f(y) + b$. Hence f is an isomorphism of graphs, and $H^k(n, 2) \cong \text{Cay}(\mathbb{F}_2^n, B_k)$. $\qquad \square$

Next, we consider the distance-transitivity of $H^k(n, 2)$.

Theorem 3.1.5. [3, Theorem 5.2.2.] *The generalised cubes $H^k(n, 2)$ are distance transitive.*

Proof. The symmetric group S_n, a subgroup of $\text{Aut}(H^k(n, 2))$ fixes $\overline{0} = 0000...0$, and acts transitively on $N_i(0)$, the ith neighbourhood of $\overline{0}$.

Also, since $H^k(n, 2)$ is Cayley, the set of left translations acts regularly on the vertices. Therefore $H^k(n, 2)$ is distance-transitive.

$\qquad \square$

3.2 Adjacency matrices and codes of $H^1(n, 2)$

In this section we describe the form of the adjacency matrices of $H^1(n, 2)$ and their codes. We present the parameters of the codes.

3.2.1 The form of adjacency matrices of $H^1(n, 2)$ and their rank

Let $\mathcal{D}_n$ denote the neighbourhood design for $H^1(n, 2)$. Note that $\mathcal{D}_n$ is a 1-design with point set $V_n = V(H^1(n, 2))$. It is a symmetric $1 - (2^n, n, n)$ design unless $n = 2k$, in which case there are repeated blocks. We will denote the block of the design $\mathcal{D}_n$ defined by a vertex $x_n \in V_n$ by $\overline{x}_n$. That is,

$$\overline{x}_n = \{y | y \in V_n, \text{wt}(x + y) = 1\}.$$

The adjacency matrix for $H^1(n, 2)$ is an incidence matrix of $\mathcal{D}_n$ (including repeated blocks in the $n = 2k$ case).

We will use the following notation: for $r \in \mathbb{Z}$ and $0 \leq r \leq 2^n - 1$, if $r = \sum_{i=1}^{n} r_i 2^{i-1}$ is the binary representation of r, then $r = (r_1, \cdots, r_n)$ is the corresponding vector in $\mathbb{F}_2^n$. We will also use $e_1, e_2, \cdots, e_n$ to denote the standard basis for V_n, so that $e_i = 2^{i-1}$, for $1 \leq i \leq n$. The complement of

16

$v \in V_n$ will be denoted by v_c. Thus $v_c(i) = 1 + v(i)$ for $1 \leq i \leq n$, where $v(i)$ denotes the ith coordinate entry of v. Similarly, for $\alpha \in \mathbb{F}_2$, $\alpha_c = \alpha + 1$. Clearly, $v_c = v + 2^n - 1$, i.e., $v_c = v + j_n$, where j_n is the all-one vector of V_n. Note that

$$\overline{(x_c)} = \{y | y \in V_n, \mathrm{wt}(x + y + j_n) = 1\} = \{y | y \in V_n, \mathrm{wt}(x + y) = n - 1\} = \overline{x}_{n-1},$$

the block of $x \in V_n$ which has supports consisting of those points which differ with it in $n - 1$ coordinate positions. Hence for the design $\mathcal{D}_n^1$ formed as such, we have $\mathcal{D}_n = \mathcal{D}_n^{n-1}$.

For example, $\mathcal{D}_4^1$ consists of the following blocks. These blocks are equal to the blocks of $\mathcal{D}_4^3$.

$$\overline{0000} = \{1000, 0100, 0010, 0001\}, \overline{1000} = \{1100, 1010, 1001, 0000\},$$
$$\overline{0100} = \{1100, 0110, 0101, 0000\}, \overline{1100} = \{1110, 1101, 1000, 0100\},$$
$$\overline{0010} = \{1010, 0110, 0011, 0000\}, \overline{1010} = \{1110, 1011, 0010, 1000\},$$
$$\overline{0110} = \{1110, 0111, 0100, 0010\}, \overline{1110} = \{1111, 0110, 1010, 1100\},$$
$$\overline{0001} = \{1001, 0101, 0011, 0000\}, \overline{1001} = \{1101, 1011, 0001, 1000\},$$
$$\overline{0101} = \{1101, 0111, 0001, 0100\}, \overline{1101} = \{1111, 0101, 1001, 1100\},$$
$$\overline{0011} = \{1011, 0111, 0001, 0010\}, \overline{1011} = \{1111, 0011, 1001, 1010\},$$
$$\overline{0111} = \{1111, 0011, 0101, 0110\}, \overline{1111} = \{0111, 1011, 1101, 1110\}.$$

For the adjacency matrices of the graphs, we will order the vertices, according to the ordering of the numbers from 0 to $2^n - 1$, in increasing order. With this ordering we denote the adjacency matrix of $H^1(n, 2)$ by A_n. Using block matrices, we have

$$A_n = \begin{pmatrix} A_{n-1} & I \\ I & A_{n-1} \end{pmatrix}, \tag{3.1}$$

where I is the identity matrix of order $n - 1$ in Equation (3.1). This is consistent with the recursive definition of $H^1(n, 2)$ discussed at the beginning of Section 3.1.

Lemma 3.2.1. [10, Lemma 2] (1) $A_n^2 = nI$ for $n \geq 2$. (2) A_n is invertible if $n \geq 3$ is odd.

17

Proof. We prove the above lemma by induction on n. Now $A_2 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$.

Therefore $A_2^2 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix} = 2\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} =$

$2I$.

For A_3, we have $A_3 = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$. Therefore $A_3^2 =$

$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 0 & 2 & 2 & 2 & 0 & 2 & 0 \\ 0 & 3 & 0 & 2 & 0 & 2 & 0 & 2 \\ 2 & 0 & 3 & 0 & 2 & 0 & 2 & 0 \\ 0 & 2 & 0 & 3 & 0 & 2 & 0 & 2 \\ 2 & 0 & 2 & 0 & 3 & 0 & 2 & 0 \\ 0 & 2 & 0 & 2 & 0 & 3 & 0 & 2 \\ 2 & 0 & 2 & 0 & 2 & 0 & 3 & 0 \\ 0 & 2 & 0 & 2 & 0 & 2 & 0 & 3 \end{pmatrix} =$

$\begin{pmatrix} 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix} = 3 \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = 3I = I.$

Hence the induction hypothesis is true for $n = 2, 3$.

Suppose the hypothesis holds for $k < n$.

$$A_n = \begin{pmatrix} A_{n-1} & I \\ I & A_{n-1} \end{pmatrix} = \begin{pmatrix} A_{n-2} & I & I & 0 \\ I & A_{n-2} & 0 & I \\ I & 0 & A_{n-2} & I \\ 0 & I & I & A_{n-2} \end{pmatrix}.$$

So, $A_n^2 = \begin{pmatrix} A_{n-2} & I & I & 0 \\ I & A_{n-2} & 0 & I \\ I & 0 & A_{n-2} & I \\ 0 & I & I & A_{n-2} \end{pmatrix} \begin{pmatrix} A_{n-2} & I & I & 0 \\ I & A_{n-2} & 0 & I \\ I & 0 & A_{n-2} & I \\ 0 & I & I & A_{n-2} \end{pmatrix}$

$$= \begin{pmatrix} (n-2)I+I+I & A+A & A+A & I+I \\ A+A & (n-2)I+I+I & I+I & A+A \\ A+A & I+I & (n-2)I+I+I & A+A \\ I+I & A+A & A+A & (n-2)I+I+I \end{pmatrix}$$

$$= \begin{pmatrix} nI & 2A & 2A & 2I \\ 2A & nI & 2I & 2A \\ 2A & 2I & nI & 2A \\ 2I & 2A & 2A & nI \end{pmatrix} = \begin{pmatrix} nI & 0 & 0 & 0 \\ 0 & nI & 0 & 0 \\ 0 & 0 & nI & 0 \\ 0 & 0 & 0 & nI \end{pmatrix} = nI.$$

Note that if n is odd, then $A_n^2 = I$. □

Lemma 3.2.2. [10, Proposition 2] *For $n \geq 2$,*

(1) $\operatorname{rank}_2(A_n) = 2^{n-1}$ *for $n \equiv 0$ (mod 2),*

(2) $\operatorname{rank}_2(A_n) = 2^n$ *for $n \equiv 1$ (mod 2).*

Proof. Recall that for $n = 2$, we have $A_2 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$

Now $r_1 = r_4$, $r_2 = r_3$, where $r_1, \cdots, r_4$ are the rows of A_2 above, and we can easily see that r_1 and r_2 are linearly independent. Therefore the rank of A_2 is 2, and the induction hypothesis is true for $n = 2$.

Suppose the hypothesis holds for $k < n$. Consider $A_n = \begin{pmatrix} A_{n-1} & I \\ I & A_{n-1} \end{pmatrix}$.

Case 1. $n \equiv 0$ (mod 2).

19

By the induction hypothesis A_{n-1} has full rank. Hence $A_n = \begin{pmatrix} A_{n-1} & I \\ A_{n-1} & I \end{pmatrix} = \begin{pmatrix} A_{n-1} & I \\ 0 & 0 \end{pmatrix}$. Therefore the rank of A_n is 2^{n-1}.

Case 2. $n \equiv 1 \pmod 2$. Since A_n is invertible when n is odd, the result follows by Lemma 3.2.1. $\qquad\square$

3.2.2 Minimum words of the code

We now describe the code $C_2(\mathcal{D}_n)$.

Proposition 3.2.3. *For $n \geq 2$ even, let $\mathcal{D}_n$ be the $1-(2^n, n, n)$ neighbourhood design of the Hamming graph $H^1(n, 2)$. Then $C_2(\mathcal{D}_n)$ is a $[2^n, 2^{n-1}, n]_2$ self-dual code. For $n \geq 6$, the minimum words are incidence vectors of the blocks of the design.*

Proof. Write $C = C_2(\mathcal{D}_2)$. Let A_n be an adjacency matrix for $H^1(n, 2)$. By Lemma 3.2.1, we have that if n is even, then $A_n^2 = nI_{2^n} = 0$, and hence the code C is self orthogonal.

To prove that the minimum weight is n and that the minimum words are the incidence vectors of the blocks, we use induction on n, observing that the hypothesis is true for $n = 6$, as was confirmed by Magma computations done in [11, 12]. Suppose that it is true for $k \geq 6$ and $k \leq n - 2$, ($6 \leq k \leq n - 2$) with k even. Then

$$A_n \sim \begin{pmatrix} A_{n-1} & I \\ 0 & 0 \end{pmatrix} \sim \left(\begin{array}{cc|cc} A_{n-2} & I & I & 0 \\ I & A_{n-2} & 0 & I \\ \hline 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right) = M.$$

A word in C consists of the concatenation of four words w_i, $1 \leq i \leq 4$, from each of the four column blocks C_i, $1 \leq i \leq 4$. Let R_1 and R_2 denote the first two row blocks of M. We will consider e_i, the ith row of the $2^{n-2} \times 2^{n-2}$ submatrix I, and b_i, the ith row of the submatrix $A_{n-2} = A$. Each b_i has weight $n-2$ by the induction hypothesis. A word w in C from the sum of $r \geq 1$ rows from the first set R_1 of 2^{n-2} rows will have $w_1 = \sum_{i \in K} b_i$ where $|K| = r$, $w_2 = w_3 = \sum_{i \in K} e_i$ and $w_4 = 0$. So if we take $w_1 \neq 0$ then the weight $\mathrm{wt}(w) \geq (n-2) + 2r \geq n$, by the induction hypothesis, with equality only if $r = 1$. If $w_1 = 0$ then $\sum_{i \in K} b_i = 0$ and it follows that $\sum_{i \in K} e_i \in C(A)^{\perp} = C(A)$, the binary code

20

from the matrix A. By the induction hypothesis we have that $r \geq n - 2$, and so $\text{wt}(w) = 2r \geq 2n - 4 > n$ for $n > 4$. Similarly for the second set R_2 of 2^{n-2} rows.

Suppose that we have a word that is the sum of r rows from the first set, and t rows from the second, where both $r, t \geq 1$. Then $w_1 = \sum_{j \in J} e_j + \sum_{i \in K} b_i$, $w_2 = \sum_{i \in K} e_i + \sum_{j \in J} b_j$, $w_3 = \sum_{i \in K} e_i$, $w_4 = \sum_{j \in J} e_j$, where $|K| = r$, $|J| = t$. Then $\text{wt}(w) = r + t + \text{wt}(w_1) + \text{wt}(w_2) > n$ if $r + t > n$. Now suppose that $r + t \leq n$, and both $r, t \leq n - 1$. Without loss of generality, suppose that $r \leq n/2$. Then $r < n - 2$, so that $\text{wt}(\sum_{i \in K} b_i) \geq n - 2$ with equality only if $r = 1$. Thus we obtain that $\text{wt}(w_1) \geq n - 2 - t$ if $t \leq n - 2$, and $\text{wt}(w_1) \geq 1$ if $t = n - 1$. Now if $t = n - 1$, $r = 1$, then $\text{wt}(w) \geq 1 + \text{wt}(w_2) + 1 + n - 1 > n$. If $t \leq n - 2$, then $\text{wt}(w) \geq n - 2 - t + \text{wt}(w_2) + r + t = n - 2 + r + \text{wt}(w_2)$. If $r \geq 2$ then $\text{wt}(w_2) > n - 2 - t$ and so $\text{wt}(w) > n$. Thus pick $r = 1$, $t \leq n - 2$, and so $\text{wt}(w) \geq n - 1 + \text{wt}(w_2)$. Then $w_2 = e_k + \sum_{j \in J} b_j$, so $\text{wt}(w_2) = 1$ if $\sum_{j \in J} b_j = 0$ and $\text{wt}(w_2) \geq n - 3$. So $\text{wt}(w) \geq (n - 1) + (n - 3) > n$ for $n > 4$. Now suppose that $\sum_{j \in J} b_j = 0$, from which it follows that $t \geq n - 2$ by using the induction hypothesis, and hence $t = n - 2$. Then $\text{wt}(w) = \text{wt}(w_1) + 1 + 1 + n - 2 > n$ unless $w_1 = 0$. Suppose we pick the first row of R_1 corresponding to the block $\bar{0}$. Then, since $w_1 = 0$, the $n - 2$ rows of R_2 that we have considered are those indexed by $\{e_i + e_{n-1} | 1 \leq i \leq n - 2\}$. Therefore $\text{Supp}(w_4) = \{e_i + e_{n-1} + e_n | 1 \leq i \leq n - 2\}$ and $\text{Supp}(w) = \{e_i + e_{n-1} + e_n | 1 \leq i \leq n\} = \overline{e_{n-1} + e_n}$. Thus for $n \geq 6$ we have our result, noting that the minimum weight is indeed $4 = n$, but there are more weight-4 vectors besides those from the blocks. $\qquad \square$

Proposition 3.2.4. *For $n \geq 6$, n even, $\text{Aut}(C_2(\mathcal{D}_n)) = \text{Aut}(\mathcal{D}_n)$.*

Proof. An automorphism of the code C preserves the words of weight n. Hence the blocks of the design are preserved. $\qquad \square$

Proposition 3.2.5. *For n even, any $x \in V_n = \mathbb{F}_2^n$, $\sum_{i=1}^{n} v^{\overline{x+e_i}} = 0$, and no sum of fewer than n of these words is zero.*

Proof. We have to show that

$$\sum_{i=1}^{n} v^{\overline{x+e_i}} = 0. \tag{3.2}$$

Since

$$v^{\overline{x+e_i}} = \sum_{j=1}^{n} v^{x+e_i+e_j}, \tag{3.3}$$

21

substituting Equation (3.3) into Equation (3.2) we get that

$$\sum_{i=1}^{n} v^{\overline{x+e_i}} = \sum_{i=1}^{n}\sum_{j=1}^{n} v^{x+e_i+e_j} = nv^x + 2\sum_{i\neq j} v^{e_i+e_j} = 0.$$

Moreover, we have that no sum of fewer than n incidence vectors of blocks is zero since C is a binary code obtained from the row span of an adjacency matrix for $H^1(n,2)$ over $\mathbb{F}_2$ and is also self-orthogonal. Hence $C = C_2(H^1(n,2)) = C^{\perp}$ is even. $\qquad\square$

3.3 Incidence matrices for $H^k(n,2)$

In this section we describe the incidence matrix for $H^k(n,2)$ and give an example of such a matrix.

Let $G_n(2)$ denote an incidence matrix for $H^k(n,2)$. The $2^n \times 2^{n-1}n$ incidence matrix $G_n(2)$ can be written in the following way: take the natural ordering of the rows corresponding to the binary representation of the natural numbers from 0 to $2^n - 1$, and divide the rows into two row blocks R_i, $i = 0, 1$, where the rows of R_i are labelled by the vectors $x = (x_1, \cdots, x_n)$. The columns are ordered so that we first take all the edges between vertices in the rows of R_0, then those between the vertices in the rows of R_1, and finally, those between vertices in R_0 and R_1. Thus $G_n(2)$ will have the following form:

$$G_n(2) = \begin{pmatrix} G_{n-1}(2) & 0 & I \\ 0 & G_{n-1}(2) & I \end{pmatrix},$$

were $I = I_{2^{n-1}}$ in $G_n(2)$.

Proposition 3.3.1. [15] *Let G_n be a $2^n \times 2^{n-1}n$ incidence matrix for $H^1(n,2)$. Then the rank of G_n is $2^n - 1$.*

Proof. Applying Lemma 2.2.3 to the graph $H^1(n,2)$, we obtain the result. $\quad\square$

The proof of the following lemma is based on these facts:

1. In $H^1(3,2)$ we have six 4-cycles; namely $(110, 111, 011, 010)$; $(110, 010, 000, 100)$; $(110, 111, 101, 100)$; $(000, 001, 101, 100)$; $(001, 101, 111, 011)$; $(000, 001, 011, 010)$.

2. For any block $\bar{x}$, $(v^{\bar{x}}, v^{x,x+e} + v^{x,x+f} + v^{x+f,x+f+e} + v^{x+e,x+e+f}) = 2 \equiv 0$ (mod 2). Therefore the blocks containing the edges of a 4-cycle are in $C^{\perp}$.

3. Each edge of $H^1(3,2)$ is in exactly two 4-cycles.

Let $\mathcal{B}_n$ be the block-set of an incidence design of $H^1(n,2)$.

Lemma 3.3.2. [15] *Let G_n be an incidence matrix of $H^1(n,2)$. Then the minimum words of the code are the scalar multiples of the rows in G_n.*

Proof. Let $w \in C$ and $\mathrm{Supp}(w) = \mathcal{S}$, where $|\mathcal{S}| = s$. Let $P = [0, e_1] \in \mathcal{S}$. Suppose that in $\mathcal{S}$ there are k points of the type that are on a block with P, and l that are not. Then $s = k+l+1$. Counting blocks of $\mathcal{B}_n$ through the point P, suppose that there are z_i that meet $\mathcal{S}$ in i points. Then $z_0 = z_1 = z_i = 0$ for $i \geq 5$, since w cannot meet a block of $\mathcal{B}_n$ only once, nor can it meet it more than four times. Thus $n - 1 = z_2 + z_3 + z_4$ and $z_2 + 2z_3 + 3z_4 = k = s - 1 - l$. Thus $n - 1 \leq s - 1$, and therefore $s \geq n$. Since there are vectors of weight n, this is the minimum weight. Suppose $s = n$. Thus the inequalities above are equalities and so $z_3 = z_4 = 0$, and $l = 0$. Thus $\mathcal{S}$ consists of $[0, e_1]$ and points of the form $[0, e_j], [e_1, e_1 + e_j], [e_j, e_1 + e_j]$, and each block of $\mathcal{B}_n$ meets $\mathcal{S}$ exactly twice, since this argument applies to any point of $\mathcal{S}$. Furthermore, since $l = 0$ for each point of $\mathcal{S}$, any two points of $\mathcal{S}$ are on a block. $\square$

Proposition 3.3.3. [15] *For $n \geq 3$,* $\mathrm{Aut}(C_p(G_n(2))) = S_2 \wr S_n = T_n \ltimes S_n$, *where T_n is the translation group on $\mathbb{F}_2^n$.*

Proof. For $n \geq 3$ the words of weight n are the scalar multiples of the rows of G_n, i.e., of the incidence vectors of the blocks of $\mathcal{D}_n$, and since any automorphism of the code must preserve weight classes, we see that the blocks of the design are preserved, and therefore we have an automorphism of the design. $\square$

3.3.1 Permutation decoding of codes from $H^1(n,2)$

In this subsection we will discuss permutation decoding. Permutation decoding can be used when a code has a sufficiently large automorphism group to ensure the existence of a set of automorphisms that satisfies certain conditions. Below we exhibit a 3-PD set for the code from an adjacency matrix for $H^1(n,2)$ for n even, $n \geq 8$.

Proposition 3.3.4. [20, Proposition 3] *For n even, $n \geq 4$, the code C_n from an adjacency matrix of $H^1(n, 2)$ is a $[2^n, 2^{n-1}, n]_2$ self-dual code with $\mathcal{I} = \{0, 1, \cdots, 2^{n-1} - 3, 2^n - 2, 2^n - 1\}$ as an information set.*

If $\mathcal{I}$ is as in the above proposition, the corresponding check set is $\mathcal{C}$. We will write
$\mathcal{I}_1 = \{0, 1, \cdots, 2^{n-1} - 3\}$
$\mathcal{C}_1 = \{2^{n-1}, 2^{n-1} + 1, \cdots, 2^n - 3\}$
$\mathcal{I}_2 = \{2^n - 2, 2^n - 1\}$
$\mathcal{C}_2 = \{2^{n-1} - 2, 2^{n-1} - 1\}$

and $a = 2^n - 2 = (0, 1, \cdots, 1, 1)$, $b = 2^n - 1 = (1, 1, \cdots, 1, 1)$,
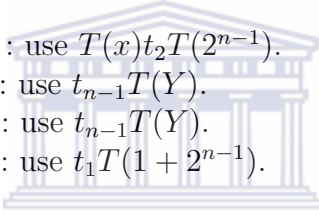$A = 2^{n-1} - 2 = (0, 1, \cdots, 1, 0), B = 2^{n-1} - 1 = (1, 1, \cdots, 1, 0)$.

Notice that the points a and b are placed in $\mathcal{I}$ in order to have points and their complements in $\mathcal{I}$.

Theorem 3.3.5. [20, Theorem 4] *For n even, $n \geq 8$, let $T_n = \{T(w)t_i | w \in \mathbb{F}_2^n, 1 \leq i \leq n\}$, where $T(w)$ is the translation by $w \in \mathbb{F}_2^n$, $t_i = (i, n)$ for $i < n$ is a transposition in the symmetric group S_n, and t_n is the identity map. Then T_n is a 3-PD-set of size $n2^n$ for the self-dual $[2^n, 2^{n-1}, n]_2$ code C_n from an adjacency matrix for the n-cube $H^1(n, 2)$, with information set $\mathcal{I} = \{0, 1, \cdots, 2^{n-1} - 3, 2^n - 2, 2^n - 1\}$.*

Proof. Let $\mathcal{T} = \{a, b, c\}$ be a set of three points in $\mathcal{P}$. We have to show that that there is an element in T_n that maps $\mathcal{T}$ into the check set $\mathcal{C}$. We consider the several possibilities for the points in $\mathcal{T}$.
If $\mathcal{T} \subseteq \mathcal{C}$, then identity map t_n suffices. Now suppose at least one of the points is in $\mathcal{I}$ and, by using a translation, we suppose that one of the points, say c, is 0. If $\mathcal{T} \subseteq \mathcal{I}$, then $T(2^{n-1})$ will work. Now we consider the other cases.

1. $a \in \mathcal{I}_1$, $b \in \mathcal{C}_1$. Then there are i_a, i_b such that $2 \leq i_a$, $i_b \leq n-1$ such that $a(i_a) = b(i_b) = 0$. If $i_a = i_b = i$, then $\mathcal{T} t_i \subseteq \mathcal{I}$, unless $bt_i \in \{X, Y\}$, so $t_i T(2^{n-1})$ will work unless $bt_i \in \{X, Y\}$. If $bt_i = X$, then $b(1) = b(i) = 0$, $b(j) = 1$ otherwise. If $a(1) = 0$, then $t_1 T(2^{n-1})$ will work. If $a(1) = 1$, then take any $j \neq 1$, i, n, and use $T(2^{j-1})t_i T(2^{n-1})$. If $bt_i = Y$, then $b(i) = 0$ and $b(j) = 1$ otherwise. Here we can take any $j \neq 1$, i, n, and use $T(2^{j-1})t_i T(2^{n-1})$. If a and b have no common zero, then if $b = x_c$, so that $a + b = y$, we can use $T(a)T(2^{n-1})$. If $a(i) = b(i) = 1$, where $1 \leq i \leq n - 1$, then $t_i T(2^{n-1} - 1)$ can be used.

24

2. $a \in \mathcal{I}_1$, $b \in \mathcal{C}_2$. Since $a \in \mathcal{I}_1$, $a(i) = 0$ for some i such that $2 \le i \le n - 1$. If there is a j such that $j \ne i$ and $2 \le j \le n - 1$ with $a(j) = 0$, then $T(2^{i-1} + 2^{n-1})$ can be used. If there is no such j, then either $a(1) = a(i) = a(n) = 0$ and $a(j) = 1$ for $j \notin \{1, i, n\}$, or $a(i) = a(n) = 0$ and $a(j) = 1$ for $j \notin \{i, n\}$. In either case, take $j \ne i$, $2 \le j \le n - 1$. Then the map $T(2^{j-1} + 2^{n-1})$ can be used.

3. $a \in \mathcal{I}_2$, $b \in \mathcal{C}_1$.
   Let us consider when $a = x$: since $b \in \mathcal{C}_1$, there is a j such that $2 \le j \le n - 1$ with $b(j) = 0$. If $b(i) = 1$ for $i \ne j$ and $1 \le i \le n$, or if $b(1) = 0$ and $b(i) = 1$ for $i \ne j$ and $2 \le i \le n$, then $T(X)$ will work. If there is an $i \ne j$ such that $b(i) = b(j) = 0$ where $2 \le i, j \le n - 1$, then $t_j T(2^{n-1})$ can be used.
   If $a = y$: this follows exactly as in the $a = x$ case except that in the first two cases for b use $T(Y)$ instead of $T(X)$.

4. $a \in \mathcal{I}_2$, $b \in \mathcal{C}_2$
   (a): $a = x$, $b = X$: use $T(x)t_2 T(2^{n-1})$.
   (b): $a = x$, $b = Y$: use $t_{n-1} T(Y)$.
   (c): $a = y$, $b = X$: use $t_{n-1} T(Y)$.
   (d): $a = y$, $b = Y$: use $t_1 T(1 + 2^{n-1})$.

5. $a, b \in \mathcal{C}$ $a, b \in \mathcal{C}_1$: if $a + b = Y$ then $T(Y)$ will work. Otherwise $a(i) = b(i)$ for some i such that $1 \le i \le n - 1$. Again $T(Y)$ will work unless a or b are $(0, \cdots, 0, 1)$ or $(1, 0, \cdots, 0, 1)$. If $a = (0, \cdots, 0, 1)$ then $b(i) = 0$ for some i such that $2 \le i \le n - 1$. Then $t_i T(2^{n-1})$ can be used unless $b(j) = 1$ for all $j \ne i$, or $b(1) = b(i) = 0$ and $b(j) = 1$ for $j \ne 1$, i; in these cases $t_i T(2^{i-1} + 2^{n-1})$ can be used. The same arguments hold if $a = (1, 0, \cdots, 0, 1)$.
   $a \in \mathcal{C}_1$, $b \in \mathcal{C}_2$: since $a \in \mathcal{C}_1$, there is a j such that $2 \le j \le n - 1$ with $a(j) = 0$. Then $t_j T(2^{j-1} + 2^{n-1})$ can be used.
   $a, b \in \mathcal{C}_2$: $T(2^{n-2} + 2^{n-1})$ will work.

This completes all the cases and proves the theorem. $\square$

Note that this result also shows that the set T_n is a 2-PD-set for C_n for $n = 6$. However, this set T_n with this information set $\mathcal{I}$ will not give a 4-PD-set. In the next chapter we consider the Hamming graphs $H^1(n, 3)$

Chapter 4

The Hamming graphs $H^1(n, 3)$ and their reflexive counterparts

In this chapter we describe the binary codes from the row span of adjacency and incidence matrices for the graphs $H^1(n, 3)$ and the associated neighbourhood designs. We also consider the graph $H^*(n, 3)$, the reflexive hypercube of $H^1(n, 3)$ and its corresponding codes.

Recall the definition of $H^1(n, 2)$ in Section 3.1. It is easy to see that the graph can be generalised to $H^1(n, m)$ by $V(H^1(n, m)) = \mathbb{F}_n^m$; $[x, y] \in E(H^1(n, m))$ if and only if $\text{wt}(x - y) = 1$. In particular, and we consider the graph $H^1(n, 3)$ defined by $V(H^1(n, 3)) = \mathbb{F}_n^3$ and $E(H^1(n, 3)) = \{[x, y] : x, y \in V(H^1(n, 3)), wt(x - y) = 1\}$. Its reflexive counterpart $H^*(n, 3)$ has the same vertices and edges as $H^1(n, 3)$ together with additional edges of the form $[x, x]$ for all $x \in V(H^1(n, 3))$, i.e.

$$V(H^*(n, 3)) = V(H^1(n, 3)); E(H^*(n, 3)) = E(H^1(n, 3)) \cup \{[x, x] | x \in V(H^1(n, 3))\}.$$

The following three properties of the Hamming graphs $H^1(n, 3)$ are immediately apparent: The number of vertices is 3^n, the valency of $H^1(n, 3)$ is $2n$ and the number of edges is $3^n n$. So for $H^1(2, 3)$ below, the valency is $2(2) = 4$. The graph has 9 vertices. These are $(0; 0), (0; 1), (0; 2), (1; 0), (1; 1), (1; 2),$ $(2; 0), (2; 1), (2, 2)$. It has 18 edges.

4.1 The graphs $H^1(n,3)$ and designs $\mathcal{D}(n,3)$ and $\mathcal{D}^*(n,3)$

Let $\mathcal{D}(n,3)$ denote the neighbourhood design of the graph $H^1(n,3)$. It is a symmetric $1-(3^n, 2n, 2n)$ design with incidence matrix and adjacency matrix for $H^1(n,3)$. If $x \in \mathbb{F}_3^n$ and we label the block it is defined by $\overline{x}$, where

$$\overline{x} = \{y | y \in \mathbb{F}_3^n, wt(x-y) = 1\}. \tag{4.1}$$

Now let $\mathcal{D}^*(n,3)$ denote the $1-(3^n, 2n+1, 2n+1)$ design defined by adjoining x to $\overline{x}$, for each $x \in \mathbb{F}_3^n$, we label the block defined by $x \in \mathbb{F}_3^n$ by $\overline{\overline{x}}$, where

$$\overline{\overline{x}} = \{y | y \in \mathbb{F}_3^n, wt(x-y) \leq 1\}. \tag{4.2}$$

$\mathcal{D}^*(n,3)$ is the neighbourhood design of $H^*(n,3)$. Then we order the n-tuples according to the ordering in $\mathbb{F}_3$, by the rule that $x < y$ if the rightmost non-zero element of x is less than that of y.

Let A_n denote the adjacency matrix of $H^1(n,3)$, using this ordering of the vertices, where $n \geq 1$. Specifically, for $r \in \mathbb{Z}$ and $0 \leq r \leq 3^n - 1$, if $r = \Sigma_{i=1}^n r_i 3^{i-1}$, $0 \leq r_i \leq 2$, is the ternary representation of r, let $r = (r_1, \cdots, r_n)$ be the corresponding vector in $\mathbb{F}_3^n$. We will also use $e_1, e_2, \cdots, e_n$ to denote the standard basis for $\mathbb{F}_3^n$. Then, for $n \geq 2$, over $\mathbb{F}_3$, writing $A = A_{n-1}$, we have

$$A_n = \begin{pmatrix} A & I & I \\ I & A & I \\ I & I & A \end{pmatrix}, \tag{4.3}$$

where I is the $3^{n-1} \times 3^{n-1}$ identity matrix. We write $A_n^* = A_n + I_{3^n}$. As mentioned previously, it is an incidence matrix for $\mathcal{D}^*(n,3)$, and an adjacency matrix for the graph from $H^1(n,3)$ that includes every loops.

4.2 The 2-rank of the adjacency matrix of $H^1(n,3)$

We now discuss the 2-rank of an adjacency matrix A_n of $H^1(n,3)$. The rank is intimately linked to the following lemma.

Lemma 4.2.1. [12, Lemma 1] *Over* $\mathbb{F}_2$, *for* $n \geq 1$, $A_n^2 = A_n$ *and* $(A_n + I)^2 = A_n + I$.

Proof. We prove the lemma by induction. Note that

$$A_1 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Therefore

$$A_1^2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

We also have $A_1 + I = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$. $(A_1 + I)^2 = A_1 + I$ follows immediately.

Suppose the hypothesis holds for $k < n$.

$$A_n = \begin{pmatrix} A & I & I \\ I & A & I \\ I & I & A \end{pmatrix}. \text{ So } A_n^2 = \begin{pmatrix} A & I & I \\ I & A & I \\ I & I & A \end{pmatrix}^2 = \begin{pmatrix} A & I & I \\ I & A & I \\ I & I & A \end{pmatrix}.$$

Therefore $A_n^2 = A_n$ and $(A_n + I)^2 = A_n + I$.

$\square$

Proposition 4.2.2. [12, Proposition 1] *Let* A_n *be adjacency matrix of* $H^1(n,3)$. *If* $a_n = \dim(C_2(A_n)) = \text{rank}_2(A_n)$, *then for* $n \geq 1$, $a_n = \frac{1}{2}(3^n - (-1)^n)$.

Proof. From Lemma 4.2.1, $A_n^2 = A_n$ and hence $C_2(A_n)^\perp = C_2(A_n + I)$. Since $A + A + I = I$, we have $C_2(A_n) + C_2(A_n + I) = \mathbb{F}_2^{3^n}$. Hence $C_2(A_n) \cap C_2(A_n + I) = \{0\}$. Further, $\text{rank}_2(A_1) = 2$.
Thus, over $\mathbb{F}_2$, writing $A = A_{n-1}$,

$$A_n \sim \begin{pmatrix} I & I & A \\ 0 & A+I & A+I \\ 0 & 0 & 0 \end{pmatrix}. \tag{4.4}$$

28

From this we have

$$a_n = 3^{n-1} + (3^{n-1} - a_{n-1}).$$

By the induction hypothesis

$$a_{n-1} = \frac{1}{2}(3^{n-1} - (-1)^{n-1}).$$

So we obtain

$$a_n = 3^{n-1} + (3^{n-1} - \frac{1}{2}(3^{n-1} - (-1)^{n-1})) = 3^{n-1} + 3^{n-1} - \frac{3^{n-1}}{2} + \frac{1}{2}(-1)^{n-1} =$$

$$\frac{3}{2}(3^{n-1}) + \frac{1}{2}(-1)^{n-1} = \frac{1}{2}(3^n + (-1)^{n-1}) = \frac{1}{2}(3^n - (-1)(-1)^{n-1}) = \frac{1}{2}(3^n - (-1)^n).$$

$$\square$$

Corollary 4.2.3. *Let A_n be an adjacency matrix of $H^1(n,2)$ and $A_n + I$ an adjacency matrix of $H^*(n,2)$. Denote the code generated by rows of A_n, $A_n + I$ by $C = C_2(A_n)$ and $C^* = C_2(A_n + I)$ respectively. Then $C^* = C^\perp$ and $C \cap C^\perp = \{0\}$.*

4.3 The binary codes of $\mathcal{D}(n,3)$ and $\mathcal{D}^*(n,3)$

In this section we discuss the binary codes of $\mathcal{D}(n,3)$ and $\mathcal{D}^*(n,3)$ are symmetrics $1 - (3^n, 2n, 2n)$ design and $1 - (3^n, 2n+1, 2n+1)$ design respectively as described in Section 4.1.

Lemma 4.3.1. [12, Proposition 2] *Let A_n be an adjacency matrix of $H^1(n,3)$ and $A_n + I$ an adjacency matrix of $H^*(n,3)$. Denote the code generated by the rows of A_n, $A_n + I$ by $C = C_2(A_n)$ and $C^* = C_2(A_n + I)$ respectively. Then the minimum words are the incidence vectors of $\mathcal{D}(n,3)$ and $\mathcal{D}^*(n,3)$ respectively.*

Proof. We prove by induction, noting that the base case is obvious. Recall that $A_n \sim \begin{pmatrix} I & I & A_{n-1} \\ 0 & A_{n-1} + I & A_{n-1} + I \\ 0 & 0 & 0 \end{pmatrix}$.

From the matrix A_n above, a word $w \in C$ or C^* will be the concatenation of three components of length 3^{n-1} which we will write as w_1, w_2, w_3.

We first consider a word w in C which is a sum of r of the first block of 3^{n-1} rows will have $w_1 = \sum_{i \in H} e_i$, $w_2 = \sum_{i \in H} e_i$, $w_3 = \sum_{i \in H} b_i$, where $|H| = r \geq 1$, and hence the word has weight at least $2r + 2(n-1) \geq 2n$ unless $w_3 = 0$. If $\text{wt}(w) = 2r + 2(n-1) = 2n$, then $r = 1$ and w is the incidence vector of a block. If $w_3 = \sum_{i \in H} b_i = 0$, then $\sum_{i \in H} b_i^* = \sum_{i \in H} e_i \neq 0$. By induction this has weight at least $2n - 1$ so $\text{wt}(w) \geq 2(2n - 1) = 4n - 2 > 2n$ for $n > 1$. For the second block of 3^{n-1} rows, if a sum of rows is not zero, then it will have weight at least $2(2n - 1) = 4n - 2 > 2n$.

By placing r rows from the first set and s from the second, and assuming that the sum is zero, we obtain that $w_1 = \sum_{i \in H} e_i$, $w_2 = \sum_{i \in H} e_i + \sum_{j \in J} b_j^*$, $w_3 = \sum_{i \in H} b_i + \sum_{j \in J} b_j^*$, where $|J| = s \geq 1$, and $\text{wt}(w) \geq r + (2n - 1 - r) + t$, where $\text{wt}(w_3) = t$. If $t = 0$, then $\sum_{i \in H} b_i = \sum_{j \in J} b_j^* = 0$, since $C_2(A) \cap C_2(A + I) = \{0\}$, which contradicts the assumption that the sum of the rows is not zero. So $t \geq 1$ and $\text{wt}(w) \geq 2n - 1 + t \geq 2n$. Further, $\text{wt}(w) > 2n$ unless $t = 1$. If $t = 1$, then $w_3 = e_k = \sum_{i \in H} b_i + \sum_{j \in J} b_j^*$, so $w_2 = \sum_{i \in H} b_i^* + e_k$. If $\sum_{i \in H} b_i^* = 0$, then $\sum_{i \in H} b_i = \sum_{i \in H} e_i \neq 0$, and hence of weight $r \geq 2(n-1)$ by the induction hypothesis, so $\text{wt}(w) \geq 2(n-1) + 2 = 2n$. If $\text{wt}(w) = 2n$ then $r = 2(n - 1)$ and by induction $\sum_{i \in H} b_i = \sum_{i \in H} e_i = b_m$. Then $w_3 = e_k = b_m + \sum_{j \in J} b_j^*$, and $b_m^* + \sum_{j \in J} b_j^* = e_k + e_m$ has weight 2 or 0. Therefore it must be 0, so $k = m$. By the ordering of the vectors, we have w the incidence vector of the block from the mth row. If $\sum_{i \in H} b_i^* \neq 0$, then $\text{wt}(w) \geq r + 2n - 2 + 1 > 2n$ unless $r = 1$. If $r = 1$ then $w_1 = e_i$, $w_2 = b_i^* + e_k$ and $w_3 = e_k$. Since $w_3 = b_i + \sum_{j \in J} b_j^* = e_k$, we get $i = k$ and hence w is the incidence vector of the ith block.

Now let us consider C^*. Placing r rows from the first $3^{n-1} \times 3^{n-1}$ submatrix of A_n^*, we have $\text{wt}(w) \geq 2r + 2n - 1 \geq 2n + 1$ for $r \geq 1$, unless $w_3 = \sum_{i \in H} b_i^* = 0$, in which case $\sum_{i \in H} e_i = \sum_{i \in H} b_i \neq 0$ and hence $\text{wt}(\sum_{i \in H} e_i) = r \geq 2(n - 1)$. Then $\text{wt}(w) = 2r \geq 4(n - 1) \geq 2n + 1$ for $n \geq 3$, for a non-zero sum of rows from the second set we get weight at least $4(n - 1) \geq 2n + 1$ for $n \geq 3$. Now, take $r \geq 1$ rows from the first set and $s \geq 1$ from the second, and assume that the sum is zero. Then $w_1 = \sum_{i \in H} e_i$, $w_2 = \sum_{i \in H} e_i + \sum_{j \in J} b_j$, $w_3 = \sum_{i \in H} b_i^* + \sum_{j \in J} b_j$, where $|H| = r \geq 1$ and $|J| = s \geq 1$. We have $\text{wt}(w) = \text{wt}(w_1) + \text{wt}(w_2) + \text{wt}(w_3) \geq r + 2(n - 1) - r + t$, where $\text{wt}(w_3) = t$, since $\sum_{j \in J} b_j \neq 0$ by assumption. Therefore $\text{wt}(w) \geq 2n + 1$ if $t \geq 3$.

$\square$

The following theorem summarises the properties of the above codes.

Theorem 4.3.2. [12, Proposition 2] *If $n \geq 4$, then $C = C_2(\mathcal{D}(n,3))$ is $[3^n, \frac{1}{2}(3^n - (-1)^n), 2n]_2$ and $C^* = C^\perp = C_2(\mathcal{D}(n,3)^*)$ is $[3^n, \frac{1}{2}(3^n + (-1)^n), 2n + 1]_2$. Further $C \cap C^\perp = \{0\}$ and the minimum weight words of C and C^* are the incidence vectors of the blocks of $\mathcal{D}(n,3)$ and $\mathcal{D}^*(n,3)$ respectively.*

Proof. By Proposition 4.2.2 we have the dimension of C and C^*. We have the minimum words by Lemma 4.3.1. That $C \cap C^* = \{0\}$ follows from Corollary 4.2.3. $\square$

4.4 The automorphism groups of $\mathcal{D}(n,3)$ and $\mathcal{D}^*(n,3)$

We now discuss the automorphism groups of $\mathcal{D}(n,3)$ and $\mathcal{D}^*(n,3)$ respectively.

Lemma 4.4.1. [12, Lemma 2] *Let x, y be two distinct points of $\mathbb{F}_3^n$. If x, y are on a blocks of $\mathcal{D}(n,3)$ and $\mathcal{D}^*(n,3)$ respectively then $d(x,y) = 1, 2$. If $d(x,y) = 1$ then they are together on either 1 block or 3 blocks.*

Proof. Consider when x, y is on a block of $\mathcal{D}(n,3)$ and $x, y \in \bar{z}$. Then $d(x,z) = d(y,z) = 1$. From the above argument we have that $d(x,y) \leq d(x,z) + d(z,y) \leq 2$. If $d(x,y) = 1$, and they differ at the 1 coordinate. Then they are together on one block $\bar{z}$ for $z = (x_1)$, $z_1 \in F_3 \setminus \{x_1, y_1\}$.

Now consider when x, y is on a block of $\mathcal{D}^*(n,3)$. Suppose $x, y \in \bar{\bar{z}}$. Then $d(x,y) \leq 2$ as has been discussed in the above argument when x, y is on a block of $\mathcal{D}(n,3)$. If $d(x,y) = 1$ then we get one block as in the previous discusion, but also the blocks $\bar{x}$ and $\bar{y}$. Therefore they are together on three blocks.

$\square$

Proposition 4.4.2. [12, Proposition 3] *For $n \neq 2$, $\mathrm{Aut}(\mathcal{D}(n,3)) = \mathrm{Aut}(\mathcal{D}^*(n,3)) = \mathrm{Aut}(H^1(n,3))$.*

Proof. First we show that $\mathrm{Aut}(\mathcal{D}(n,3)) = \mathrm{Aut}(\mathcal{D}^*(n,3))$. Write $\mathcal{T} = \mathcal{D}(n,3)$ and $\mathcal{T}^* = \mathcal{D}^*(n,3)$. We show by using the results from Lemma 4.4.1.

(i) In order to show that $\sigma \in \mathrm{Aut}(\mathcal{D}^*(n,3))$, we suppose $\sigma \in \mathrm{Aut}(\mathcal{D}(n,3))$. If $x, y \in \bar{z}$ then $d(x,y) = 1, 2$. If $d(x,y) = 1$ then x, y are together on one block of $\mathcal{T}$ and so $\sigma(x), \sigma(y)$ are on one block of $\mathcal{T}$ and hence of $\mathcal{T}^*$. Therefore $\sigma \in \mathrm{Aut}(\mathcal{D}^*(n,3))$.

(ii) Now suppose $\sigma \in \text{Aut}(\mathcal{D}^*(n,3))$. If $x, y \in \bar{\bar{z}}$ then $d(x,y) = 1, 2$. If $d(x,y) = 1$ then x, y are together on 3 blocks of $\mathcal{T}^*$, and so $\sigma(x)$, $\sigma(y)$ are on 3 blocks of $\mathcal{T}^*$. Since $\sigma(x)$, $\sigma(y)$ are in $H^1(n,3)$, $d(\sigma(x), \sigma(y)) = 1$ and $\sigma(x)$, $\sigma(y)$ are on one block of $\mathcal{T}$.

From (i) and (ii) it is clearly to see that $\text{Aut}(\mathcal{D}(n,3)) = \text{Aut}(\mathcal{D}^*(n,3))$. Therefore $\text{Aut}(H^1(n,3)) \leq \text{Aut}(\mathcal{D}(n,3)) = \text{Aut}(\mathcal{D}^*(n,3))$. Suppose $\sigma \in \text{Aut}(\mathcal{D}^*(n,3))$, and suppose $[x,y] \in E(H^1(n,3))$. Then $d(x,y) = 1$ and so x, y are together on 3 blocks of $\mathcal{T}^*$. Thus $\sigma(x)$, $\sigma(y)$ are together on 3 blocks of $\mathcal{T}^*$. Hence we have $d(\sigma(x), \sigma(y)) = 1$, and $[\sigma(x), \sigma(y)] \in E(H^1(n,3))$. $\qquad\square$

Corollary 4.4.3. [12, Corollary 2] *For $n \geq 1$, $\text{Aut}(C_2(\mathcal{D}(n,3))) \cong S_3 \wr S_n$.*

Proof. Recall Proposition 4.3.2, it reads as follows, the minimum words are the incidence vectors of the design, when $n \geq 4$. Then any automorphism of the code preserve the blocks of the design, and the result follows from Proposition 4.4.2. $\qquad\square$

In the next chapter, we will discuss the binary codes from the line graph of $H^1(n,2)$.

Chapter 5

Binary codes from the line graph of $H^1(n,2)$

In this chapter, we consider binary codes from the line graph of the $H^1(n,2)$. In Section 5.2 we describe the binary codes from line graph of $H^1(n,2)$. Further, in Section 5.3 we consider codes from adjacency matrices of these line graphs, and in Section 5.4 we focus on automorphism groups of $L(H^1(n,2))$ as well as the hulls.

5.1 The graph $L(H^1(n,2))$

Let $L(H^1(n,2))$ denote the line graph of the n-cube $H^1(n,2)$. Then in $L(H^1(n,2))$, two distinct vertices $[x,y]$ and $[u,w]$ are adjacent if $|\{x,y\} \cap \{u,w\}| = 1$. The neighborhood design $\mathcal{D}_n$ of $L(H^1(n,2))$ has for points the vertices of $L(H^1(n,2))$, i.e, the set $\mathcal{P}_n$ of edges of $H^1(n,2)$. For each point $[x,y]$ we defined the block

$$\overline{[x,y]} = \{[x,u]|\mathrm{wt}(x+u) = 1, u \neq y\} \cup \{[y,w]|\mathrm{wt}(y+w) = 1, w \neq x\}. \quad (5.1)$$

Hence $\mathcal{D}_n$ has a block set $\left\{\overline{[x,y]}|[x,y] \in \mathcal{P}_n\right\}$. Let G_n denote the $2^n \times n2^{n-1}$ vertex by edge incidence matrix of the graph $H^1(n,2)$ with the vertices (rows) ordered in the usual standard way by the binary representation of the numbers 0 to $2^n - 1$, writing

$$\Sigma_{i=0}^{n-1} a_i 2^i = (a_0, a_1, \cdots, a_{n-1}),$$

where $a_i \in \mathbb{F}_2$ for $0 \le i \le n-1$.

The columns of G_n, representing the edges of $H^1(n, 2)$, are ordered in the following manner. Take $G_1 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$. Suppose G_{n-1} has been defined. For G_n we order the rows in the standard way as described. For the columns, the first $2^{n-2}(n-1)$ columns will represent the edges between the first 2^{n-1} vertices, the next 2^{n-1} columns will represent the edges $[x, x+e_n]$ between the first 2^{n-1} and the second 2^{n-1} vertices, starting with the edges $[0, e_n], [e_1, e_1+e_n], [e_2, e_2+e_n]$, and so on, i.e. ordered according to the vertices in the first set of 2^{n-1}. The final $2^{n-2}(n-1)$ columns will represent the edges between vertices in the second set of vertices, i.e. those with nth coordinate 1. For $n = 3$, the ordering of rows is $0, e_1, e_2, e_1+e_2, e_3, e_1+e_3, e_2+e_3, e_1+e_2+e_3$, and the ordering of the edges is $[0, e_1], [0, e_2], [e_1, e_1+e_2], [e_2, e_1+e_2], [0, e_3], [e_1, e_1+e_3], [e_2, e_2+e_3], [e_1+e_2, e_1+e_2+e_3], [e_3, e_1+e_3], [e_3, e_2+e_3], [e_1+e_3, e_1+e_2+e_3], [e_2+e_3, e_1+e_2+e_3]$.

Now let us consider the case for $n = 4$.

Example 5.1.1. *For $n = 4$, the ordering of the rows is*

$0, \ e_1, \ e_2, \ e_1+e_2, \ e_3, \ e_1+e_3, \ e_2+e_3, \ e_1+e_2+e_3, \ e_4, \ e_1+e_4, \ e_2+e_4, \ e_1+e_2+e_4, \ e_3+e_4, \ e_1+e_3+e_4, \ e_2+e_3+e_4, \ e_1+e_2+e_3+e_4,$

and the ordering of the edges is

$[0, e_1], \ [0, e_2], \ [e_1, e_1+e_2], \ [e_2, e_1+e_2], \ [0, e_3], \ [e_1, e_1+e_3], \ [e_2, e_2+e_3], \ [e_1+e_2, e_1+e_2+e_3], \ [e_3, e_1+e_3], \ [e_3, e_2+e_3], \ [e_1+e_3, e_1+e_2+e_3], \ [e_2+e_3, e_1+e_2+e_3], [0, e_4], \ [e_1, e_1+e_4], \ [e_2, e_2+e_4], \ [e_3, e_3+e_4], \ [e_1+e_2, e_1+e_2+e_4], \ [e_3, e_3+e_4], [e_1+e_3, e_1+e_3+e_4], \ [e_2+e_3, e_2+e_3+e_4], \ [e_1+e_2+e_3, e_1+e_2+e_3+e_4], [e_4, e_1+e_4], \ [e_4, e_2+e_4], \ [e_1+e_4, e_1+e_2+e_4], \ [e_2+e_4, e_1+e_2+e_4], \ [e_4, e_3+e_4], [e_1+e_4, e_1+e_3+e_4], \ [e_2+e_4, e_2+e_3+e_4], \ [e_1+e_2+e_4, e_1+e_2+e_3+e_4], [e_3+e_4, e_1+e_3+e_4], \ [e_3+e_4, e_2+e_3+e_4], \ [e_1+e_3+e_4, e_1+e_2+e_3+e_4], [e_2+e_3+e_4, e_1+e_2+e_3+e_4]$.

Thus, $G_4 = \left(\begin{array}{ccc|cc|cc} \begin{array}{c} 110010000000 \\ 101001000000 \\ 010100100000 \\ 001100010000 \\ 000010001100 \\ 000001001010 \\ 000000100101 \\ 000000010011 \\ \hline 000000000000 \\ 000000000000 \\ 000000000000 \\ 000000000000 \\ 000000000000 \\ 000000000000 \\ 000000000000 \\ 000000000000 \end{array} & \begin{array}{c} 10000000 \\ 01000000 \\ 00100000 \\ 00010000 \\ 00001000 \\ 00000100 \\ 00000010 \\ 00000001 \\ \hline 10000000 \\ 01000000 \\ 00100000 \\ 00010000 \\ 00001000 \\ 00000100 \\ 00000010 \\ 00000001 \end{array} & \begin{array}{c} 000000000000 \\ 000000000000 \\ 000000000000 \\ 000000000000 \\ 000000000000 \\ 000000000000 \\ 000000000000 \\ 000000000000 \\ \hline 110010000000 \\ 101001000000 \\ 010100100000 \\ 001100010000 \\ 000010001100 \\ 000001001010 \\ 000000100101 \\ 000000010011 \end{array} \end{array}\right)$.

With this ordering described, we see that

$$G_n = \left(\begin{array}{c|c|c} G_{n-1} & I_{2^{n-1}} & 0 \\ \hline 0 & I_{2^{n-1}} & G_{n-1} \end{array}\right). \tag{5.2}$$

Let A_n be the adjacency matrix of $L(H^1(n,2))$ with this ordering of the edges. Writing $I = I_{2^{n-1}n}$,

$$A_n = G_n^T G_n - 2I$$

$$= \left(\begin{array}{ccc} G_{n-1}^T G_{n-1} & G_{n-1}^T & 0 \\ G_{n-1} & I_{2^{n-1}} & G_{n-1} \\ 0 & G_{n-1}^T & G_{n-1}^T G_{n-1} \end{array}\right) - 2I = \left(\begin{array}{ccc} A_{n-1} & G_{n-1}^T & 0 \\ G_{n-1} & 0 & G_{n-1} \\ 0 & G_{n-1}^T & A_{n-1} \end{array}\right), \tag{5.3}$$

where

$$G_n^T = \left(\begin{array}{cc} G_{n-1}^T & 0 \\ I_{2^{n-1}} & I_{2^{n-1}} \\ 0 & G_{n-1}^T \end{array}\right). \tag{5.4}$$

35

Let $\mathcal{G}_n$ be the $1 - (2^{n-1}n, n, 2)$ design with incidence matrix G_n. Then the point set of $\mathcal{G}_n$ is that of $\mathcal{D}_n$, i.e $\mathcal{P}_n$, and the block defined by $x \in V_n$ is given by

$$\bar{\bar{x}} = \{[x, x + e_i] | 1 \le i \le n\}. \tag{5.5}$$

5.2 Binary codes

In this section we consider the graphs and designs as has been described in Section 5.1. Note that Equation (5.3) implies that $A_n = G_n^\perp G_n$. Let $C_2(\mathcal{D}_n)$ be the binary code from $\mathcal{D}_n$ and $C_2(A_n)$ the binary code from A_n.

Also, we have $C_2(L(H^1(n,2))) = C_2(\mathcal{D}_n) = C_2(A_n)$ and $C_2(G_n) = C_2(\mathcal{G}_n)$. For any $x \in V_n$, $1 \le i \le n$,

$$v^{\overline{[x, x+e_i]}} = v^{\bar{\bar{x}}} + v^{\overline{x+e_i}}, \tag{5.6}$$

since

$$\overline{[x, x + e_i]} = (\bar{\bar{x}} \cup \overline{\overline{x + e_i}}) \backslash (\bar{\bar{x}} \cap \overline{\overline{x + e_i}}).$$

Lemma 5.2.1. [13, Lemma 3.] *For $n \ge 1$ and $n \ge 2$, let (G_n) be the incident matrix of the graph $L(H^1(n, 2))$. Then*

(1) $\text{rank}_2(G_n) = 2^n - 1$, $n \ge 1$

(2) $\text{rank}_2(A_n) = 2^n - 2$, $n \ge 2$

Proof. We employ inductions. (1) For $n = 1$, we have $G_1 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$. Now $r_1 = r_2$, where r_1 and r_2 are the rows of G_1 is 1 and induction hypothesis is true for $n = 1$. Suppose the hypothesis holds for $k \le n$. Consider

$$G_n = \left(\begin{array}{c|c|c} G_{n-1} & I_{2^{n-1}} & 0 \\ \hline 0 & I_{2^{n-1}} & G_{n-1} \end{array} \right).$$

By the induction hypothesis G_{n-1} has full rank. Hence

$$G_n = \left(\begin{array}{c|c|c} G_{n-1} & I_{2^{n-1}} & 0 \\ \hline G_{n-1} & I_{2^{n-1}} & 0 \end{array} \right).$$

Therefore the rank of G_n is $2^n - 1$.

(2) Let $Y = C_2(G_n^T)$. We define the map $\tau : G_n \to C_2(A_n)$ by $\tau(v) = vG_n$ for $v \in Y$. Since Equation (5.3) have $\mathrm{rank}_2(A_n) \le 2^n - 1$ and $C_2(A_n) \subseteq C_2(G_n)$, then it is easly to see that the sum of the middle block of rows of G_n^T is the vectors $\jmath_{2^n}$. Therefore $\jmath_{2^n} \in Y$ and $\jmath_{2^n} \in ker(\tau)$. Hence $\dim(C_2(A_n)) = 2^n - 2$.

$\square$

Corollary 5.2.2. [13, Corollary 4.]

For $n \ge 4$, as described from the column of matrix G_n, and $\mathcal{T}_n = \bigcup_{i=2}^{n-1} \{2^{i-2}(i+2) + t \mid 1 \le t \le 2^{i-2}(i-2)\}$, the columns in the set of positions $\mathcal{T}_n$. Then $\mathcal{T}_n$ are placed at the end of the matrix G_n and the first $2^n - 1$ column will be an information set for $C_2(G_n)$.

Proof. We consider the matrix G_n from Equation (5.2). It is easily seen $C_2(G_n)$ by using the inductive step. The same argument holds for $C_2(A_n)$, so that the first $2^{n-1} - 1$ position will be obtanained from the results for $C_2(G_n)$. Next we consider the matrix G_{n-1}^T. Since G_{n-1}^T has rank $2^{n-1} - 1$ and $2^{n-1} - 1$ columns, then it is easy to see that $2^{n-1} - 1$ has been taken from G_{n-1}^T. $\square$

Proposition 5.2.3. *For $n \ge 2$, $C_2(A_n)$ is a $[2^{n-1}n, 2^n - 2, 2(n-1)]_2$ code. For $n \ge 4$ the minimum words of $C_2(A_n)$ are the rows of A_n.*

Proof. (By Induction). By Equation (5.3), when $n = 4$, we have

$$A_4 = \begin{pmatrix} A_3 & G_3^T & 0 \\ G_3 & 0 & G_3 \\ 0 & G_3^T & A_3 \end{pmatrix},$$

from this matrix we have that A_n have weight $2(n-1)$. Suppose it is true for $n - 1$. We have

$$A_{n-1} = \begin{pmatrix} A_{n-1} & G_{n-1}^T & 0 \\ G_{n-1} & 0 & G_{n-1} \\ 0 & G_{n-1}^T & A_{n-1} \end{pmatrix}.$$

This matrix will be concatenation of the vectors, w_1, w_2 and w_3 corresponding to the block matrices. Label the row blocks R_i, $i = 1, 2, 3$.

(i) From matrix A_{n-1} we take $k \ge 1$ rows from R_1, then $w_1 = \Sigma_{i \in I} a_i$, where a_i is the ith row of A_{n-1} and $|I| = k$. Then if g_i is the ith row of

G_{n-1}^T, $w_2 = \Sigma_{i \in I} g_i$ and $a_i = g_i G_{n-1}$. Also $w_3 = 0$. So $w_1 = w_2 G_{n-1}$. So $w_2 \neq 0$ and hence has weight at least 2, since $C_2(G_{n-1}^T)$ is an even weight code. If $w_1 \neq 0$ then $\text{wt}(w_1) \geq 2(n-2)$ by the induction hypothesis, and so $\text{wt}(w) \geq 2(n-2)+2 = 2(n-1)$. If $\text{wt}(w) = 2(n-1)$ then $\text{wt}(w_1) = 2(n-1)$, so that $w_1 = a_m = \Sigma_{i \in I} a_i$, by the induction hypothesis, and $\text{wt}(w_2) = 2$. So $a_m = g_m G_{n-1} = w_2 G_{n-1}$, and thus $g_m + w_2 = \jmath_{2^{n-1}}$ or 0. Both g_m and w_2 have weight 2, so we must have $g_m = w_2$, which means that w is a row of A_n. If $w_1 = 0$ then $w_2 G_{n-1} = 0$ so $w_2 = \jmath_{2^{n-1}}$, and $\text{wt}(w) = 2^{n-1} > 2(n-1)$ for $n \geq 4$.

(ii) If we take $k \geq 1$ rows from R_2, then $w_1 = w_3 = \Sigma_{i \in I} s_i \neq 0$, where s_i is the ith row of G_{n-1}, i.e. $s_i = g_i^T$. So $\text{wt}(w) \geq 2(n-1)$, with equality only if $w_1 = w_3 = s_m$, i.e. a row of A_n.

(iii) When $k \geq 1$ rows from R_3, we apply the same argument in (i).

(iv) Now take $k \geq 1$ rows from R_1 and $j \geq 1$ rows from R_2. Here $w_1 = \Sigma_{i \in I} g_i G_{n-1} + \Sigma_{j \in J} s_j = u + v$, $w_2 = \Sigma_{i \in I} g_i$, $w_3 = \Sigma_{j \in J} s_j = v \neq 0$, if $w_2 = 0$ then $u = 0$. So $\text{wt}(w_2) \geq 2$. If $w_1 \geq 0$ then $\text{wt}(w) \geq n-1+2+n-1 \geq 2(n-1)$ (since $u \in C_2(A_{n-1}) \subset C_2(G_{n-1})$). Here if $\text{wt}(w) = 2(n-1)$ then $\text{wt}(w_1) = \text{wt}(w_3) = n-1$, and $v = u + v = s_m$ for some m. Thus $u = \Sigma_{i \in I} g_i G_{n-1} = 0$ so that $w_2 G_{n-1} = 0$, which implies that $w_2 = \jmath_{2^{n-1}}$ or 0, which gives a contradiction in each case. If $w_1 = 0$ then $u = v \in C_2(A_{n-1})$. Thus $u \neq 0$ and $\text{wt}(w) \geq 2+2(n-2) = 2(n-1)$. If $\text{wt}(w) = 2(n-1)$ then $u = v = s_m$, for some m, by induction, so $w_2 = g_m G_{n-1}$ and w is a row of A_n. Next, take $k \geq 1$ rows from R_1 and $j \geq 1$ rows from R_3. Here $w_1 = \Sigma_{i \in I} g_i G_{n-1}$, $w_2 = \Sigma_{i \in I} g_i + \Sigma_{j \in J} g_j$, $w_3 = \Sigma_{j \in J} g_j G_{n-1}$. If $w_1, w_3 \neq 0$ then $\text{wt}(w) \geq 2(n-2) + 2(n-2) > 2(n-1)$ for $n \geq 4$. If $w_1 = 0$ then $\Sigma_{i \in I} g_i = \jmath_{2^{n-1}}$. If $w_2 = 0$ then $\Sigma_{j \in J} g_j = \jmath_{2^{n-1}}$ and hence $w_3 = 0$. Thus $w_2 \neq 0$. Since $w_3 \neq 0$ (otherwise $w = 0$), we have $\text{wt}(w) \geq 2+2(n-2) = 2(n-1)$, with equality if and only if $w_3 = a_m$ for some m, by induction. Then, as before, $\Sigma_{j \in J} g_j + g_m = \jmath_{2^{n-1}}$ or 0. If the former then $w_2 = g_m$, and we get a row of A_n, if 0 then we get $\text{wt}(w_2) > 2$. Similarly if $w_3 = 0$.

(v) Take $k \geq 1$ rows from R_1, $j \geq 1$ rows from R_2, $l \geq 1$. Then $w_1 = \Sigma_{i \in I} g_i G_{n-1} + \Sigma_{j \in J} s_j = u + v$, $w_2 = \Sigma_{i \in I} g_i + \Sigma_{t \in K} g_t$, where $|K| = l$, and $w_3 = \Sigma_{t \in K} g_t G_{n-1} + \Sigma_{j \in J} s_j = y + v$. If $w_1, w_3 \neq 0$ then $\text{wt}(w) \geq 2(n-1)$ with equality only if $w_1 = s_m$, $w_3 = s_r$, $w_2 = 0$, for some m, r. Since $w_2 = 0$ we have $\Sigma_{i \in I} g_i = \Sigma_{t \in K} g_t$, and so $\Sigma_{i \in I} g_i G_{n-1} = \Sigma_{t \in K} g_t G_{n-1}$, i.e. $u = y$ and so $s_m = s_r$ and we have a row of A_n. If $w_1 = 0$ then $u = v$, so $w_3 = \Sigma_{t \in K} g_t G_{n-1} + \Sigma_{i \in I} g_i G_{n-1} = w_2 G_{n-1}$. If $w_3 = 0$, then $w_2 = 0$ or $\jmath_{2^{n-1}}$, so

for $w \neq 0$, $\text{wt}(w) = 2^{n-1} > 2(n-1)$ for $n \geq 4$. If $w_3 \neq 0$ then $w_2 \neq 0$, so $\text{wt}(w) \geq 2 + 2(n-2)$, with equality if $w_3 = a_m$, for some m, and so $w_3 = a_m = g_m G_{n-1} = w_2 G_{n-1}$, so that $w_2 + g_m = j_{2^{n-1}}$, 0. Since $\text{wt}(w_2) = 2$, we must have $w_2 = g_m$, and again we have a row of A_n.

(vi) When $k \geq 1$ rows from R_1, $j \geq 1$ rows from R_3, $l \geq 1$, then we apply the same argument in (v). $\qquad\square$

Lemma 5.2.4. [13, Lemma 7.] *If* $C = C_2(\mathcal{D}_n)$ *or* $C_2(\mathcal{G}_n)$, *then for* $n \geq 2$, $C^\perp$ *contains the weight-4 codeword*

$$u(x,y,z) = v^{[x,y]} + v^{[x,z]} + v^{[x+y+z,y]} + v^{[x+y+z,z]}, \qquad (5.7)$$

where $x \in V_n$, $y = x + e_i$, $z = x + e_j$, $1 \leq i, j \leq n$, $i \neq j$. *Further,* $C^\perp$ *has minimum weight-4 .*

Proof. The result follows from Lemma 2.3.9, $\qquad\square$

Lemma 5.2.5. *Blocks of the design* $\mathcal{D}_n$ *meet in 0, 1, 2, or* $n - 2$ *points.*

Proof. Consider the block $\overline{[0, e_2]}$.
(i) Take the edges $[0, e_i]$ and $[0, e_j]$, where $2, i, j$ are distinct. Then these edges $(n-2)$ blocks $\overline{[0, e_k]}$ for $k \neq i, j$.
Similarly, $[e_2, e_2 + e_i]$ and $[e_2, e_2 + e_j]$, where $2, i, j$ are distinct, are on the $(n-2)$ blocks $[e_2, e_2 + e_k]$ for $k \neq i, j$, there are $(n-1)(n-2)$ pairs of points.

(ii) The edges $[0, e_i]$ and $[e_2, e_2 + e_i]$, $i \neq 2$, are on the two blocks $\overline{[0, e_2]}$ and $\overline{[e_i, e_2 + e_i]}$. There are $n - 1$ pairs of such points.

(iii) Now, we place the pair of ordering of edges $[0, e_i]$ and $[e_2, e_2 + e_j]$, where $2, i, j$ are distinct. Then there are together on the one block $\overline{[0, e_2]}$. There are $(n-1)(n-2)$ such pairs of points.

Now we consider the number of blocks that meet $\overline{[0, e_2]}$:

(iv) The blocks $\overline{[e_i, e_i + e_j]}$ and $\overline{[e_i + e_2, e_i + e_2 + e_j]}$ for $2, i, j$ all distinct, meets in exactly one point. There are $2(n-1)(n-2)$ of these.

(v) The block $\overline{[e_i, e_i + e_2]}$ meets in two points, there are $n - 1$ of these.

(vi) Finally the blocks $\overline{[0, e_i]}$ and $\overline{[e_1, e_i + e_1]}$, for $i \neq 1$, meets in $n - 2$ points. We have $2(n-1)$ of these. Therefore it does not intersect $2^{n-1}n - 1 - (2n^2 - n - 2n + 1) = 2^{n-1}n - 1 - (2n^2 - 3n + 1) = 2^{n-1}n - 1 - (n-1)(2n-1)$ blocks.

$\qquad\square$

5.3 Codes from adjacency matrices of line graphs

In this section we look at the codes $C_p(A_n)$, where A_n is an adjacency matrix of $L(H^1(n, 2))$, the line graph of the n-cube.

$G_n = G_n(2)$ will be a $2^n \times \frac{1}{2}2^n n$ incidence matrix of $H^1(n, 2)$, and $G_n^T G_n = A_n + 2I_{\frac{1}{2}2^n n}$. Recall that
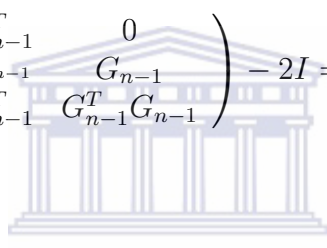
$$G_n = \left(\begin{array}{c|c|c} G_{n-1} & I_{2^{n-1}} & 0 \\ \hline 0 & I_{2^{n-1}} & G_{n-1} \end{array} \right)$$

and

$$A_n = G_n^T G_n - 2I$$

$$= \left(\begin{array}{ccc} G_{n-1}^T G_{n-1} & G_{n-1}^T & 0 \\ G_{n-1} & I_{2^{n-1}} & G_{n-1} \\ 0 & G_{n-1}^T & G_{n-1}^T G_{n-1} \end{array} \right) - 2I = \left(\begin{array}{ccc} A_{n-1} & G_{n-1}^T & 0 \\ G_{n-1} & 0 & G_{n-1} \\ 0 & G_{n-1}^T & A_{n-1} \end{array} \right)$$

where

$$G_n^T = \left(\begin{array}{cc} G_{n-1}^T & 0 \\ I_{2^{n-1}} & I_{2^{n-1}} \\ 0 & G_{n-1}^T \end{array} \right).$$

Proposition 5.3.1. [15] *Let G_n be an incidence matrix for $H^1(n, 2)$, and A_n adjacency matrix for the line graph $L(H^1(n, 2))$.*
(1) $C_2(A_n)$ is the subcode of $C_2(G_n)$ spanned by the difference of the rows of G_n.
(2) $C_p(A_n)$ has minimum weight at most 4, and for $n \geq 3$ $C_p(A_n) \supseteq C_p(G_n)^\perp$, for p an odd prime.

Proof. (1) Recall $C_2(G_n)$ has dimension $2^n - 1$. We have $G_n^\perp G_n = A_n$. Therefore $C_2(A_n) \subseteq C_2(G_n)$, For $\jmath_{2^n}$, the all-one vector of length 2^n, we have $\jmath_{2^n} G = 0$.

(2) Let G be the row span of G_n^T over $\mathbb{F}_2$. Define a map $\tau : G \to C$ by $\tau : g = (g_1, \cdots, g_{2^n}) \mapsto (g_1, \cdots, g_{2^n})G_n$, so that $\tau(G) = C$ and $\dim(C) + \dim(\ker(\tau)) = \dim(G) = 2^n - 1$.

Note that $\dim(G) = 2^n - 1$. The map $\tau : G \to C$ is defined by a vector g is in the kernel if and only if $g \in G$ and $gG_n = 0$. Since $\jmath_{2^n}G_n = 0$. We need to determine when $\jmath_{2^n} \in G$. If n is odd, then $\jmath_{2^n}$ is the sum of all the rows of G_n^T. Otherwise $\jmath_{2^n}$ is the sum of all the rows besides those containing $I_{2^{n-1}}$. So $\dim(C) = 2^n - 2$. Since this is the dimension of the code spanned by the difference of the rows of G_n, it follows that C is precisely this subcode of $C_2(G_n)$ since $C \subseteq C_2(G_n)$. For p odd, since $C_p(A)$ contains all the weight-4 vectors of the form described in Equation (2.1), it follows by Proposition 3.2.4 that $C_p(A_n) \supseteq C_p(G_n))^\perp$. $\qquad\square$

5.4 Codes from incidence matrices of $L(H^1(n,2))$

In this section, we briefly discuss the codes from an incidence matrix of $L(H^1(n,2))$. We also consider the row span over $\mathbb{F}_p$, for any prime p, of $L_n(2)$ the incidence matrix, for the line graph of $H^1(n,2)$ for $n \geq 1$.

Consider a $2^{n-1}n \times 2^{n-1}n(n-1)$ incidence matrix $L_n(2)$ of $L(H^1(n,2))$ with a particular ordering on the rows and columns. Each row of $L_n(2)$ has $2(n-1)$ entries equal to 1, including the case $n = 1$. In this which case the line graph has no edges.

Let $G_n = G_n(2)$ be an incidence matrix of $H^1(n,2)$. Now for the rows of $L_n(2)$ we use the same ordering we had for the columns of $G_n(2)$. Call these sets R_1, R_2, R_3. For the columns, we assume we have an ordering for $L_{n-1}(2)$, and for the first set of columns for $L_n(2)$ insert $L_{n-1}(2)$ in the rows R_1. For the next set of columns, insert $L_{n-1}(2)$ in R_2 to show the edges between $[x + e_n, y + e_n]$, and $[x + e_n, z + e_n]$, where $[x, y]$, $[x, z]$ are on an edge in $L(H^1(n,2))$. For the next columns take all edges between those points in R_1 and R_3, followed by those in R_2 and R_3. We need to start with $L_2(2)$, and from our ordering for $G_2(2)$ we can order the columns so that $L_2(2)$ is as follows:

$$G_2(2) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, L_2(2) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}. \qquad (5.8)$$

Therefore,

$$L_3(2) = \begin{pmatrix} \begin{array}{cccc} 1100 & 0000 & 11000000 & 00000000 \\ 0011 & 0000 & 00110000 & 00000000 \\ 1010 & 0000 & 00001100 & 00000000 \\ 0101 & 0000 & 00000011 & 00000000 \\ \hline 0000 & 1100 & 00000000 & 11000000 \\ 0000 & 0011 & 00000000 & 00110000 \\ 0000 & 1010 & 00000000 & 00001100 \\ 0000 & 0101 & 00000000 & 00000011 \\ \hline 0000 & 0000 & 10001000 & 10001000 \\ 0000 & 0000 & 01000010 & 01000010 \\ 0000 & 0000 & 00100100 & 00100100 \\ 0000 & 0000 & 00010001 & 00010001 \end{array} \end{pmatrix}. \tag{5.9}$$

For $n = 4$, $L_4(2)$ have 16 entries and $2^3.4 \times 2^3 4(3) = 8.3 \times 8(12) = 32 \times 96$, meaning that $L_4(2)$ have 32 columns and 96 rows.

In general, for $n \geq 2$, recalling that for $n = 2$ the matrix $L_{n-1}(2)$ has no columns,

$$L_n(2) = \left(\begin{array}{cc|c|c} L_{n-1}(2) & 0 & N & 0 \\ \hline 0 & L_{n-1}(2) & 0 & O \\ \hline 0 & 0 & P & Q \end{array} \right), \tag{5.10}$$

where N, O are $2^{n-2}(n-1) \times 2^{n-1}(n-1)$ matrices, and P, Q are $2^{n-1} \times 2^{n-1}(n-1)$ matrices. Every column of N, O, P, Q has exactly one non-zero entry 1 in it, and every row of N and O has precisely two non-zero entries 1 in it. Row of P and Q has precisely $(n-1)$ non-zero entries 1 in it. Clearly every row of $L_{n-1}(2)$ has $2(n-2)$ entries equal to 1. We represent the column blocks C_i for $i = 1, 2, 3, 4$. The following lemma will be used as our inductive base

Lemma 5.4.1. [15] $C_2(L_4(2)) = [96, 32, 6]_2$. *The vectors of weight* 6 *are the scalar multiples of the rows of* $L_4(2)$ *for all* p.

Proof. Consider $p = 2$, from the matrix of $L_2(2)$, $w = \Sigma_{i=1}^4 \alpha_i r_i = (\alpha_1 + \alpha_2, \alpha_3 + \alpha_4, \alpha_1 + \alpha_3, \alpha_2 + \alpha_4) = 0$ for $1 \leq i \leq 4$. This implies that $\alpha_1 = -\alpha_2 = -\alpha_3 = \alpha_4$.

Consider $L_4(2)$, as have been discussed immediately after Equation (5.9). Label the first four rows as R_1, the next four as R_2 and the last four as R_3. Then any vector $w \in C_p(L_4(2))$ can be viewed as a concatenation of vectors in the four column blocks. So write $w = (w_1, w_2, w_3, w_4)$ where w_1, w_2 are in F_p^{12} and w_3, w_4 are in F_p^{42}. $\mathrm{Wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_2) + \mathrm{wt}(w_3) + \mathrm{wt}(w_4)$. To prove that C has dimension 32, notice that $([0, e_1], [e_1, e_1 + e_2], [e_1 + e_2, e_1 + e_2 + e_3]$, $[e_1 + e_2 + e_3, e_1 + e_3], [e_1 + e_3, e_1])$ is a closed path of odd length 5.

Now take w to be a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1. Then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + 2k$. If $w_1 = 0$ then from the above discussion we must have $k = 6$ and thus $\mathrm{wt}(w) = 12$. If $w_1 \neq 0$ then $\mathrm{wt}(w) \geq 2 + 2k \geq 12$, with equality only when $k = 1$ and we have a multiple of a row. The same argument applies to a sum of rows from R_2, since N is equivalent to O. If w is a sum of $k \geq 1$ non-zero scalar multiples of rows from R_3, then $\mathrm{wt}(w) = 6k \geq 6$ with equality only if $k = 1$. If w is a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1 and $m \geq 1$ non-zero scalar multiples of rows from R_2, then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_2) + 2k + 2m \geq 2(k+m) \geq 12$ with equality only if $k = m = 1$ and $w_1 = w_2 = 0$, and this cannot happen. If w is a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1 and $m \geq 1$ non-zero scalar multiples of rows from R_3, then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_3) + 2m$. If $w_1 = 0$ then $k = 6$ and $\mathrm{wt}(w) = \mathrm{wt}(w_3) + 2m > 12$ if $m \geq 3$. If $m = 1$ then $\mathrm{wt}(w_3) \geq 6$. So all the words we get are of weight greater than 6. So $\mathrm{wt}(w_1) \geq 2$, and so $\mathrm{wt}(w) \geq 6$ with equality only if $m = 1$, $\mathrm{wt}(w_1) = 2$ and $w_3 = 0$. The latter is impossible since the rows of N with one row of O are linearly independent, where N and O are as shown in Equation (5.10). A similar argument applies to w a sum of rows from R_2 and R_3. Therefore we cannot get words of weight 6 this way. Finally, take w to be a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1, $j \geq 1$ non-zero scalar multiples of rows from R_2 and $m \geq 1$ non-zero scalar multiples of rows from R_3. Then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_2) + \mathrm{wt}(w_3) + \mathrm{wt}(w_4)$. Denoting the 32 rows of L_4 by r_i for $1 \leq i \leq 32$, write $w = \Sigma_{i=1}^6 \alpha_i r_i + \Sigma_{i=1}^6 \beta_i r_{6+i} + \Sigma_{i=1}^6 \gamma_i r_{12+i}$ where k of the α_i, m of the β_i and j of the γ_i are not zero. From L_4 we see that

$$w_3 = (\alpha_1 + \gamma_1, \alpha_1 + \gamma_2, \alpha_2 + \gamma_3, \alpha_2 + \gamma_4, \alpha_3 + \gamma_1, \alpha_3 + \gamma_3, \alpha_4 + \gamma_2, \alpha_4 + \gamma_4 \cdots). \quad (5.11)$$

If $w_3 = 0$ then $\gamma_i = \gamma = -\alpha_i$ for all $1 \leq i \leq 6$ and hence $k = m = 6$, and $\mathrm{wt}(w_1) = 6$. It also follows from Equation (5.11) that if $w_3 \neq 0$ then $\mathrm{wt}(w_3) \geq 2$. The same argument applies to w_4, so if $w_4 = 0$ then $m = j = 6$, and $\mathrm{wt}(w_2) = 6$, so $\mathrm{wt}(w) > 6$. So $w_4 \neq 0$ and hence $\mathrm{wt}(w_3) \geq 2$ and $\mathrm{wt}(w) \geq 6$. So we can assume neither $w_3, w_4 \neq 0$. Then $\mathrm{wt}(w) \geq 6$ if one of w_1 or w_2 is not 0. So supposing $w_1, w_2 = 0$ then $k = 6 = j$, and, with $\alpha, \beta \neq 0$,

43

$w_3 = \alpha(1,1,1,1,-1,-1,-1,-1)+(\gamma_1,\gamma_2,\gamma_3,\gamma_4,\gamma_1,\gamma_3,\gamma_2,\gamma_4) = (\alpha+\gamma_1,\alpha+\gamma_2,\alpha+\gamma_3,\alpha+\gamma_4,-\alpha+\gamma_1,-\alpha+\gamma_3,-\alpha+\gamma_2,-\alpha+\gamma_4)$.

From this we see that $\mathrm{wt}(w_3) \geq 6$. Similarly,

$w_4 = \beta(1,1,1,1,-1,-1,-1,-1)+(\gamma_1,\gamma_2,\gamma_3,\gamma_4,\gamma_1,\gamma_3,\gamma_2,\gamma_4) = (\beta+\gamma_1,\beta+\gamma_2,\beta+\gamma_3,\beta+\gamma_4,-\beta+\gamma_1,-\beta+\gamma_3,-\beta+\gamma_2,-\beta+\gamma_4)$.

So $\mathrm{wt}(w_4) \geq 6$. $\qquad\square$

Proposition 5.4.2. [15] *For $n \geq 1$, let $L_n(2)$ be a $2^{n-1}n \times 2^{n-1}n(n-1)$ incidence matrix for $L(H^1(n,2))$. For $n \geq 4$,*
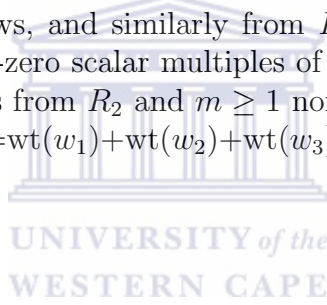
(1) $C_2(L_n(2)) = [2^{n-1}n(n-1), 2^{n-1}n - 1, 2(n-1)]_2$,

(2) $C_p(L_n(2)) = [2^{n-1}n(n-1), 2^{n-1}n, 2(n-1)]_p$, *for p odd.*

Proof. (1) For $p = 2$, we recall Lemma 5.4.1. We therefore have the result for $n = 4$. So we proceed by induction. Suppose $n \geq 4$ and that the induction hypothesis is true for $n - 1$, and consider $L_n(2)$ as shown in Equation (5.10). We use the same constructions and labelling as from previous Lemma. $w = (w_1, w_2, w_3, w_4)$. Let $C = C_2(L_n(2))$. It is clear that $\dim(C) \leq 2^{n-1}n - 1$ since the sum of all the rows is 0. Further, notice that any $2^{n-1}n - 1$ rows of $L_{n-1}(2)$ are linearly independent. By induction the dimension is at least this as the rows from R_1 give dimension at least $2^{n-2}(n-1) - 1$, and the those from R_2 and R_3 give dimension $2^{n-2}(n-1)$ and 2^{n-1}, respectively, since each column has exactly one entry 1 in it, and each row has at least one entry 1. If w is a sum of $k \geq 1$ rows r_i from R_1, then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_3) = \mathrm{wt}(w_1) + 2k$ since N has every row containing exactly two entries 1, and every column exactly one entry 1. If $w_1 = 0$ then $k = 2^{n-2}(n-1)$ and $\mathrm{wt}(w) = 2^{n-1}(n-1) > 2(n-1)$. Otherwise $\mathrm{wt}(w) \geq 2(n-2) + 2k \geq 2(n-2) + 2 = 2(n-1)$ with equality only if $k = 1$. The same argument holds for w a sum of rows from R_2. If w is a sum of $k \geq 1$ rows from R_2, then $\mathrm{wt}(w) = 2(n-1)k \geq 2(n-1)$,(since P, Q each have their rows consisting of $n - 1$ entries equal to 1), with equality only if $k = 1$ and w is a scalar multiple of a row.

(2) Now consider the cases for p odd. We prove the result using induction, having established the induction base in Lemma 5.4.1. Suppose the statement is true for $n - 1$, where $n \geq 4$, and consider $L_n(2)$ as shown in Equation (5.10). Use the same constructions and labelling as for the proof of the case when $n = 3$. Thus $w = (w_1, w_2, w_3, w_4)$. Let $C = C_p(L_n(2))$. It is clear that

$\dim(C) = 2^{n-1}n$ since the rows from R_1 and R_2 each give dimension $2^{n-1}(n-1)$ by induction, and those from R_3 give dimension 2^{n-1} since each column has exactly one non-zero entry 1 in it, and each row has at least one entry 1. If w is a sum of $k \geq 1$ non-zero scalar multiples of rows r_i from R_1, then $\text{wt}(w) = \text{wt}(w_1) + \text{wt}(w_3) \geq 2(n-2) + 2k$ since N has every row containing exactly two entries 1, and every column containing exactly one entry 1. If $k \geq 2$ then $\text{wt}(w) \geq 2n$, so we only get weight $2(n-1)$ when $k = 1$. The same argument holds for w a sum of rows in R_2. If w is a sum of $k \geq 1$ non-zero scalar multiples of rows from R_3, then $\text{wt}(w) = 2(n-1)k \geq 2(n-1)$, (since P, Q each have their rows consisting of $n-1$ entries equal to 1), with equality only if $k = 1$ and w is a scalar multiple of a row. If w is a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1 and $m \geq 1$ non-zero scalar multiples of rows from R_2 then $\text{wt}(w) = \text{wt}(w_1) + \text{wt}(w_2) + 2k + 2m > 2(n-1)$. If w is a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1 and $m \geq 1$ non-zero scalar multiples of rows from R_3, then $\text{wt}(w) = \text{wt}(w_1) + \text{wt}(w_3) + m(n-1) \geq 2(n-2) + \text{wt}(w_3) + m(n-1) \geq 3n - 5 > 2n - 2$ for $n \geq 4$. So no weight $2(n-1)$ can arise from this combination of rows, and similarly from R_2 and R_3. Finally, take w to be a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1, $j \geq 1$ non-zero scalar multiples of rows from R_2 and $m \geq 1$ non-zero scalar multiples of rows from R_3. Then $\text{wt}(w) = \text{wt}(w_1) + \text{wt}(w_2) + \text{wt}(w_3) + \text{wt}(w_4) \geq 4(n-2) > 2n - 4$ for $n \geq 4$.

$\square$

5.5 Automorphism groups of the codes and designs from $L(H^1(n, 2))$

In this section we consider the automorphism groups of the designs and their codes.

Proposition 5.5.1. [13, Proposition 9.] *For $n \geq 4$, $\text{Aut}(L(H^1(n, 2))) = \text{Aut}(\mathcal{D}_n) = \text{Aut}(\mathcal{G}_n) \cong \text{Aut}(H^1(n, 2))$.*

Proof. Let $H = \text{Aut}(L(H^1(n, 2)))$, $H^* = \text{Aut}(\mathcal{D}_n)$ and $G = \text{Aut}(\mathcal{G}_n)$.
First we need to show that $H = H^*$. Since $H \leq H^*$, we prove that $\sigma \in H$ implies that $\sigma \in H^*$.

Suppose $[x, y]$, $[z, w] \in E(H^*)$, $z = x$, $\sigma([x, y])$ are on $n - 2$ blocks for $n > 4, 5$. This means that $\sigma([x, y]) = [X, Y]$, $\sigma([x, w]) = [X, W] \in E(H^*)$. Hence $\sigma \in \text{Aut}(H^*)$. $\square$

45

Corollary 5.5.2. [13, Corollary 10.] (1) *For $n \geq 4$, $\mathrm{Aut}(C_2(\mathcal{D}_n)) = T \rtimes S_n$, and (2) for $n \geq 3$, $\mathrm{Aut}(C_2(\mathcal{G}_n)) = T \rtimes S_n$.*

Proof. (1)By Proposition 5.5.1 above, since an automorphism of the code must preserves the weight classes, then it preserves the blocks and hence the design. Then the words of weight $2n - 2 = 2(n-1)$ of $C_2(\mathcal{D}_n)$ are the incidence vectors of the blocks of $\mathcal{D}_n$.

(2) The same argument holds for $C_2(\mathcal{G}_n)$. □

5.6 The hulls

In this section we consider the hulls of the two designs $\mathcal{D}_n$ and $\mathcal{G}_n$. Let $\mathrm{Hull}_p(\mathcal{D}) = C_p(\mathcal{D}) \cap C_p(\mathcal{D})^\perp$. This is also denoted by $\mathrm{Hull}(\mathcal{D})$, when p is clear from the context.

We denote vectors of V_n by the numbers $0, 1, \cdots, 2^n - 1$ in the usual way, and as has been described in Section 5.1. Then

$$E_i = \langle e_j | j \in \{1, \cdots, n\} \setminus \{i\} \rangle, \tag{5.12}$$

for $1 \leq i \leq n$.

Lemma 5.6.1. [13, Lemma 11.] *For $n \geq 2$, $1 \leq i \leq n$, let*

$$S_i = \{[u, u + e_i] | u \in E_i\}, \tag{5.13}$$

$$T_i = \{[e_i + u, e_i + e_{i+1} + u] | u \in \langle e_j | j \in \{1, \cdots, n\} \setminus \{i, i+1\} \rangle\}, \tag{5.14}$$

(where i is taken modulo n in the definition of T_i). Then, for $1 \leq i \leq n$,

$$v^{S_i} = \Sigma_{x \in T_i} v^{\bar{x}},$$

has weight 2^{n-1}, and is in $\mathrm{Hull}(\mathcal{D}_n)$. Each S_i is an arc for $\mathcal{D}_n$.

Proof. Let $S = S_1 = \{[2k, 2k+1] | 0 \leq k \leq 2^{n-1} - 1\}$, $T = T_1 = \{[4i+1, 4i+3] | 0 \leq i \leq 2^{n-1} - 1\}$, $C = C_2(\mathcal{D}_n)$, $w = \Sigma_{z \in T} v^{\bar{z}}$ and $W = Supp(w)$.

46

First we need to show that $S \subseteq W$. Now Let $P = [2k, 2k + 1] \in S$. If $k = 2l$ then $P = [4l, 4l + 1] \in \overline{[4l + 1, 4l + 3]}$ Therefore $P \in W$

We denote the points in terms of the vectors in $V_n = \mathbb{F}_2^n$: $4i + 1 = e_1 + \Sigma_{k=3}^n \alpha_k e_k$, $4i + 3 = e_1 + e_2 + \Sigma_{k=3}^n \alpha_k e_k$, and writing $u = \Sigma_{k=3}^n \alpha_k e_k$, then
$\overline{[4i + 1, 4i + 3]} = \{[e_1 + u, e_1 + u + e_k] | 3 \leq k \leq n\} \cup$
$\{[e_1 + u, u]\} \cup \{[e_1 + e_2 + u, e_1 + e_2 + u + e_k] | 3 \leq k \leq n\} \cup$
$\{[e_1 + e_2 + u, e_2 + u]\}$.
If $[x, y] \in \overline{[4i + 1, 4i + 3]}$, and $[x, y] \notin S$, then, with this notation, $[x, y] = [e_1 + u, e_1 + u + e_k]$ or $[x, y] = [e_1 + e_2 + u, e_1 + e_2 + u + e_k]$, for some $k \geq 3$. On other hand, $[x, y] \in \overline{[e_1 + (u + e_k), e_1 + e_2 + (u + e_k)]}$, i.e $[x, y]$ is in exactly one other block $\bar{z}$ for $z \in T$. Thus the points eliminate out in the sum, and we have obtained that $w = v^S$. Thus $v^S \in C$.
To prove that $v^S = w \in C^{\perp}$, we show that every block of the design meets it in zero or two points. If $[u, u + e_1] \in S$ is in $\overline{[v, v + e_k]}$, then $[u, u + e_1] = [v, v + e_j]$ or $[u, u + e_1] = [v + e_k, v + e_k + e_j]$ for some $j \neq k$. If $u = v$, $u + e_1 = v + e_j$, so $j = 1$ and $k \neq 1$ and then $u + e_k = v + e_k$, $u + e_k + e_1 = v + e_k + e_1$, so $[u + e_k, u + e_k + e_1] \in \overline{[v, v + e_k]}$. If another point $[t, t + e_1] \in S$ is in $\overline{[v, v + e_k]}$ simply show that it must be one of the points. Then $v^S \in C^{\perp}$ and S is an arc. $\qquad\square$

Lemma 5.6.2. [13, Lemma 12.] *For $n \geq 3$, let*

$$w_n = \Sigma_{i=1}^n v^{\overline{[0, e_i]}} = n v^{\bar{0}} + \Sigma_{i=1}^n v^{\overline{e_1}}. \qquad (5.15)$$

Then $w_n \in \mathrm{Hull}(\mathcal{D}_n) \cap \mathrm{Hull}(\mathcal{G}_n)$,

$$Supp(w) = S = \{[e_i, e_i + e_j] | 1 \leq i, j \leq n\} \text{ for } n \text{ even}, \qquad (5.16)$$
$$Supp(w) = S = \{[e_i, e_i + e_j] | 1 \leq i, j \leq n, i \neq j\} \text{ for } n \text{ odd}, \qquad (5.17)$$

and $\mathrm{wt}(w_n) = n(n - 1)$ for n odd, $\mathrm{wt}(w_n) = n^2$ for n even.

Proof. First we need to show that $w_n \in C^{\perp}$. Now consider the blocks $\overline{[u, u + e_i]}$. It is easy to see that $w_n \in C = C_2(\mathcal{D}_n)$. If $\mathrm{wt}(u) \geq 3$ and $\mathrm{wt}(u + e_i) \geq 3$, then is clear to conclude that $\overline{[u, u + e_i]}$ does not meet w_n at all. We also apply the same argument in order to verify that $w_n \in C_2(\mathcal{G}_n)^{\perp}$. $\qquad\square$

For the following Lemma, we recall S from Equation (5.17) and Equation (5.18) respectively and E_i for Equation (5.14).

Lemma 5.6.3. [13, **Lemma 13.**] *For $n \geq 3$, if S is as in (5.17) and (5.18) and*

$$\mathcal{S} = \{T_w(S) | w \in E_1\},$$

then the points of $\mathcal{P}$ can be in the following number of sets in $\mathcal{S}$:

$$
\begin{aligned}
Case\ 1: \quad & 2, n, 2(n-1)\ for\ n\ even, \\
Case\ 2: \quad & 2, n-1, 2(n-1)\ for\ n\ odd.
\end{aligned}
$$

Further, $\Sigma_{R \in \mathcal{S}} v^R = 0$.

Proof. Consider when n even. Then we have

$$S = \{[e_i, e_i + e_j] | 1 \leq i, j \leq n\}.$$

Now, we list and count the element of $w \in E_1$ for $T_w(P) \in \mathcal{S}$ at a point $P = [u, u + e_i]$, where $1 \leq i \leq n$. $[e_1 + \Sigma_{i \in I} e_i, e_1 + \Sigma_{i \in I} e_i + e_j]$, $1, j \notin I : \Sigma_{i \in I} e_i$, $\Sigma_{i \in I} e_i + e_j$, bringing 2 elements.

$[\Sigma_{i \in I} e_i, e_1 + \Sigma_{i \in I} e_i]$, $1 \notin I : \Sigma_{i \notin I} e_i$, $\Sigma_{i \in I} e_i + e_i (i \in I)$, $\Sigma_{i \in I} e_i + e_k (k \notin I, k \neq 1)$, bringing n elements. $[\Sigma_{i \in I} e_i, e_j + \Sigma_{i \in I} e_i]$, $j \notin I$, $j \neq 1$: $\Sigma_{i \in I} e_i$, $\Sigma_{i \in I} e_i + e_j$, $\Sigma_{i \in I} e_i + e_i (i \in I)$, $\Sigma_{i \in I} e_i, e_i + e_j (i \in I)$, $\Sigma_{i \in I} e_i + e_k (k \notin I, k \neq 1)$, $\Sigma_{i \in I} e_i + e_k + e_j (k \notin I, k \neq 1, j)$, bringing $2n - 2$ elements.

For n is odd. Then

$$S = \{[e_i, e_i + e_j] | 1 \leq i, j \leq n, i \neq j\}.$$

$[e_1 + \Sigma_{i \in I} e_i, e_1 + \Sigma_{i \in I} e_i + e_j]$, $j \notin I : \Sigma_{i \in I} e_i$, $\Sigma_{i \in I} e_i + e_j$, bringing 2 elements. $[\Sigma_{i \in I} e_i, e_1 + \Sigma_{i \in I} e_i]$, $1 \notin I : \Sigma_{i \in I} e_i + e_i (i \in I)$, $\Sigma_{i \in I} e_i + e_k (k \notin I, k \neq 1)$, bringing $n - 1$ elements. $[\Sigma_{i \in I} e_i, e_j + \Sigma_{i \in I}]$, $j \notin I$, $j \neq 1 : \Sigma_{i \in I} e_i + e_i (i \in I)$, $\Sigma_{i \in I} e_i + e_i + e_j (i \in I)$, $\Sigma_{i \in I} e_i + e_k (k \notin I, k \neq 1, j)$, $\Sigma_{i \in I} e_i + e_k + e_j (k \notin I, k \neq 1, j)$, bringing $2n - 2$ elements.

$\square$

Proposition 5.6.4. [13, **Proposition 14.**] (1) *For $n \geq 3$, with $\mathcal{S}$ as in Lemma 5.6.3, $\dim \langle v^R | R \in \mathcal{S} \rangle = 2^{n-1} - 1$. (2) $\dim(\text{Hull}(\mathcal{G}_n)) \geq 2^{n-1} - 1$ and $\dim(\text{Hull}(\mathcal{D}_n)) \geq 2^{n-1}$.*

Proof. (1) Firstly we need to show that the set $\{v^R | R \in \mathcal{S} \setminus \{S\}\}$ is linearly independent. By using the count method from Lemma 5.6.3.

Now for n even, then $u \in E_1$, take $S_u = T_u(S)$. Let $U \subset E_1$, $0 \notin U$ and $U \neq \emptyset$. Suppose $\Sigma_{u \in U} v^{S_u} = 0$. Now let $I = \emptyset$, and $e_i \in U$ for any i we see that from the first case when n is even, $e_i + e_j \notin U$ for any i and j. Now we use this case inductively so prove that U is empty, contrary to our assumption. Thus the set is linearly independent.

For case when n is odd the identical argument holds.

(2) By Lemma 5.6.3 we immediately conclude that the dim(Hull($\mathcal{G}_n$)) $\geq 2^{n-1} - 1$. For the statement concern about Hull($\mathcal{D}_n$)) we need to prove that the words v_{S_i} of weight 2^{n-1} of Equations (5.14)(5.15) of Lemma 5.6.1 are in Hull($\mathcal{D}_n$) but not in Hull($\mathcal{G}_n$), so that the code spanned by the v^R together with one of these words will have dimension 2^{n-1}. □

It is easy to see that $\Sigma_{i=1}^{n} v^{T_{e_i}(S)} = 0$ and also v^S for n even and odd respectively.

Now we recall Equation (5.8) in the dual code $C^\perp$. With the notation $u(x, y, z)$, note that any three vectors of the set $\{x, y, z, x + y + z\}$ are together in the support of at most one of these weight-4 vectors.

Proposition 5.6.5. [13, Proposition 15.] *For $n \geq 3$, the weight-4 vectors $u(x, y, z)$ span $C_2(\mathcal{G}_n)^\perp$.*

Proof. Recall the ordering of the points of the design as has been described in Section 5.1, with at least a leading terms $2^{n-1}(n - 2) + 1$. Since this is the dimension of $C_2(\mathcal{G}_n)^\perp$ and all the vectors are in $C_2(\mathcal{G}_n)^\perp$ by Lemma 5.6.3, they will thus span $C_2(\mathcal{G}_n)^\perp$. We refer to the leading term with this ordering. Thus for example the leading term of $u(0, e_2, e_3)$ is $[0, e_2]$.

For $n \geq 3$ we will construct a set $\mathcal{F}_n$ of vectors $u(x, y, z)$ that have $f_n = 2^{n-1}(n - 2) + 1$ leading terms in echelon array. Let $l_n = 2^{n-1}n$, the length of the code $C_2(\mathcal{G}_n)$ or $C_2(\mathcal{G}_n)^\perp$. We will order the columns as described in Section 5.1 for G_n, and label them with the numbers from 1 to l_n.

We start with $n = 3$. Here $l_3 = 12$, $f_3 = 5$, and we take $\mathcal{F}_3$ to consist of the five weight-4 vectors:

$u(0, e_1, e_3)$ (leading term $[0, e_1]$ at position 1),
$u(0, e_2, e_3)$ (leading term $[0, e_2]$ at position 2),

$u(e_1, e_1 + e_2, e_1 + e_3)$ (leading term $[e_1, e_1 + e_2]$ at position 3),
$u(e_2, e_2 + e_1, e_2 + e_3)$ (leading term $[e_2, e_1 + e_2]$ at position 4),
$u(e_3, e_1 + e_3, e_2 + e_3)$ (leading term $[e_3, e_1 + e_3]$ at position 9).
Notice that we have no leading terms in the range $5 \leq k \leq 8$ of length $4 = 2^{n-1}$.

Next we construct the set for $n = 4$. Here $l_4 = 32$, $f_4 = 17$, and we take $\mathcal{F}_4$ to consist of the 17 weight-4 vectors:
$u(0, e_1, e_3)$ (leading term $[0, e_1]$ at position 1),
$u(0, e_2, e_3)$ (leading term $[0, e_2]$ at position 2),
$u(e_1, e_1 + e_2, e_1 + e_3)$ (leading term $[e_1, e_1 + e_2]$ at position 3),
$u(e_2, e_2 + e_1, e_2 + e_3)$ (leading term $[e_2, e_1 + e_2]$ at position 4),
$u(0, e_3, e_4)$ (leading term $[0, e_3]$ at position 5),
$u(e_1, e_1 + e_3, e_1 + e_4)$ (leading term $[e_1, e_1 + e_3]$ at position 6),
$u(e_2, e_2 + e_3, e_2 + e_4)$ (leading term $[e_2, e_2 + e_2]$ at position 7),
$u(e_1 + e_2, e_1 + e_2 + e_3, e_1 + e_2 + e_4)$ (leading term $[e_1 + e_2, e_1 + e_2 + e_3]$ at position 8),
$u(e_3, e_1 + e_3, e_3 + e_4)$ (leading term $[e_3, e_1 + e_3]$ at position 9),
$u(e_3, e_2 + e_3, e_3 + e_4)$ (leading term $[e_3, e_2 + e_3]$ at position 10),
$u(e_1 + e_3, e_1 + e_2 + e_3, e_1 + e_3 + e_4)$ (leading term $[e_1 + e_3, e_1 + e_2 + e_3]$ at position 11),
$u(e_2 + e_3, e_1 + e_2 + e_3, e_2 + e_3 + e_4)$ (leading term $[e_2 + e_3, e_1 + e_2 + e_3]$ at position 12),
$u(e_4, e_1 + e_4, e_3 + e_4)$ (leading term $[e_4, e_1 + e_4]$ at position 21),
$u(e_4, e_2 + e_4, e_3 + e_4)$ (leading term $[e_4, e_2 + e_4]$ at position 22),
$u(e_1 + e_4, e_1 + e_2 + e_4, e_1 + e_3 + e_4)$ (leading term $[e_1 + e_4, e_1 + e_2 + e_4]$ at position 23),
$u(e_2 + e_4; =, e_1 + e_2 + e_4, e_2 + e_3 + e_4)$ (leading term $[e_2 + e_4, e_1 + e_2 + e_4]$ at position 24),
$u(e_3 + e_4, e_1 + e_3 + e_4, e_2 + e_3 + e_4)$ (leading term $[e_3 + e_4, e_1 + e_3 + e_4]$ at position 25.

Notice that we have no leading term in the range $13 \leq k \leq 20$ of length $8 = 2^{n-1}$ corresponding to the middle section of G_4 as given in the matrix of Equation (5.2).
Now, suppose that $n \geq 3$ and we have constructed $\mathcal{F}_{n-1}$ of size f_{n-1} in this way , having the centre section of 2^{n-2} positions with no leading terms. We construct $\mathcal{F}_n$ as follows: the first l_{n-1} positions will all be leading terms by first taking all the elements of $\mathcal{F}_{n-1}$ except for the last one,$(\Sigma_{i=3}^{n-1} e_i, e_1 + \Sigma_{i=3}^{n-1} e_i, e_2 + \Sigma_{i=3}^{n-1} e_i)$ with the right most leading term $[\Sigma_{i=3}^{n-1} e_i, e_1 + \Sigma_{i=3}^{n-1} e_i]$. Then, for each of the remaining columns in the first set of l_{n-1}t, for the edge $[x, x + e]$ where $x \in \langle e_i | 1 \leq i \leq n - 1 \rangle$ and $e = e_i$, for $1 \leq i \leq n - 1$, we adjoin to

our set $\mathcal{F}_n$ the word $u(x, x + e, x + e_n)$ which will clearly have leading term $[x, x + e]$. Thus far we have l_{n-1} elements in $\mathcal{F}_n$. Now, we skip the next 2^{n-1} column positions, and then adjoin f_{n-1} words formed from the words of $\mathcal{F}_{n-1}$ as follows: if $u(x, x + e, x + f) \in \mathcal{F}_{n-1}$ with leading term $[x, x + e]$ then $u(x + e_n, x + e + e_n, x + f + e_n) \in \mathcal{F}_n$ with leading term $[x + e_n, x + e + e_n]$. This gives the required $f_n = l_{n-1} + f_{n-1}$ words and they are in echelon form, with the middle section of length 2^{n-1} excluded. This concludes the proof. $\qquad\square$

Below, we show the 49 elements of f_5 obtained in this way. Note that for $n = 5$, the ordering of the rows is

0, e_1, e_2, e_3, e_4, $e_1 + e_2$, $e_1 + e_3$, $e_1 + e_4$, $e_2 + e_3$, $e_2 + e_4$, $e_3 + e_4$, $e_1 + e_2 + e_3$, $e_1 + e_2 + e_4$, $e_1 + e_3 + e_4$, $e_2 + e_3 + e_4$, $e_1 + e_2 + e_3 + e_4$, e_5, $e_1 + e_5$, $e_2 + e_5$, $e_3 + e_5$, $e_4 + e_5$, $e_1 + e_2 + e_5$, $e_1 + e_3 + e_5$, $e_1 + e_4 + e_5$, $e_2 + e_3 + e_5$, $e_2 + e_4 + e_5$, $e_3 + e_4 + e_5$, $e_1 + e_2 + e_3 + e_5$, $e_1 + e_2 + e_4 + e_5$, $e_1 + e_3 + e_4 + e_5$, $e_2 + e_3 + e_4 + e_5$, $e_1 + e_2 + e_3 + e_4 + e_5$.

and the ordering of the edges is

$[0, e_1]$, $[0, e_2]$, $[0, e_3]$, $[0, e_4]$, $[e_1, e_1 + e_2]$, $[e_1, e_1 + e_3]$, $[e_1, e_1 + e_4]$, $[e_2, e_1 + e_2]$, $[e_2, e_2 + e_3]$, $[e_2, e_2 + e_4]$, $[e_3, e_1 + e_3]$, $[e_3, e_2 + e_3]$, $[e_3, e_3 + e_4]$, $[e_4, e_1 + e_4]$, $[e_4, e_2 + e_4]$, $[e_4, e_3 + e_4]$, $[e_1 + e_2, e_1 + e_2 + e_3]$, $[e_1 + e_2, e_1 + e_2 + e_4]$, $[e_1 + e_3, e_1 + e_2 + e_3]$, $[e_1 + e_3, e_1 + e_3 + e_4]$, $[e_1 + e_4, e_1 + e_2 + e_4]$, $[e_1 + e_4, e_1 + e_3 + e_4]$, $[e_2 + e_3, e_1 + e_2 + e_3]$, $[e_2 + e_3, e_2 + e_3 + e_4]$, $[e_2 + e_4, e_1 + e_2 + e_4]$, $[e_2 + e_4, e_2 + e_3 + e_4]$, $[e_3 + e_4, e_1 + e_3 + e_4]$, $[e_3 + e_4, e_2 + e_3 + e_4]$, $[e_1 + e_2 + e_3, e_1 + e_2 + e_3 + e_4]$, $[e_1 + e_2 + e_4, e_1 + e_2 + e_3 + e_4]$, $[e_1 + e_3 + e_4, e_1 + e_2 + e_3 + e_4]$, $[e_2 + e_3 + e_4, e_1 + e_2 + e_3 + e_4]$, $[0, e_5]$, $[e_1, e_1 + e_5]$, $[e_2, e_2 + e_5]$, $[e_3, e_3 + e_5]$, $[e_4, e_4 + e_5]$, $[e_1 + e_2, e_1 + e_2 + e_5]$, $[e_1 + e_3, e_1 + e_3 + e_5]$, $[e_1 + e_4, e_1 + e_4 + e_5]$, $[e_2 + e_3, e_2 + e_3 + e_5]$, $[e_2 + e_4, e_2 + e_4 + e_5]$, $[e_3 + e_4, e_3 + e_4 + e_5]$, $[e_1 + e_2 + e_3, e_1 + e_2 + e_3 + e_5]$, $[e_1 + e_2 + e_4, e_1 + e_2 + e_4 + e_5]$, $[e_1 + e_3 + e_4, e_1 + e_3 + e_4 + e_5]$, $[e_2 + e_3 + e_4, e_2 + e_3 + e_4 + e_5]$, $[e_1 + e_2 + e_3 + e_4, e_1 + e_2 + e_3 + e_4 + e_5]$, $[e_5, e_1 + e_5]$, $[e_5, e_2 + e_5]$, $[e_5, e_3 + e_5]$, $[e_5, e_4 + e_5]$, $[e_1 + e_5, e_1 + e_2 + e_5]$, $[e_1 + e_5, e_1 + e_3 + e_5]$, $[e_1 + e_5, e_1 + e_4 + e_5]$, $[e_2 + e_5, e_1 + e_2 + e_5]$, $[e_2 + e_5, e_2 + e_3 + e_5]$, $[e_2 + e_5, e_2 + e_4 + e_5]$, $[e_3 + e_5, e_1 + e_3 + e_5]$, $[e_3 + e_5, e_2 + e_3 + e_5]$, $[e_3 + e_5, e_3 + e_4 + e_5]$, $[e_4 + e_5, e_1 + e_4 + e_5]$, $[e_4 + e_5, e_2 + e_4 + e_5]$, $[e_4 + e_5, e_3 + e_4 + e_5]$, $[e_1 + e_2 + e_5, e_1 + e_2 + e_3 + e_5]$, $[e_1 + e_2 + e_5, e_1 + e_2 + e_4 + e_5]$, $[e_1 + e_3 + e_5, e_1 + e_2 + e_3 + e_5]$, $[e_1 + e_3 + e_5, e_1 + e_3 + e_4 + e_5]$, $[e_1 + e_4 + e_5, e_1 + e_2 + e_4 + e_5]$, $[e_1 + e_4 + e_5, e_1 + e_3 + e_4 + e_5]$, $[e_2 + e_3 + e_5, e_1 + e_2 + e_3 + e_5]$, $[e_2 + e_3 + e_5, e_2 + e_3 + e_4 + e_5]$, $[e_2 + e_4 + e_5, e_1 + e_2 + e_4 + e_5]$, $[e_2 + e_4 + e_5, e_2 + e_3 + e_4 + e_5]$, $[e_3 + e_4 + e_5, e_1 + e_3 + e_4 + e_5]$, $[e_3 + e_4 + e_5, e_2 + e_3 + e_4 + e_5]$, $[e_1 + e_2 + e_3 + e_5, e_1 + e_2 + e_3 + e_4 + e_5]$,

$[e_1 + e_2 + e_4 + e_5, e_1 + e_2 + e_3 + e_4 + e_5], [e_1 + e_3 + e_4 + e_5, e_1 + e_2 + e_3 + e_4 + e_5],$
$[e_2 + e_3 + e_4 + e_5, e_1 + e_2 + e_3 + e_4 + e_5].$

Example 5.6.6. *For $n = 5$ note that $f_5 = 49 = 32 + 17 = l_4 + f_4$. We show the weight-4 vectors and the leading terms and their positions in Table 5.1 and 5.2, where* L.T *denotes the leading term and* Pos. *denotes the position. The* $2^{n-1} = 16$ positions 33 to 48 are excluded.

Table 5.1: Basis weight-4 vectors and leading terms for $C_2(\mathcal{G}_5)^{\perp}$

Weight-4 vector for n = 5	Leading Term L.T. of n = 5	Pos.
$u(0, e_1, e_3)$	$[0, e_1]$	1
$u(0, e_2, e_3)$	$[0, e_2]$	2
$u(e_1, e_1 + e_2, e_1 + e_3)$	$[e_1, e_1 + e_2]$	3
$u(e_2, e_2 + e_1, e_2 + e_3)$	$[e_2, e_1 + e_2]$	4
$u(0, e_3, e_4)$	$[0, e_3]$	5
$u(e_1, e_1 + e_3, e_1 + e_4)$	$[e_1, e_1 + e_3]$	6
$u(e_2, e_2 + e_3, e_2 + e_4)$	$[e_2, e_2 + e_3]$	7
$u(e_1 + e_2, e_1 + e_2 + e_3, e_1 + e_2 + e_4)$	$[e_1 + e_2, e_1 + e_2 + e_3]$	8
$u(e_3, e_1 + e_3, e_3 + e_4)$	$[e_3, e_1 + e_3]$	9
$u(e_3, e_2 + e_3, e_3 + e_4)$	$[e_3, e_2 + e_3]$	10
$u(e_1 + e_3, e_1 + e_2 + e_3, e_1 + e_3 + e_4)$	$[e_1 + e_3, e_1 + e_2 + e_3]$	11
$u(e_2 + e_3, e_1 + e_2 + e_3, e_2 + e_3 + e_4)$	$[e_2 + e_3, e_1 + e_2 + e_3]$	12
$u(0, e_4, e_5)$	$[0, e_4]$	13
$u(e_1, e_1 + e_4, e_1 + e_5)$	$[e_1, e_1 + e_4]$	14
$u(e_2, e_2 + e_4, e_2 + e_5)$	$[e_2, e_2 + e_4]$	15
$u(e_3, e_3 + e_4, e_3 + e_5)$	$[e_3, e_3 + e_4]$	16
$u(e_1 + e_2, e_1 + e_2 + e_4, e_1 + e_2 + e_5)$	$[e_1 + e_2, e_1 + e_2 + e_4]$	17
$u(e_1 + e_3, e_1 + e_3 + e_4, e_1 + e_3 + e_5)$	$[e_1 + e_3, e_1 + e_3 + e_4]$	18
$u(e_2 + e_3, e_2 + e_3 + e_4, u(e_2 + e_3 + e_5)$y	$[e_2 + e_3, e_2 + e_3 + e_4]$	19
$u(e_1 + e_2 + e_3, e_1 + e_2 + e_3 + e_4, e_1 + e_2 + e_3 + e_5)$	$[e_1 + e_2 + e_3, e_1 + e_2 + e_3 + e_4]$	20
$u(e_4, e_1 + e_4, e_4 + e_5)$	$[e_4, e_1 + e_4]$	21
$u(e_4, e_2 + e_4, e_4 + e_5)$	$[e_4, e_2 + e_4]$	22
$u(e_4, e_3 + e_4, e_4 + e_5)$	$[e_4, e_3 + e_4]$	23
$u(e_1 + e_4, e_1 + e_2 + e_4, e_1 + e_4 + e_5)$	$[e_1 + e_4, e_1 + e_2 + e_4]$	24
$u(e_1 + e_4, e_1 + e_3 + e_4, e_1 + e_4 + e_5)$	$[e_1 + e_4, e_1 + e_3 + e_4]$	25
$u(e_2 + e_4, e_1 + e_2 + e_4, e_2 + e_4 + e_5)$	$[e_2 + e_4, e_1 + e_2 + e_4]$	26
$u(e_2 + e_4, e_2 + e_3 + e_4, e_2 + e_4 + e_5)$	$[e_2 + e_4, e_2 + e_3 + e_4]$	27
$u(e_3 + e_4, e_1 + e_3 + e_4, e_3 + e_4 + e_5)$	$[e_3 + e_4, e_1 + e_3 + e_4]$	28
$u(e_3 + e_4, e_2 + e_3 + e_4, e_3 + e_4 + e_5)$	$[e_3 + e_4, e_2 + e_3 + e_4]$	29
$u(e_1 + e_2 + e_4, e_1 + e_2 + e_3 + e_4, e_1 + e_2 + e_4 + e_5)$	$[e_1 + e_2 + e_4, e_1 + e_2 + e_3 + e_4]$	30

53

Table 5.2: Basis weight-4 vectors and leading terms for $C_2(\mathcal{G}_5)^{\perp}$

Weight-4 vector for n = 5	Leading Term L.T. of n = 5	Pos.
$u(e_1 + e_3 + e_4, e_1 + e_2 + e_3 + e_4, e_1 + e_3 + e_4 + e_5)$	$[e_1 + e_3 + e_4, e_1 + e_2 + e_3 + e_4]$	31
$u(e_2 + e_3 + e_4, e_1 + e_2 + e_3 + e_4, e_2 + e_3 + e_4 + e_5)$	$[e_2 + e_3 + e_4, e_1 + e_2 + e_3 + e_4]$	32
$u(e_5, e_1 + e_5, e_4 + e_5)$	$[e_5, e_1 + e_5]$	49
$u(e_5, e_2 + e_5, e_4 + e_5)$	$[e_5, e_2 + e_5]$	50
$u(e_5, e_3 + e_5, e_4 + e_5)$	$[e_5, e_3 + e_5]$	51
$u(e_1 + e_5, e_1 + e_2 + e_5, e_1 + e_4 + e_5)$	$[e_1 + e_5, e_1 + e_2 + e_5]$	52
$u(e_1 + e_5, e_1 + e_4 + e_5, e_1 + e_3 + e_5)$	$[e_1 + e_5, e_1 + e_4 + e_5]$	53
$u(e_2 + e_5, e_1 + e_2 + e_5, e_2 + e_4 + e_5)$	$[e_2 + e_5, e_1 + e_2 + e_5]$	54
$u(e_2 + e_5, e_2 + e_4 + e_5, e_2 + e_3 + e_5)$	$[e_2 + e_5, e_2 + e_4 + e_5]$	55
$u(e_3 + e_5, e_1 + e_3 + e_5, e_3 + e_4 + e_5)$	$[e_3 + e_5, e_1 + e_3 + e_5]$	56
$u(e_3 + e_5, e_3 + e_4 + e_5, e_2 + e_3 + e_5)$	$[e_3 + e_5, e_3 + e_4 + e_5]$	57
$u(e_4 + e_5, e_1 + e_4 + e_5, e_3 + e_4 + e_5)$	$[e_4 + e_5, e_1 + e_4 + e_5]$	58
$u(e_4 + e_5, e_3 + e_4 + e_5, e_2 + e_4 + e_5)$	$[e_4 + e_5, e_3 + e_4 + e_5]$	59
$u(e_1 + e_2 + e_5, e_1 + e_2 + e_3 + e_5, e_1 + e_2 + e_4 + e_5)$	$[e_1 + e_2 + e_5, e_1 + e_2 + e_3 + e_5]$	60
$u(e_1 + e_3 + e_5, e_1 + e_2 + e_3 + e_5, e_1 + e_3 + e_4 + e_5)$	$[e_1 + e_3 + e_5, e_1 + e_2 + e_3 + e_5]$	61
$u(e_1 + e_4 + e_5, e_1 + e_2 + e_4 + e_5, e_1 + e_3 + e_4 + e_5)$	$[e_1 + e_4 + e_5, e_1 + e_2 + e_4 + e_5]$	62
$u(e_2 + e_3 + e_5, e_1 + e_2 + e_3 + e_5, e_2 + e_3 + e_4 + e_5)$	$[e_2 + e_3 + e_5, e_1 + e_2 + e_3 + e_5]$	63
$u(e_2 + e_4 + e_5, e_1 + e_2 + e_4 + e_5, e_2 + e_3 + e_4 + e_5)$	$[e_2 + e_4 + e_5, e_1 + e_2 + e_4 + e_5]$	64
$u(e_3 + e_4 + e_5, e_1 + e_3 + e_4 + e_5, e_2 + e_3 + e_4 + e_5)$	$[e_3 + e_4 + e_5, e_1 + e_3 + e_4 + e_5]$	65

The set of weight-4 vectors

$$\mathcal{W}_n = \bigcup_{i=2}^{n} u(x, x + e, x + e_i) = \mathcal{W}_{n-1} \cup \bigcup_{[x,x+e]\in\mathcal{P}_{n-1}} u(x, x + e, x + e_n),$$

have precisely the vectors in $\mathcal{C}_n$ as the right-most terms in the echelon array. If we are reading to the right, the ordering is according to that of the columns of G_n.

Lemma 5.6.7. [13, Lemma 16.] *For $n \geq 3$,*

(1) $\dim(C_2(\mathcal{G}_n) + C_2(\mathcal{G}_n)^{\perp}) \geq 2^{n-1}(n - 1) + 1$.
(2) $\dim(C_2(\mathcal{D}_n) + C_2(\mathcal{D}_n)^{\perp}) \geq 2^{n-1}(n - 1)$.

Proof. (1) The statement concern the achelon form from the code $C_2(\mathcal{G}_n)^{\perp}$ has been obtained in Proposition 5.6.5, we show that the first $2^{n-2}(n - 1)$ positions are all leading terms and that the middle Section of 2^{n-1} positions has no

54

leading terms. In a generating matrix for $C_2(\mathcal{G}_n) + C_2(\mathcal{G}_n)^\perp$, now, we reduce the first $2^{n-2}(n-1)$ position to 0, and obtained leading terms for all the next 2^{n-1} without disturbing the remaining leading terms for $C_2(\mathcal{G}_n)^\perp$. This provides $2^{n-1}(n-2)+1+2^{n-1} = 2^{n-1}(n-1)+1$ leading terms for $C_2(\mathcal{G}_n)+C_2(\mathcal{G}_n)^\perp$.

(2) For $C_2(\mathcal{D}_n) + C_2(\mathcal{D}_n)^\perp$, we use a similar argument that we have been used in (1), but for the form of the matrix A_n in Equation (5.3). We have the first $2^{n-2}n - 2^{n-2} = 2^{n-2}(n-1)$ leading terms from $C_2(\mathcal{D}_n)^\perp$, of $G_{n-1}^\perp$. Therefore, we have $2^{n-1}(n-2)+1+2^{n-1}-1 = 2^{n-1}(n-1)$ leading terms. $\square$

Corollary 5.6.8. [13, Corollary 17.] *For $n \geq 3$,*
(1) dim*(Hull$(\mathcal{G}_n)$) $= 2^{n-1} - 1$, dim(Hull$(\mathcal{D}_n)$) $= 2^{n-1}$
(2) Hull$(\mathcal{G}_n) \subset$ Hull$(\mathcal{D}_n)$.

Proof. (1) By Lemma 5.6.7, dim(Hull$(\mathcal{G}_n)$) $\leq 2^{n-1}$ and dim(Hull$(\mathcal{D}_n)$) $\leq 2^{n-1}-1$, and also by Proposition 5.6.4 dim(Hull$(\mathcal{G}_n)$) $\geq 2^{n-1}-1$ and dim(Hull$(\mathcal{D}_n)$) $\geq 2^{n-1}$. Therefore we have equality.
(2) Since the words v^R of Proposition 5.6.4 which span Hull$(\mathcal{G}_n)$ are in Hull$(\mathcal{D}_n)$, then we have inclusion. $\square$

Chapter 6

Concluding remarks

In this Chapter, we discuss the overall chapters of the thesis and give indication of future work.

In Chapter 3, we describe the generalized cube $H^k(n, 2)$ graph and its codes. The iterative construction of the $H^k(n, 2)$ graph has been described and we also present $H^1(4, 2)$. In Section 3.1, we describe the properties of $H^1(n, 2)$ and we show that its automorphism group is given by $S_2 \wr S_n$. Permutation decoding has been discussed.

In chapter 4 we describe the graph $H^1(n, 3)$ and its designs. Chapter 5 describes the binary codes from the line graph $L(H^1(n, 2))$ of the n-cube.

What is clear is that there is need to explore codes generated by adjacency matrices of higher cubes.

Bibliography

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

[2] I. Anderson, *A First Course in Combinatorial Mathematics*, Oxford University Press, 1989.

[3] R. F. Bailey (4MH) *Distance-transitive graph*, Department of Pure Mathematics University of Leeds Leeds, LS2 9JT May 10, 2002.

[4] E. P. Bautista, *Error Correcting Codes*, May 29, 2004.

[5] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language, *J. Symbolic Comput.*, 24(3-4) (1997), 235-265.

[6] A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-Regular Graphs*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Folge 3, Band 18. Berlin, New York: Springer-Verlag, 1989.

[7] J. Cannon, A. Steel, and G. White. *Linear codes over finite fields.* Department of Mathematics, University of Sydney, 2006. Vol 2.

[8] H.H. Cho, H.S. Shin and T.K. Yeo, Codes Automorphism Group Algorithm and Applications, *Comm. Korean Math. Soc. 11* (1996), no.3, $575 - 584$.

[9] D. Cries and B. Schneider, *A logical Approach to Discrete Math*, Springer, 1993, 436.

[10] W. Fish, J. Key, E. Mwambene, Graphs, designs and codes related to the n-cube, *Discrete Mathematics* 309 (2009) 3255-3269.

[11] W. Fish, J. Key, E. Mwambene Binary codes from designs from the reflexive n-cube, *Utilitas, to appear.*

[12] W. Fish, J. Key, E. Mwambene, Codes, designs and groups from the Hamming graphs, *Journal of Combinatorics, Information and System Sciences* (JCISS) on the theme "Combinatorics - A special issue dedicated to Ray-Chaudhuri for his 75th birthday", 34: 2009,169-182, .

[13] W. Fish, J. Key, E. Mwambene, Binary codes of line graphs of the n-cube, *Journal of Symbolic Computation*, 45, 2010, 800-812.

[14] W. Fish, J. D. Key, and E. Mwambene. Codes from the incidence matrices and line graphs of Hamming graphs, *Discrete Math.*, 310 2010, 1884-1897.

[15] J.I. Hall, *Notes on Coding Theory*. Department of Mathematics Michigan State University East Lansing, MI 48824, USA, 3 January 2003.

[16] F. Harary, The Automorphism Group of a Hypercube, *Journal of Universal Computer Science,* 6, no. 1 (2000), 136 − 138.

[17] W. C. Huffman. Codes and groups. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory,* pages 1345 − 1440. Amsterdam: Elsevier, 1998. Volume 2, Part 2, Chapter 17.

[18] J. D. Key and P. Seneviratne. Binary codes from rectangular lattice graphs and permutation decoding. *European J. Combin.*, 28 : 121126, 2006.

[19] J.D. Key, P. Seneviratne, Permutation decoding for binary self-dual codes from the graph Q_n where n is even, in: T. Shaska, W. C Huffman, D. Joyner, V. Ustimenko (Eds.), *Advances in Coding Theory and Cryptology*, in: Series on Coding Theory and Cryptology, vol. 2, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2007, pp. 152 − 159.

[20] J. D. Key, Designs, Codes and graphs from the Janko groups J_1 and J_2, *J. Combin. Math. and Combin. Comput.* 40, 2002, 143 − 159.

[21] J. D. Key, J. Moori, and B. G. Rodrigues. Permutation decoding of binary codes from graphs on triples. *Ars Combin.*, 91, 2009, 263 − 371.

[22] J. D. Key, J. Moori, and B. G. Rodrigues. Permutation decoding for binary codes from triangular graphs. *European J. Combin.*, 25, 2004, 113 − 123.

[23] J. D. Key and P. Seneviratne. Permutation decoding of binary codes from lattice graphs. *Discrete Math.* (Special issue dedicated to J. Seberry),2008, 223-231.

[24] F. J. MacWilliams. Permutation decoding of systematic codes. *Bell System Tech. J.*, 43, 485-505, 1964.

[25] F.J. MacWilliams and N.J. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[26] V. Pless, *Introduction to the Theory of Error-Correcting Codes*, John Wiley and Sons, Inc., New York, 1982.

[27] D. Reinhard (2005), *Graph Theory (3rd ed.)* Berlin, New York: Springer-Verlag.

[28] G. Sabidussi, Vertex-transitive graphs, Monatsh. *Math.*, 68 (1968), 426-438.

[29] G. Sierksma and H. Hoogeveen, Seven criteria for integer sequences being graphic, *Journal of Graph Theory, 15*: (1991), 223 - 231.

[30] J. van den Boomen. *The Matrix Tree Theorem*. Bachelor Thesis, Radboud Universiteit Nijmegen, 2007

[31] Washiela Fish. *Codes from uniform subset graphs and cyclic products.* PhD thesis, University of the Western Cape, 2007.

[32] H. Whitney. Congruent graphs and the connectivity of graphs. *Amer. J. Math.*, 54, 1932, 154-168.

[33] D. West (2001), *Introduction to Graph Theory*, Prentice-Hall, Upper Saddle River.

[34] H. Wilf (1989), *Combinatorial Algorithms An Update*, SIAM, Philadelphia.