Codes, graphs and designs from maximal subgroups of alternating groups

Nephtale B. Mumba

A thesis submitted in fulfilment of the requirements for the degree of **Doctor of Philosophy** in the Department of Mathematics and Applied Mathematics, University of the Western Cape.

Supervisor
Prof Eric Mwambene

Co-supervisors
Dr Washiela Fish
Prof Bernardo Rodrigues

July, 2018

Codes, graphs and designs from maximal subgroups of alternating groups

Nephtale B. Mumba

KEYWORDS

Alternating groups

Automorphism groups

Antipodal graphs

Bipartite graphs

Designs

Graphs

Graph covers

Incidence design

Linear code

Maximal subgroups

Neighbourhood design

Permutation decoding

PD-sets

Uniform subset graphs

Abstract

The main theme of this thesis is the construction of linear codes from adjacency matrices or sub-matrices of adjacency matrices of regular graphs. We first examine the binary codes from the row span of biadjacency matrices and their transposes for some classes of bipartite graphs. In this case we consider a sub-matrix of an adjacency matrix of a graph as the generator of the code.

We then shift our attention to uniform subset graphs by exploring the automorphism groups of graph covers and some classes of uniform subset graphs. In the sequel, we explore equal codes from adjacency matrices of non-isomorphic uniform subset graphs and finally consider codes generated by an adjacency matrix formed by adding adjacency matrices of two classes of uniform subset graphs.

We let $k \geq 3$ be an integer and Ω a set of size $2k$. Let $\Omega^{\{k\}}$ denote the set of all subsets of Ω of size k. We explore the pertinent properties of the bipartite graphs $\Gamma(2k, k, k+1, 1)$. Adjacency in these graphs is defined by two vertices as k-subsets and $(k+1)$-subsets of Ω being adjacent if and only if they have one element in common. Firstly, we examine the binary codes generated by the row span of biadjacency matrices of the graphs. We determine the parameters of the codes. We show that S_{2k} is contained in the automorphism group of both the graphs and the corresponding codes. In addition, we determine the duals of the codes, and by identifying suitable information sets, we construct 2-PD sets for the dual codes.

Secondly, we explore the properties of the bipartite graphs $\Gamma(2k+1, k, k+2, 1)$. We examine the codes generated by the row span of adjacency matrices and present the results as for the case of the graphs $\Gamma(2k, k, k+1, 1)$.

Thirdly, we explore automorphism groups of graph covers and some classes of uniform subset graphs. We extend the exploration of automorphism groups of distance-preserving graph covers. Specifically, we apply the technique of graph covers and their corresponding quotients to determine the automorphism groups of the uniform subset graphs $\Gamma(2k,k,k-1)$ and $\Gamma(2k,k,1)$. The determination of automorphism group of $\Gamma(2k,k,k-1)$ answers a conjecture posed by Mark Ramras and Elizabeth Donovan in [85]. They conjectured that $\text{Aut}(\Gamma(2k,k,k-1)) \cong S_{2k} \times < T >$, where T is the complementation map $X \mapsto T(X) = X^c = \{1,2,\ldots,2k\} \setminus X$, and $X \in \Omega^{\{k\}}$.

Fourthly, in the same enterprise, we also explore the binary codes from the row span of adjacency matrices of a class of uniform subset graphs. By analysing adjacency matrices of the non-isomorphic uniform subset graph $\Gamma(2k,k,1)$ and the Johnson graph $\Gamma(2k,k,k-1)$, we show that the codes coincide. We further extend our results analysing adjacency matrices of the non-isomorphic uniform subset graphs $\Gamma(2k,k,i)$ and $\Gamma(2k,k,k-i)$ for $i \neq 0, \frac{k}{2}$. We show that the codes generated by the row span of their adjacency matrices coincide.

The biadjacency matrices of the bipartite graphs $\Gamma(2k,k,k+1,1)$ and $\Gamma(2k+1,k,k+2,1)$ (at lower level) are sub-graphs of the uniform subset graph $\Gamma(2k,k,1)$ hence the codes from the row span of these biadjacency matrices are sub-codes of the codes from an adjacency matrix of $\Gamma(2k,k,1)$.

The code from the graph $\Gamma(2k,k,1)$ is also explored as a code from the maximal sub-groups of the alternating group A_{2k} hence the sub-codes in context are also the sub-codes from the maximal subgroups of the alternating group A_{2k}.

Finally, by using a different construction, we explore codes from an adjacency matrix of a generalised uniform subset graph $\Gamma(2k,k,\{1,k-1\})$. In this graph two vertices u and v as k-subsets of Ω are adjacent if and only if $|u \cap v| = i$ for $i \in \{1,k-1\}$.

Declaration

I declare that *Codes, graphs and designs from maximal subgroups of alternating groups* is my own work, that it has not been submitted 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 relevant and complete references.

Nephtale B. Mumba July, 2018

Signed: ....

List of symbols

Symbol	**Description**
A_n	alternating group on a set of n elements
C	linear code
$\mathrm{Aut}(C)$	automorphism group of a linear code C
$\mathcal{D}$	design
$\mathrm{Aut}(\mathcal{D})$	automorphism group of a design $\mathcal{D}$
$\mathrm{Aut}(\Gamma)$	automorphism group of a graph Γ
$A(\Gamma)$	antipodal graph of a graph Γ
$\mathcal{B}$	block set of a design
$C^{\perp}$	dual code of a code C
$\mathrm{d}(C)$	minimum distance of a code C
$\dim(C)$	dimension of of a code C
$d(x, y)$	Hamming distance between codewords x and y
$\mathbb{F}_q$	finite field of order q where $q = p^t$, p a prime
$\mathbb{F}_q^n$	vector space of n-tuples over $\mathbb{F}_q$
$\mathrm{Graph}(\Delta)$	orbital graph
Γ	graph
H	parity-check matrix of a code C
I_k	identity matrix of rank k
$\mathcal{I}$	incidence relation
$\mathcal{I}_n$	information set
$\cong$	isomorphism of two structures
$\jmath_n$	all-one vector of length n in a given code
$K_{m,n}$	complete bipartite graph with bipartition (X, Y)

M	generator matrix of a code
$N(v)$	open neighbourhood of a vertex v
$N[v]$	closed neighbourhood of a vertex v
Ω	a set of size n
$\Omega^{\{k\}}$	set of subsets of Ω of size k
$\Omega \setminus X$	elements of Ω not in X
$\mathcal{P}$	point set of a design
$\mathrm{Supp}(x)$	support of a vector x
S_n	symmetric group on a set of n elements
$\overline{v}$	block of $\mathcal{D}$ indexed by a vertex v of a graph Γ
$v^{\overline{v}}$	incidence vector of $\overline{v}$
$\mathrm{wt}(x)$	Hamming weight of a vector x

Acknowledgement

I am deeply indebted to

- God for the good health and well-being that were necessary to complete the thesis, let alone the research.

- My three supervisors: Prof Eric Mwambene, Dr Washiela Fish and Prof Bernardo Rodrigues, for the assiduous continuous support of my PhD study and related research, for their patience, motivation, and immense knowledge. They took time and effort necessary to provide insightful guidance and directions throughout the research: it helped me to learn the ropes. You definitely provided me with the tools that I needed to choose the right direction and successfully complete my research and thesis. It has been a period of intense learning for me, not only in the scientific arena, but also on a personal level.

- The support of my family members: my sister Miriam Mumba and my cousin Mickson Mbewe. Words cannot express my gratitude towards you all. Each one of you, inimitable. It is impossible to thank you enough for your unflinching support and constant encouragement.

- Friends who lightened the stress with the many moments we shared, in person and online. Thanks a lot to Mr and Mrs Banda, Loveness Nogwe, Ben Mdala, Godfrey Banda, and to everybody in the mathematics postgraduate laboratory at the University of the Western Cape.

- The support of my employers, Mzuzu University. In particular, I acknowledge the role played by the Dean of the faculty of Education, Prof Golden Msilimba, the Head of Department (Mathematics) Mr Paul

Kubwalo at the time of my departure, the Head of Department (Mathematics) during the period of my studies Dr Khumbo Kumwenda, and the entire Mathematics Department.

- The joint postgraduate scholarship I received from the African Institute for Mathematical Sciences(AIMS) and the University of the Western Cape. To this end, I acknowledge the vital role played by Prof Eric Mwambene in facilitating the scholarship.

- The Head of Department (Mathematics and Applied Mathematics), University of the Western Cape, during the period of my studies, Prof David Holgate, in facilitating the scholarship and the support I got from the department during the whole period of study.

To my late **Mum** and late **Dad**.

Contents

Chapter 1

Introduction

Significant effort with considerable success has been directed towards the description of linear codes from neighbourhood and incidence designs of various classes of regular graphs. A neighbourhood design of a regular graph is formed by taking as points the vertices of the graph, and each block consists of the neighbours of a given vertex. In an incidence design, the points are the edges of the graph and each block consists of the edges incident with a given vertex. In most cases, these codes have been decoded using permutation decoding, a method due to MacWilliams [77]. This is because combinatorial properties of the graphs and designs are intimately linked to important properties of the codes including the minimum weight, the minimum words, information sets and the automorphism groups which are amenable for successful permutation decoding.

In recent studies on codes from incidence matrices of some classes of graphs, (see for example [35], [37], [38], [60] and [73] for further details) it was shown that these codes have some useful common properties. Among others, it is shown that the minimum weight coincides with the valency of the graph and the minimum words are the non-zero scalar multiples of the rows of the incidence matrix. This implies that in these cases the graphs can be retrieved from the code. However, codes from adjacency matrices of graphs seem not to enjoy such properties in the general case (see [11], [30], [48], [57] and [59] for further details). What may seem to be a recurring feature is that many such codes inherit the automorphism group of the graph and that they are amenable to permutation decoding. A question that seems plausible to investigate is whether or not the codes generated by biadjacency matrices of the particular class of bipartite graphs that we consider in this thesis inherit any properties. We give an affirmative answer to this question and show that the minimum words of the codes in question are the rows of the biadjacency matrices. The codes also allow for partial permutation decoding.

In [36] codes from incidence matrices of some classes of bipartite graphs $\Gamma(n, k, l, i)$ are considered. In this thesis, using the construction method given in [36], we examine the codes defined by some classes of bipartite graphs. However, unlike in [36], instead of the full adjacency matrix of the graph as the generator of the code, we look at the biadjacency matrix. As far as we are aware, this is the first time that codes generated by the rows of biadjacency matrices of bipartite graphs are considered.

We start by considering some specific properties of the bipartite graphs $\Gamma(2k, k, k+1, 1)$ followed by the construction of codes from the row span of the biadjacency matrices. In particular, we consider biadjacency matrices of order $\binom{2k}{k} \times \binom{2k}{k+1}$ and $\binom{2k}{k+1} \times \binom{2k}{k}$. These biadjacency matrices can also be viewed as incidence matrices of the 1-$(\binom{2k}{k+1}, k, k+1)$ and 1-$(\binom{2k}{k}, k+1, k)$-designs respectively, in which the blocks are the $\Omega^{\{k\}}$ vertices and the points the $\Omega^{\{k+1\}}$ vertices of the graph and vice-versa. We determine a basis and the minimum weight for the codes and their duals. In the case of the codes, we show that they are generated by minimum weight codewords.

Similarly, specific properties of the bipartite graphs $\Gamma(2k+1, k, k+2, 1)$ are explored. This is followed by the construction of binary codes from the row span of biadjacency matrices of these graphs. In particular, we consider biadjacency matrices of order $\binom{2k+1}{k} \times \binom{2k+1}{k+2}$ and $\binom{2k+1}{k+2} \times \binom{2k+1}{k}$. Again biadjacency matrices can be viewed as incidence matrices of the 1-$(\binom{2k+1}{k+2}, k, k+2)$ and 1-$(\binom{2k+1}{k}, k+2, k)$-designs respectively where for a set Ω of size $2k+1$, the blocks are indexed by the k-subsets of Ω and the points by the $(k+2)$-subsets in the first case, and vice-versa in the second. We determine the dimension and the minimum weight of the codes and their duals. In the case of both the codes and their duals, we show that they are generated by minimum weight codewords.

Let Ω be a non-empty set and S_Ω denote the set of permutations of the set Ω. If $\Omega = \{1, 2, \ldots, n\}, S_\Omega$ is written S_n. Chen and Lih [15] introduced uniform subset graphs. Let n, k be positive integers such that $n \geq 2k$, and r a non-negative integer with $r < k$. The uniform subset graph denoted $\Gamma(n, k, r)$, is defined as the graph whose vertex-set is $\Omega^{\{k\}}$, the set of all the k-subsets of Ω with adjacency defined by any two k-subsets meeting in r elements of Ω, where $0 \leq r \leq k-1$. Since S_n is k-transitive for all $k \leq n$ and preserves the size of intersection sets, it is easy to see that uniform subset graphs are vertex-transitive.

However, it is surprisingly difficult to determine their full automorphism groups. Amongst the many classes of uniform subset graphs it has only been determined that $\text{Aut}(\Gamma(2k+1, k, 0))$, the automorphism group of the so called Odd graphs, is S_{2k+1}, and more recently, Ramras and Donovan [85] proved that $\text{Aut}(\Gamma(n, k, k-1)), n \neq 2k$ coincides with S_n. Further, they conjectured that $\text{Aut}(\Gamma(2k, k, k-1)) \cong S_{2k} \times < T >$, where T is the complementation map $X \mapsto T(X) = X^c = \{1, 2, \ldots, 2k\} \setminus X$, and $X \in \Omega^{\{k\}}$.

As part and parcel of determining salient properties of the graph $\Gamma(2k, k, 1)$, we consider the automorphism group of the graphs $\Gamma(2k, k, 1$ and $\Gamma(2k, k, k-1)$.

In order to determine the automorphism groups of the graphs in question, we employ the strategy of Hofmeister [51]. He determines the automorphism group of a graph cover by first looking at the quotient (folded) graph. The key observation in analysing the automorphism group of the cover is in understanding the interplay between automorphisms of the cover and their corresponding quotient. We determine the automorphism groups of the uniform subset graphs $\Gamma(2k, k, 1)$ and $\Gamma(2k, k, k-1)$ and show that $\text{Aut}(\Gamma(2k, k, k-1)) = \text{Aut}(\Gamma(2k, k, 1)) \cong S_{2k} \times S_2$.

Determining codes generated by the row span of adjacency matrices of graphs has been a fruitful enterprise (see [28, 29, 30, 33, 34, 47, 48, 58] for further details). Many of the codes generated by strongly regular graphs have been amenable to decoding (see [45, 57, 63, 73] for further details). In some cases, relatively small PD sets have been obtained (see [45, 63] for further details).

One would expect that non-isomorphic graphs would always generate non-isomorphic codes, considering that an adjacency matrix of a graph describes the graph up to isomorphism. It is surprising that that is not the case. By determining a basis for the binary code generated by the row span of an adjacency matrix of $\Gamma(2k, k, 1)$, we show that the code coincides with that generated by an adjacency matrix of the Johnson graph $\Gamma(2k, k, k-1)$. We then show that adjacency matrices of $\Gamma(2k, k, 1)$ and $\Gamma(2k, k, k-1)$ are equivalent and hence the codes from their row span coincide. We further prove for the general case that the codes generated by an adjacency matrix of $\Gamma(2k, k, i)$ and $\Gamma(2k, k, k-i)$ for $i \neq 0, \frac{k}{2}$, coincide, despite the graphs being non-isomorphic.

In another context, $\Gamma(2k, k, 1)$ can be described as a graph obtained by the method of Key and Moori [61, Proposition 1]. In that context, the group is S_{2k}, and G_α is the maximal subgroup $S_k \times A_k$. In view of the symmetries involved, it was anticipated that the codes would be amenable to permutation decoding.

The biadjacency matrices of the bipartite graphs $\Gamma(2k, k, k+1, 1)$ and $\Gamma(2k+1, k, k+2, 1)$ (at lower level) are identified as sub-graphs of the uniform subset graph $\Gamma(2k, k, 1)$. Because of this relationship, before we explore the codes from $\Gamma(2k, k, 1)$ we deal with the codes from the sub-graphs which are the sub-codes of the code from $\Gamma(2k, k, 1)$. It follows immediately that the codes from biadjacency matrices of the bipartite graphs $\Gamma(2k, k, k+1, 1)$ and $\Gamma(2k+1, k, k+2, 1)$ (at a lower level) are sub-codes of the code from the maximal subgroup of alternating group A_{2k}.

Codes obtained from permutation representation of finite groups have been given particular attention by some authors (see [61], [62], [86] for further details).

The primitive action of the simple alternating group $A_{2k},\ k \geq 2$, provides an alternative perspective on the construction of graphs, designs and codes from the maximal groups.

The stabilizer of $X \in \Omega^{\{k\}}$ in the action of a group H on $\Omega^{\{k\}}$, is the set-wise stabilizer H_X in the action of H on Ω. We denote the point-wise stabilizer by $H_{X'}$. It is clear that $H_{X'} \leq H_X$. The permutation representation of H_X with respect to its action on X defines a homomorphism of H_X into the symmetric group $S_X \cong S_k$ which has as its kernel $H_{X'}$, and hence the factor group $H_X/H_{X'}$ is isomorphic to a subgroup of S_k. Since the action of any odd permutation in S_{2k} on a k-subset can be mimicked by a permutation in A_{2k}, the orbits of $(S_{2k})_X$ and $(A_{2k})_X$ are identical. Hence it is sufficient to consider the stabilizer in A_{2k}, rather than in S_{2k} which is a larger group.

The rank of $\Omega^{\{k\}}$ is the number of orbits of H_X, for any $X \in \Omega^{\{k\}}$.The primitive action of A_{2k} on $\Omega^{\{k\}}$ is transitive. The stabilizer of a point denoted by $(A_{2k})_X$, for $X \in \Omega^{\{k\}}$, in the action of A_{2k} on $\Omega^{\{k\}}$ is maximal.

In studies done on codes from adjacency matrices A of classes of graphs or from $A + aI + bJ$ where I and J are the identity and all-one matrices respectively and a, b are integers (see [11], [30], [48], [59] and [57] for further details), it is shown that the codes do not seem to have any uniform properties as regards their dimension, minimum weight or minimum words.

In this thesis, we also focus on codes from the row span of an adjacency matrix $A = A_1 + A_2$ of a graph $\Gamma(2k, k, i), i \in \{1, k-1\}$, where A_1 is an adjacency matrix of the Johnson graph $\Gamma(2k, k, k-1)$ and A_2 one of $\Gamma(2k, k, 1)$. We determine a basis for the new code and we also determine its minimum weight and show that it is equal to twice the minimum weight of the code generated by an adjacency matrix of $\Gamma(2k, k, k-1)$ in all the cases. The results obtained are interesting as they show that we can combine graphs to produce a graph that generates a code that has double the minimum weight of the original code while maintaining its length with half or less the size of the basis.

1.1 Outline of the thesis

We begin by presenting preliminaries related to codes, graphs and designs in Chapter 2. The material is standard: however, to aid the discussion, we have given a lot of results in terms of theorems, lemmas, and propositions.

In Chapter 3, we start by considering some specific properties of the bipartite graphs $\Gamma(2k, k, k+1, 1)$, followed by the construction of codes from the row span of the biadjacency matrices. The specific properties of the graphs are proved. We examine further the codes constructed from biadjacency matrices of these graphs. More attention is given to determining the parameters of the codes and a basis for the codes. We also consider permutation decoding. Complete proofs are given for the new results presented.

In Chapter 4, we start by considering some specific properties of the bipartite graphs $\Gamma(2k+1, k, k+2, 1)$, followed by the construction of binary codes from the row span of their biadjacency matrices. We complete the rest of the results following the same pattern and arguments used in Chapter 3.

In Chapter 5, we explore the automorphism groups of graph covers and uniform subset graphs $\Gamma(2k, k, k-1)$ and $\Gamma(2k, k, 1)$. This answers the conjecture posed by Ramras and Donovan in [85]. In order to determine the automorphism groups of the graphs in question, we employ the Hofmeister [51] strategy. He determines the automorphism group of graph cover by first looking at the quotient (folded) graph. The key observation in analysing the automorphism group of the cover is in understanding the interplay between automorphisms of the cover and their corresponding quotient.

In Chapter 6, we argue through a series of results, that non-isomorphic graphs may generate equal codes. We first determine some pertinent properties of the graphs $\Gamma(2k, k, i), i = 1, k-1$. In turn, we focus on the binary codes generated by adjacency matrices of $\Gamma(2k, k, 1)$ and $\Gamma(2k, k, k-1)$ and show that they are equal. In general, we show that binary codes generated by adjacency matrices of $\Gamma(2k, k, i)$ and $\Gamma(2k, k, k-i)$ for $i \neq 0, \frac{k}{2}$, coincide, in spite of the fact that the graphs are non-isomorphic.

Finally in Chapter 7, we focus on codes from the row span of an adjacency matrix $A = A_1 + A_2$ of a graph $\Gamma(2k, k, i), i \in \{1, k-1\}$, where A_1 is an adjacency matrix of the Johnson graph $\Gamma(2k, k, k-1)$ and A_2 is an adjacency matrix of $\Gamma(2k, k, 1)$. The codes have interesting properties and parameters.

The thesis ends with a conclusion in Chapter 8, where a synopsis of the whole thesis has been considered and the highlight is a statement of open problems or further related work.

1.2 Papers from this thesis

The following papers were prepared from the work presented in this thesis.

1. N. B. Mumba, E. Mwambene, Automorphism groups of graph covers and uniform subset graphs, *AKCE Int. J. Graphs Comb.*, (2018).

2. W. Fish, N. B. Mumba, E. Mwambene and B. G. Rodrigues, Binary codes and partial permutation decoding sets from biadjacency matrices of the bipartite graphs $\Gamma(2k+1, k, k+2, 1)$, *Graphs Combin.*, **33** (2017), 357–368.

3. W. Fish, N. B. Mumba, E. Mwambene and B. G. Rodrigues, Binary codes and partial permutation decoding sets from biadjacency matrices of the bipartite graphs $\Gamma(2k, k, k+1, 1)$. *In preparation.*

4. W. Fish, N. B. Mumba, E. Mwambene and B. G. Rodrigues, Equality of codes in the face of non-isomorphism in uniform subset graphs. *Submitted.*

5. W. Fish, N. B. Mumba, E. Mwambene and B. G. Rodrigues, Codes from generalised uniform subset graphs $\Gamma(2k, k, i)$ for $i \in \{1, k-1\}$. In preparation.

Chapter 2

Preliminaries

In this chapter we present terminology, notation and an overview of known results related to graphs, designs and codes which are needed later in the thesis for reference purposes. For more detailed and additional information the reader may consult [7, 9, 13, 18, 23, 43, 44, 52, 57, 59, 63, 64, 67, 70, 77, 78, 93] and [96].

2.1 Graphs

In this section we introduce some general notions about graphs.

Definition 2.1. A *graph* is a pair $\Gamma = (V, E)$ of sets such that $E \subseteq V^{\{2\}}$, i.e. elements of E are subsets of V of size 2. V is the vertex-set of Γ and E is its edge-set.

If $e = \{u, v\} \in E(\Gamma)$ then u and v are *adjacent.* Two vertices which are incident with a common edge are adjacent, as are two edges which are incident with a common vertex. Two distinct adjacent vertices are said to be *neighbours.* The set of neighbours of a vertex v in Γ is denoted $N_\Gamma(v)$.

Definition 2.2. Let Γ be a graph. The *degree* or *valency* of a vertex is the number of edges incident with it. If all the vertices of Γ are incident with the same number of edges, then Γ is *regular*, and its valency is the valency of each vertex.

A graph Γ is *strongly regular* with parameters (n, k, λ, μ) if it has n vertices, its valency is k, any two adjacent vertices are commonly adjacent to λ vertices, and any two non-adjacent vertices are commonly adjacent to μ vertices.

Definition 2.3. A *walk* in a graph is a sequence $v_0, v_1, \ldots, v_k$ of vertices such that $\{v_{i-1}, v_i\}$ is an edge for $1 \leq i \leq k$; k is the length of the walk. A walk is called a *trail* if all the edges appearing in it are distinct. It is closed if $v_0 = v_k$. If all its vertices are distinct then a walk is called a *path*.

A graph is *connected* if there is a path joining every pair of vertices. A *cycle* is a closed trail with no repeated vertices other than the starting and ending vertices. By an n-cycle is meant a cycle containing n vertices. A *Hamiltonian cycle* is a cycle that goes through every vertex exactly once. A *Hamiltonian graph* is a graph with a Hamiltonian cycle. An *Euler tour* in a graph is a closed walk which traverses every edge exactly once. A graph is *Eulerian* if it admits an Euler tour.

A *subgraph* $\Gamma' = (V', E')$ of $\Gamma = (V, E)$ is a graph with $V' \subseteq V$ and $E' \subseteq E$.

Let Ω be a non-empty set. A complete graph K_Ω is a graph on Ω in which every pair of distinct vertices is adjacent. If $\Omega = \{1, \ldots, n\}$ then K_Ω is denoted K_n. A graph with n vertices has at most $\binom{n}{2}$ edges, the number of edges of K_n. A complete subgraph of a given graph is called a *clique*. The complement $\overline{\Gamma}$ of a given graph $\Gamma = (V, E)$ is the graph on V such that two vertices are adjacent if and only if they are not adjacent in Γ.

Definition 2.4. Let Γ be a graph. Then Γ is t-connected if and only if a minimum number of t vertices need to be removed from Γ to result in a disconnected graph or a trivial graph.

Definition 2.5. In a connected graph, the *distance* between any two vertices u, v denoted $d(u, v)$, is the number of edges in a shortest path connecting them.

The notion of distance allows us to define the eccentricity of a vertex, the diameter of a graph and whether a graph is distance-regular. These will be used in discussing our results in the chapters that follows.

Definition 2.6. Let Γ be a graph. Then the *eccentricity* of a vertex u in Γ, denoted $\epsilon(u)$, is defined by

$$\epsilon(u) := \max_{v \in V(\Gamma)} d(u, v).$$

Definition 2.7. Let Γ be a graph. Then the *diameter* of Γ, denoted $\mathrm{diam}(\Gamma)$, is defined by

$$\mathrm{diam}(\Gamma) := \max_{v \in V(\Gamma)} \epsilon(v).$$

Definition 2.8. A graph is *distance-regular* if for any two vertices u and v such that $d(u, v) = i$, the number of vertices w such that $d(u, w) = j$ and $d(w, v) = k$, is independent of u and v.

The following are well-known results which give the relationship between the degrees of the vertices of a graph and the number of its edges.

Theorem 2.9. [9, Theorem 1.1] *The sum of the degrees of all the vertices of a graph is equal to twice the number of edges of the graph.*

Corollary 2.10. [96, Corollary 1.3.6] *A graph with n vertices and valency k has $\dfrac{nk}{2}$ edges.*

2.1.1 Graph homomorphisms

Graph homomorphisms are used to characterise graphs. A *homomorphism* from Γ_1 to Γ_2 is a mapping $\alpha : V(\Gamma_1) \to V(\Gamma_2)$ such that $\{u, v\} \in E(\Gamma_1)$ implies that $\{\alpha(u), \alpha(v)\} \in E(\Gamma_2)$. If α is injective then it is an *embedding.*

Definition 2.11. Let $\Gamma_1 = (V_1, E_1)$ and $\Gamma_2 = (V_2, E_2)$. Then Γ_1 and Γ_2 are isomorphic if there exists a bijection $\alpha : V_1 \to V_2$ such that for all $u, v \in V_1$, $\{u, v\} \in E_1$ if and only if $\{\alpha(u), \alpha(v)\} \in E_2$. We call the mapping α an isomorphism. If Γ_1 and Γ_2 are isomorphic, it is denoted $\Gamma_1 \cong \Gamma_2$, otherwise it is written $\Gamma_1 \ncong \Gamma_2$.

Two graphs Γ_1 and Γ_2 are edge-isomorphic if there exists a bijection σ between their edge-sets that preserves adjacency of edges, i.e $\sigma : E(\Gamma_1) \to E(\Gamma_2)$ is an edge-isomorphism if edges e and f are adjacent in Γ_1 if and only if

$\sigma(e)$ and $\sigma(f)$ are adjacent in Γ_2. Since every edge is defined by two vertices, an isomorphism between two graphs induces an edge-isomorphism. However, the existence of an edge-isomorphism σ does not imply the existence of an isomorphism α from Γ_1 to Γ_2 that induces σ. Whitney [97] proved that, with only four exceptions, edge isomorphisms between finite connected graphs are induced by graph isomorphisms. Exceptional cases have been illustrated by Hemminger [49]. We now state Whitney's [97] result as deduced from Hemminger [49].

Theorem 2.12. [49, Theorem 1] *Let Γ_1 and Γ_2 be connected graphs. Let α be a one-to-one function from the edge-set of Γ_1 into the edge-set of Γ_2. Then α is induced by an isomorphism of Γ_1 onto Γ_2 if and only if α and α^{-1} preserve stars.*

We now deal with the concept of an automorphism of a graph.

Definition 2.13. Let Γ be a graph. Then an *automorphism* α of Γ is a permutation of the vertices such that $\{u, v\} \in E(\Gamma)$ if and only if $\{\alpha(u), \alpha(v)\} \in E(\Gamma)$. The set of automorphisms of Γ, denoted $\mathrm{Aut}(\Gamma)$, forms a group under composition.

An automorphism of Γ is thus a permutation on its vertices which preserves its edges. Hence $\mathrm{Aut}(\Gamma)$ is a subgroup of the symmetric group of all the permutations of the vertex set $V(\Gamma)$.

A stronger property which involves the automorphism group of a graph is that of distance-transitivity, which is defined as follows.

Definition 2.14. Let Γ be a graph. Then Γ is *distance-transitive* if and only if for any vertices s, t, u, v such that $d(s, t) = d(u, v)$, there exists $\sigma \in \mathrm{Aut}(\Gamma)$ such $\sigma(s) = u$ and $\sigma(t) = v$.

Edge- and vertex-transitivity are defined analogously, and are implied by distance-transitivity.

At the core of the construction in this thesis are two matrices associated with graphs. These matrices provide the link between graphs, designs and codes.

Definition 2.15. Let Γ be a graph with n vertices, m edges. An *incidence matrix* A of Γ is an $n \times m$ matrix $A = [a_{ij}]$ whose n rows correspond to the n vertices and m columns to the m edges such that;

$$a_{ij} \quad = \quad \begin{cases} 1 & \text{if the } i^{th} \text{ vertex is incident with the } j^{th} \text{ edge } m_j; \\ 0 & \text{otherwise.} \end{cases}$$

It is also called a *vertex-edge incidence matrix.*

Definition 2.16. Let Γ be a graph with n vertices. The *adjacency matrix* B of Γ is an $n \times n$ matrix $B = [b_{ij}]$ whose (i, j) entry is given by:

$$b_{ij} \quad = \quad \begin{cases} 1 & \text{if the } i^{th} \text{ vertex is connected to the } j^{th} \text{ vertex;} \\ 0 & \text{otherwise.} \end{cases}$$

Note that an adjacency matrix is symmetric.

These matrices can be used to generated codes. In this thesis, we use adjacency matrices and in other cases sub-matrices of adjacency matrices in the generation of the codes.

2.1.2 Bipartite graphs

We also consider codes from some classes of bipartite graphs in this thesis. The codes considered are generated by the row span of part of the adjacency matrix (biadjacency matrix) of the graph.

A graph $\Gamma = (V, E)$ is *bipartite* if V can be partitioned into two non-empty sets X and Y such that each edge $e = \{x, y\}$ of Γ has the property that $e \cap X$ and $e \cap Y$ are non-empty. The pair (X, Y) is a bipartition of the graph. A bipartite graph with bipartition (X, Y) is denoted $\Gamma(X, Y)$.

Definition 2.17. Let n, k, l be positive integers and i a non-negative integer. Let $n \geq k, l$ and $k, l \geq i$. Define a *bipartite graph* $\Gamma(n, k, l, i)$ by

$$\begin{aligned} V(\Gamma(n, k, l, i)) &= \Omega^{\{k\}} \dot{\cup} \Omega^{\{l\}}; \\ \{x, y\} \in E(\Gamma(n, k, l, i)) &\iff |x \cap y| = i, \ \textit{where} \ \ x \in \Omega^{\{k\}}, y \in \Omega^{\{l\}}. \end{aligned} \tag{2.1}$$

If each vertex $x \in \Omega^{\{k\}}$ is adjacent to all vertices of $\Omega^{\{l\}}$ then $\Gamma(n, k, l, i)$ is a *complete bipartite graph.* A complete bipartite graph $\Gamma(X, Y)$ such that $|X| = m$ and $|Y| = n$ is denoted $K_{m,n}$. The graph $K_{1,n}$ is called a star.

Some of the properties of bipartite graphs are that a connected bipartite graph has a unique bipartition and a bipartite graph without isolated vertices and with t connected components has 2^{t-1} bipartitions (see also [3]).

It is easy to show that even cycles are also bipartite, but that odd cycles are not. In fact, this observation, slightly generalized, forms the criterion for a graph to be bipartite.

Proposition 2.18. [3],[23, Proposition 1.6.1] *A graph is bipartite if and only if it has no odd cycle.*

A similar argument gives the following corollary.

Corollary 2.19. [3, Corollary 2.1.4] *A connected graph Γ is bipartite if and only if for very vertex v there is no edge $\{x, y\}$ with $d(v, x) = d(v, y)$.*

There are many characterisations of bipartite graphs, and therefore many algorithmic ways to recognise them. Corollary 2.19 gives rise to one such algorithm: choose a vertex $v \in V(\Gamma)$ and consider the level representation of Γ with respect to v. If each $N_\Gamma(v)$ spans no edges then Γ is bipartite, otherwise Γ is not bipartite. The following is a variation of Theorem 2.18.

Corollary 2.20. [3, Corollary 2.1.5] *A graph Γ is bipartite if and only if it contains no closed walk of odd length.*

Proof. Since an odd cycle is also an odd walk the condition is certainly sufficient. Thus it suffices to show that a bipartite graph contains no closed walk of odd length. Let Γ be bipartite and $W = v_0v_1v_2 \cdots v_kv_0$ be a closed walk in Γ. Consider the level representation of Γ with respect to v_0. We define the sequence $\alpha_1, \alpha_2, \ldots, \alpha_{k+1}$ by

$$\alpha_i = \begin{cases} 1 & \text{if } 1 \leq i \leq k \text{ and the level of } v_{i-1} \text{ is less than the level of } v_i; \\ 0 & \text{otherwise.} \end{cases}$$

Then, since W is closed, the sequence must contain equal numbers of 1's and 0's, and hence must be of even length. Therefore, W is also of even length. □

Obviously, a graph could yield several different adjacency matrices if the vertices are arranged in different orders, but there are a few common configurations worth mentioning. The adjacency matrix of a bipartite graph is conveniently represented with each partition ordered consecutively so that it forms a block matrix defined by the partition. An adjacency matrix A of a bipartite graph whose partitions have p and q vertices could be expressed as

$$A = \begin{pmatrix} \mathbf{0}_{p\times p} & B \\ B^T & \mathbf{0}_{q\times q} \end{pmatrix},$$

where B is a $p \times q$ matrix and $\mathbf{0}$ represents the zero matrix. The sub-matrix B is called a *biadjacency matrix*. In our consideration, for a bipartite graph $\Gamma(n, k, l, i)$, when we speak of a biadjacency matrix B we mean that we have chosen a sub-matrix with the rows indexed by $\Omega^{\{k\}}$ and the columns by $\Omega^{\{l\}}$.

Let n, k, l be positive integers and i a non-negative integer. Let $n \geq k, l$ and $k, l \geq i$. The bipartite graph $\Gamma(n, k, l, i)$ has $\binom{n}{k} + \binom{n}{l}$ vertices. The degree of each vertex in $\Omega^{\{k\}}$ is $\binom{k}{i}\binom{n-k}{l-i}$ and that in $\Omega^{\{l\}}$ is $\binom{l}{i}\binom{n-l}{k-i}$. The graph has $\binom{n}{k}\binom{k}{i}\binom{n-k}{l-i}$ edges.

Lemma 2.21 states whether given bipartite graphs are isomorphic.

Proposition 2.21. [36, Lemma 4.1, p. 1826] *For $n > k, \Gamma(n, k, l, i) \cong \Gamma(n, n-k, l, l-i)$.*

Proof. The congruence comes from the correspondence $u \mapsto u^c$ (the complement of u in Ω) for $u \in \Omega^{\{k\}}$, and $v \mapsto v$ for $v \in \Omega^{\{l\}}$, since $\{u, v\}$ is an edge in $\Gamma(n, k, l, i)$ if and only if $\{u^c, v\}$ is an edge in $\Gamma(n, n-k, l, l-i)$. □

2.1.3 Uniform subset graphs

In this section we will give a brief account of uniform subset graphs as it appears in the literature. Some of their fundamental properties will also be described. Finally, their relationship to vertex-transitive graphs in general will be explored.

We first define generalised uniform subset graph.

Definition 2.22. Let n, k be positive integers, $I \subseteq \{0, 1, 2, \ldots, k-1\}$ such that $n \geq 2k$. Let $\Omega = \{1, 2, \ldots, n\}$ and $\Omega^{\{k\}}$ the set of all k-subsets of Ω. A *generalised uniform subset graph* $\Gamma(n,k,I)$ is defined by

$$\begin{aligned} V(\Gamma(n,k,I)) &= \Omega^{\{k\}}; \\ \{x,y\} \in E(\Gamma(n,k,I)) &\iff |x \cap y| \in I, \ \textit{where } x,y \in \Omega^{\{k\}}. \end{aligned}$$

We now define uniform subset graphs.

Definition 2.23. Let n,k be positive integers such that $n \geq 2k$, and i a non-negative integer with $i < k$. Let $\Omega = \{1,2,\ldots,n\}$ and $\Omega^{\{k\}}$ the set of all k-subsets of Ω. A *uniform subset graph* $\Gamma(n,k,i)$ is defined by

$$\begin{aligned} V(\Gamma(n,k,i)) &= \Omega^{\{k\}}; \\ \{x,y\} \in E(\Gamma(n,k,i)) &\iff |x \cap y| = i, \ \textit{where } x,y \in \Omega^{\{k\}}. \end{aligned}$$

The uniform subset graphs constitute a large class of graphs. Some of the well-known uniform subset graphs are the class $\Gamma(n,k,k-1)$ known as the *Johnson graphs,* of which the class $\Gamma(n,2,1)$ known as the *Triangular graphs* is a subclass. The other class that has featured prominently is $\Gamma(n,k,0)$ known as the *Kneser graphs.* The subclass of Kneser graphs $\Gamma(2k+1,k,0)$ is the so called *Odd graphs.*

Lemma 2.24 states whether given uniform subset graphs are isomorphic.

Proposition 2.24. [28, Lemma 4.1.1] *For* $n \geq k \geq i, \Gamma(n,k,i) \cong \Gamma(n,n-k,n-2k+i)$.

Proof. For $u \in \Omega^{\{k\}}$, define a function $f : \Omega^{\{k\}} \to \Omega^{\{n-k\}}$ by

$$f(u) = \Omega \setminus u.$$

If $[u,v]$ is an edge in $\Gamma(n,k,i)$ then $|u \cap v| = i$ by definition, and so

$$\begin{aligned} |f(u) \cap f(v)| &= |(\Omega \setminus u) \cap (\Omega \setminus v)| \\ &= |\Omega \setminus (u \cup v)| \\ &= n - |u \cup v| \\ &= n - (2k - i) \\ &= n - 2k + i. \end{aligned}$$

Hence $[f(u), f(v)]$ is an edge in $\Gamma(n,n-k,n-2k+i)$, and since f is clearly a bijection, the result follows. □

We now give some basic properties of uniform subset graphs.

Proposition 2.25. [28, Proposition 4.1.1] *For $n \geq k \geq i$, the following hold for $\Gamma(n,k,i)$.*

(a) *$\Gamma(n,k,i)$ has $\binom{n}{k}$ vertices.*

(b) *$\Gamma(n,k,i)$ is regular and each vertex has valency $\binom{k}{i}\binom{n-k}{k-i}$.*

(c) *$\Gamma(n,k,i)$ is not strongly regular.*

Proof. (a) The number of vertices of $\Gamma(n,k,i)$ is just the number of k-subsets of $\Omega = \{1,2,3,\dots,n\}$ of which there are $\binom{n}{k}$.

(b) Suppose that u is a vertex of $\Gamma(n,k,i)$. Any vertex v adjacent to u consists of any i of the k elements of u, as well as any $k-i$ elements of $\Omega \setminus u$. Hence u has valency $\binom{k}{i}\binom{n-k}{k-i}$.

(c) Suppose that $u = \{x_1, x_2, x_3, \dots, x_i, x_{i+1}, \dots, x_k\}$ and $v = \{x_1, x_2, x_3, \dots, x_i, x_{k+1}, \dots, x_{2k-i}\}$ are vertices of $\Gamma(n,k,i)$ having i elements in common. Then u and v are adjacent, and any vertex commonly adjacent to u and v consists either of $\{x_1, x_2, x_3, \dots, x_i\}$ and $k-i$ elements of $\Omega \setminus (u \cup v)$, or of $i-1$ elements of $\{x_1, x_2, x_3, \dots, x_i\}$, one each of $\{x_{i+1}, x_{i+2}, \dots, x_k\}$ and $\{x_{k+1}, x_{k+2}, \dots, x_{2k-i}\}$ and $k-i$ elements of $\Omega \setminus (u \cup v)$, or $i-2$ elements of $\{x_1, x_2, x_3, \dots, x_i\}$, and so on. Hence u and v are commonly adjacent to $\sum_{j=0}^{i}\binom{i}{i-j}\binom{k-i}{j}^2\binom{n-2k+i}{k-i-j}$ vertices. However, if any two vertices u and v are not adjacent and $i \neq 0$ nor 1, then u and v are commonly adjacent to $\binom{k}{i}^2\binom{n-2k}{k-2i}$ vertices if $|u \cap v| = 0$, and to $\binom{k-1}{i-1}^2\binom{n-2k+1}{k-2i+1} + \binom{k-1}{i}^2\binom{n-2k+1}{k-2i}$ vertices if $|u \cap v| = 1$. Hence $\Gamma(n,k,i)$ is not strongly regular.

□

Proposition 2.26. [28, Proposition 4.2.3] *For $n \geq k \geq i$, $\Gamma(n,k,i)$ is distance-transitive.*

From 2.26, it follows that uniform subset graphs are vertex- and edge-transitive.

The next property deals with the connectivity of $\Gamma(n,k,i)$.

Proposition 2.27. [28, Proposition 4.2.5] *For $n \geq k \geq i$, $\Gamma(n,k,i)$ is $\binom{k}{i}\binom{n-k}{k-i}$-connected.*

Lemma 2.28 and Theorem 2.29 below expresses a direct relationship between the maximum distance between any two vertices and the size of their intersection. This consequently determines the eccentricities of the vertices and the diameters of some classes of uniform subset graphs.

Lemma 2.28. [17, Lemma 3] *Let k, i be positive integers with $k > i$ and $n = 2k - i$. Let $\mathcal{V}$ denote the set of all the pairs (u, v) with $u, v \in V(\Gamma(n,k,i))$ and $|u \cap v| = x > i$. Then*

$$d(u,v) = \min\left\{2\left\lceil\frac{k-x}{i}\right\rceil, 2\left\lceil\frac{x-i}{i}\right\rceil + 1\right\}. \tag{2.2}$$

Theorem 2.29. [17, Theorem 5] *Let k, i be positive integers with $k > i$ and $n = 2k - i$. Then*

$$\operatorname{diam}(\Gamma(n,k,i)) = \left\lceil\frac{k-1}{i}\right\rceil. \tag{2.3}$$

2.2 Designs

This section is devoted to a summary of basic results and concepts from the theory of designs. These can be found in [4].

We discuss basic concepts from design theory needed in our development of the use of linear codes as an aid in classifying designs. We restrict our attention to finite structures.Thus whenever a set, group or other mathematical structure is mentioned the reader should assume it to be finite.

The most basic structure of the theory is a *finite incidence structure* which we denote by $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, and which consists of two disjoint finite sets $\mathcal{P}$ and $\mathcal{B}$, and subset $\mathcal{I}$ of $\mathcal{P} \times \mathcal{B}$. The members of $\mathcal{P}$ are called *points* and are generally denoted by lower-case Roman letters; the members of $\mathcal{B}$ are called *blocks* and are generally denoted by upper-case Roman letters. If the ordered pair (p, B) is in $\mathcal{I}$ we say that p is incident with B or that B contains the point p, or that p is on B. The pair (p, B) is called a *flag* if it is in $\mathcal{I}$, and an *anti-flag* if it is not.

We consider incidence structures with a particular degree of regularity. If the degree of regularity is emphasized, we call these t-designs.

Definition 2.30. An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is a t-(v, k, λ) design, or simply a t-design, where t, v, k and λ are non-negative integers, if:

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

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

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

We speak of a t-design provided that $|B|$, the cardinality of a subset B of $\mathcal{P}$, is k for every subset $B \in \mathcal{B}$ and that for every subset T of $\mathcal{P}$ of cardinality t, $|\{B \in \mathcal{B} \mid B \supseteq T\}| = \lambda$. Thus the blocks all have the same cardinality and every t-subset (i.e a subset of cardinality t) is contained in the same number of blocks.

The non-negative integers t, v, k and λ are referred to as the parameters of the design and we will sometimes refer to a t-(v, k, λ) design as "the design with parameters t-(v, k, λ)".

Various conditions are usually included to the definition to exclude degenerate cases. We assume that $\mathcal{P}$ and $\mathcal{B}$ are non-empty and $v \geq k \geq t$ (so $\lambda > 0$). A t-design with $\lambda = 1$ is called a *Steiner system.* The conditions of a design imply that each point is contained in the same number of blocks. Suppose that $t < k < v - t$. Then there is a t-(v, k, λ) structure for some λ, in which not every set of k points is incident with a block.

Theorem 2.31. [8, Theorem 3.2.2] *A t-design $\mathcal{D}$ is also an s-design, for $1 \leq s \leq t$. If the given design has parameters t-(v, k, λ) then its parameters as an s-design are s-(v, k, λ_s) where*

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

Definition 2.32. A 2-(v, k, λ) design is called a *symmetric design* if the number of blocks is the same as the the number of points.

A t-(v, k, λ) design is said to be *trivial* if every set of k points is incident with a block in which case the block set $\mathcal{B}$ has $\binom{v}{k}$ elements. Distinct blocks are said to be *repeated* if they are incident with the same set of points.

In this thesis we are dealing with non-trivial simple designs that do not have *repeated blocks.*

Proposition 2.33. [4, Proposition 4.2.1] *If $\mathcal{D}$ is a t-(v, k, λ) design with $t \geq 3$ and with equally many points and blocks, then $\mathcal{D}$ is trivial.*

Theorem 2.34. [4, Proposition 4.2.1] *For a block design $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ each element of $\mathcal{P}$ occurs in exactly r blocks (the so called replication number) where*

$$r(k-1) = \lambda(v-1) \quad \textit{and} \quad bk = vr.$$

Definition 2.35. Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ and $\mathcal{D}' = (\mathcal{P}', \mathcal{B}', \mathcal{I}')$ be incidence structures and let α be a bijection from $\mathcal{P} \cup \mathcal{B}$ to $\mathcal{P}' \cup \mathcal{B}'$. We say that α is an isomorphism from $\mathcal{D}$ to $\mathcal{D}'$ if $\alpha(\mathcal{P}) = \mathcal{P}'$ and $\alpha(\mathcal{B}) = \mathcal{B}'$ with $(p, B) \in \mathcal{I}$ if and only if $(\alpha(p), \alpha(B)) \in \mathcal{I}'$. It is an automorphism if $\mathcal{D} = \mathcal{D}'$.

Definition 2.36. Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be an incidence structure with $|\mathcal{P}| = v$ and $|\mathcal{B}| = b$. Let the points be labelled $\mathcal{P} = \{p_1, p_2, \ldots, p_v\}$ and the blocks $\mathcal{B} = \{B_1, B_2, \ldots, B_b\}$. An *incidence matrix* for $\mathcal{D}$ is the $b \times v$ matrix $A = [a_{ij}]$ of 0's and 1's such that

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

For a block $B_i \in \mathcal{B}$, its characteristic function is the vector

$$v^{B_i} = \sum_{(p, B_i) \in \mathcal{I}} v^{\{p\}},$$

where $v^{\{p\}}$ is a vector $(v_1, \ldots, v_p, \ldots, v_n)$ with $v_p = 1$ and $v_i = 0$ for all $i \neq p$. The vector v^{B_i} will be called the *incidence vector* of the block B_i. In our construction, the incidence vectors are essentially the rows of the incidence matrices.

A *neighbourhood design* $\mathcal{D}(\Gamma)$ of a regular graph Γ with n vertices and valency r is the 1-(n, r, r) symmetric design formed by taking the points to be the vertices of Γ and each block consists of the neighbours of a given vertex.

Incidence matrices of the neighbourhood designs are also adjacency matrices of the graphs and the incidence vectors are rows of the matrices.

In an incidence design, the points are the edges of the graph and each block consists of the edges incident with a given vertex.

2.3 Codes

For primes p, a p-ary $[n,k,d]_p$ *linear code* C is a k-dimensional subspace of $\mathbb{F}_p^n$, the vector space of n-tuples over $\mathbb{F}_p$. If D is another code such that $D \subseteq C$, then D is called a sub-code of C. The elements of C are called *codewords* . The $\boldsymbol{j}$-vector is the codeword consisting of 1's in all its coordinate positions. The *support* of a codeword $c \in C$, denoted Supp(c), is the set of coordinate positions i such that c_i is non-zero. The *Hamming distance* between two codewords 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 an alphabet F. The minimum distance of a code C, denoted $\mathrm{d}(C)$, is the minimum of the distances between any two distinct codewords in C. The *Hamming weight* of a codeword $c \in C$, denoted $\mathrm{wt}(c)$, is defined as the number of its non-zero coordinate positions. Hence $\mathrm{wt}(c) = |\mathrm{Supp}(c)|$. The *minimum weight* of a code C, denoted $\mathrm{wt}(C)$, is defined as the smallest of the Hamming weights of the non-zero codewords in C. A binary code is called *doubly-even* if the Hamming weight of each codeword is divisible by 4.

The relationship between the minimum weight and the minimum distance of a linear code is stated in Theorem 2.37 below.

Theorem 2.37. [75, Theorem 4.38] *Let C be a linear code over $\mathbb{F}_q$. Then* $\mathrm{d}(C) = \mathrm{wt}(C)$.

Properties of a linear code are best described by its generator and parity check matrices. A *generator matrix* of a linear code C is a matrix whose rows form a basis for the code. The *dual* of C is the set $C^\perp$ of all vectors $v \in \mathbb{F}_p^n$ such that $(v,c) = 0$ for all codewords $c \in C$ where $(\cdot,\cdot)$ denotes the standard inner product in $\mathbb{F}_p^n$. A *check matrix* for C is a generator matrix H for $C^\perp$; the *syndrome* of a vector $y \in \mathbb{F}^n$ is Hy^T. C is *self-orthogonal* if $C \subseteq C^\perp$, and *self-dual* if $C = C^\perp$. The *hull* of C, denoted Hull(C), is the subspace $C \cap C^\perp$ of $\mathbb{F}_q^n$. The $\boldsymbol{j}$-vector plays a role in determining the relationship between codes and their duals.

2.3.1 Error-detection and error-correction in codes

We formalise the meaning of an error-detecting and an error-correcting code, and we shall see the connection between the distance and the error detection and correction capabilities of the code.

Definition 2.38. Let $s \in \mathbb{Z}^+$. A code C is s-error-detecting if whenever at least one but at most s errors are made in any codeword, then the resulting word is not a codeword. A code C is exactly s-error-detecting if it is s-error-detecting but not $(s+1)$-error-detecting.

From this definition and that of the distance of a code, it is clear that a code of distance d can detect up to $d-1$ errors. A more important definition for us is that of an error-correcting code.

Definition 2.39. Let $t \in \mathbb{Z}^+$. A code C is said is to be exactly t-error-correcting if it is t-error-correcting but not $(t+1)$-error-correcting.

To help understand Definition 2.39, suppose a codeword v is transmitted and at most t errors are made. That is, we have that at most t components of the codeword are changed, resulting in a word w. If the code is t-error-correcting, and since w is a distance of at most t from v, then the distance from w to any other codeword is greater than t. Therefore, v is the closest codeword to w. We would correct w to v, and thus recover the correct codeword.

We now show the relation between the distance and the error-correcting capability of a code. This is stated in Theorem 2.40 below.

Theorem 2.40. [75, Theorem 2.5.10] *Let C be a code with minimum distance d. Then C is t-error-correcting for $t = \lfloor (d-1)/2 \rfloor$ but is not $(t+1)$-error-correcting.*

Two codes are isomorphic if the one can be obtained from the other by permuting the coordinate positions. An automorphism of C is an isomorphism of C onto itself. The permutation automorphism group of a linear code C of length n, denoted $\mathrm{Aut}(C)$, is a set of coordinate permutations $\sigma \in S_n$ that map C to itself. Any code is isomorphic to a code with generator matrix in standard form, i.e. the form $[I_k|A]$; a check matrix is then given by $[-A^T|I_{n-k}]$. The first k coordinates in the standard form represent information positions and the last $n-k$ coordinates form check positions . The identification of a basis for a code C implies the identification of a set of information positions for C since the coordinates and the basis words can be arranged so that a matrix of the form $[I_k|A]$ results.

The choice of information positions plays a crucial role in permutation decoding. This, in turn, entails the determination of a set of automorphisms of the code which may exploit the full error-correcting capability of the code. Permutation decoding uses a subset $\mathcal{S}$ of $\mathrm{Aut}(C)$, called a PD-set . For a t-error-correcting-code, $\mathcal{S}$ should have the property that any set of t coordinate positions is mapped by at least one member of $\mathcal{S}$ into the check positions. Permutation decoding was first introduced by MacWilliams in [77]. See also [52] for an updated account on the topic. Among others, it has been used to decode codes from various classes of graphs (see [35], [57], [59] and [71]). An algorithm for permutation decoding is given in [52]. The minimum size of $\mathcal{S}$ is given by Gordon in [45] and it states as follows:

Theorem 2.41. [52, Theorem 10.2.2, p. 404], [45] *If $\mathcal{S}$ is a PD-set for a t-error-correcting $[n,k,d]_p$ code C then*

$$|\mathcal{S}| \geq \left\lceil \frac{n}{n-k} \left\lceil \frac{n-1}{n-k-1} \left\lceil \cdots \left\lceil \frac{n-t+1}{n-k-t+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil . \tag{2.4}$$

PD-sets that exploit the full error-correcting capability of the code may not even exist, and hence partial PD-sets may be resorted to. An s-**PD-set** for a t-error-correcting code maps any set of $s \leq t$ coordinate positions into the check positions (see [28] and [30]).

2.4 Codes from designs

Codes constructed from designs have enriched the theory of designs in that new designs have been constructed and existing designs have been extended in some cases. Certain designs have been shown not to exist at all. It has been shown that not all codes yield designs [4].

The code $C_{\mathbb{F}}$ of the design $\mathcal{D}$ over the finite field $\mathbb{F}$ is the space spanned by the incidence vectors of the blocks over $\mathbb{F}$. If we take $\mathbb{F}$ to be the prime field $\mathbb{F}_p = G\mathbb{F}(p)$, we write C_p for $C_{\mathbb{F}}$, and refer to the dimension of C_p as the p-**rank** of $\mathcal{D}$. The point-set of $\mathcal{D}$ is denoted by $\mathcal{P}$ and the block set by $\mathcal{B}$. If $\mathcal{Q}$ is any subset of $\mathcal{P}$, then we will denote the incidence vector of $\mathcal{Q}$ by $v^{\mathcal{Q}}$. Thus $C_{\mathbb{F}} = \langle v^B | B \in \mathcal{B} \rangle$ is a subspace of $\mathbb{F}^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to $\mathbb{F}$. The length of the code is the cardinality of $\mathcal{P}$ and its dimension is the rank of the incidence matrix of the design $\mathcal{D}$.

2.5 Codes from graphs

An alternative method of constructing codes that have a rich structure and in most cases elucidate symmetry are codes from graphs with a high degree of regularity. In [20] it is shown how a binary code can be obtained directly from the edge-graph of the icosahedron. Through the construction of codes done in [20], we immediately get a natural basis for the code and also a simple description of all the codewords. It is also noted that this is a special case of a general method of constructing codes from graphs. It is demonstrated how a certain technique applied to adjacency matrices of graphs yields many interesting linear codes. The method is presented over an arbitrary finite field, although it is perhaps over the field of order 2 that the construction has its most natural geometric interpretation.

The incidence vector of a block $\overline{u}$ corresponding to a vertex u of a graph is a vector

$$v^{\overline{u}} = \sum_{w \in N(u)} v^w$$

where v^w is the standard vector in $\mathbb{F}_q^n$ with entry 1 in the w-indexed coordinate position. The vector $v^{\overline{u}}$ is the row of the adjacency matrix of the graph Γ indexed by u.

For any prime p, the p-ary linear code $C_p(A)$ is the span over $\mathbb{F}_p$ of the rows of an adjacency matrix, A, of the graph Γ. Thus

$$C_p(A) = \langle v^{\overline{u}} | u \in V(\Gamma) \rangle.$$

$C_p(A)$ has length n, the number of vertices of the graph. Its dimension is the rank of A over $\mathbb{F}_p$.

Similar constructions to those done in [11], [30], [48], [59] and [57] have been carried out in this thesis, and we dwell much on the concept of constructing codes from an adjacency matrix and also in some cases from a sub-matrix of an adjacency matrix.

2.5.1 Codes from adjacency matrices of uniform subset graphs $\Gamma(n, k, i)$

For the construction of the codes from the row span of an adjacency matrix of a uniform subset graph $\Gamma(n, k, i)$, consider its adjacency matrix as an incidence matrix of the 1-design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$. We take $\mathcal{P} = \Omega^{\{k\}}$ as the point set. Each $X \in \Omega^{\{k\}}$ has a block $\overline{X}$ corresponding to it. The block is defined by

$$\overline{X} = N(X) = \{Y \in \Omega^{\{k\}} : |Y \cap X| = i\}.$$

The block set $\mathcal{B}$ is given by

$$\mathcal{B} = \{\overline{X} : X \in \Omega^{\{k\}}\},$$

and the incidence vector of the block $\overline{X}$ by

$$v^{\overline{X}} = \sum_{|Y \cap X| = i} v^Y. \tag{2.5}$$

2.5.2 Codes from biadjacency matrices of bipartite graphs $\Gamma(n, k, l, i)$

For the construction of the codes from the row span of a biadjacency matrix of a bipartite graph $\Gamma(n, k, l, i)$, consider its biadjacency matrix as an incidence matrix of a design. We take $\mathcal{P} = \Omega^{\{l\}}$ as the point set of the 1-design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ in which each point $X \in \Omega^{\{k\}}$ has a block $\overline{X}$ corresponding to it. The block is defined by

$$\overline{X} = N(X) = \{Y \in \Omega^{\{l\}} : |Y \cap X| = i\}.$$

The block set $\mathcal{B}$ is defined by

$$\mathcal{B} = \{\overline{X} : X \in \Omega^{\{k\}}\}.$$

The incidence vector associated with $\overline{X}$ is defined by

$$v^{\overline{X}} = \sum_{|Y \cap X| = i} v^{Y}. \tag{2.6}$$

2.6 Transitivity, blocks and primitivity

The action of the alternating group A_n on k subsets of Ω is both transitive and primitive. Moreover, it is k-transitive. We now present these concepts so as to fix notation and usage of vocabulary. The concepts are found in [24],[79] and [98].

If G is a group acting on a set Ω and k is an integer with $1 \leq k \leq |\Omega|$, then we say G is k-transitive if G is transitive on $\Omega^{\{k\}}$, the set of all the k-subsets of Ω.

We now extend the action of a group G on Ω to subsets of Ω by denoting $B^x = \{\beta^x | \beta \in G\}$ for each $B \subseteq \Omega$. A non-empty subset Δ of Ω is called a *block* for G if for each $x \in G$ either $\Delta^x = \Delta$ or $\Delta^x \cap \Delta = \emptyset$. Every group acting on Ω has Ω and the singletons $\{\alpha\}, \alpha \in \Omega$, as blocks. These blocks are called trivial blocks, otherwise any other blocks are called non-trivial.

We give the following definitions.

Definition 2.42. Let G act transitively on a set Ω. We say that the group is *primitive* if G has no non-trivial block on Ω. Otherwise G is *imprimitive.*

Definition 2.43. Let H be a subgroup of G. H is called a *maximal subgroup* if there is no subgroup K with $H < K < G$.

We now introduce a very important theorem. This theorem gives a link between the transitive primitive action of a group and its maximal subgroups. More precisely we have the following proposition.

Proposition 2.44. [98, Proposition 2.1] *Suppose that the group G acts transitively on the set Ω, and let H be the stabiliser of $\alpha \in \Omega$. Then G acts primitively on Ω if and only if H is a maximal subgroup of G.*

The *rank* of a transitive permutation group G on Ω is the number of orbits of G in its action on $\Omega \times \Omega$. This is equal to the number of orbits of G_α on Ω, for $\alpha \in G$.

2.7 The O'Nan-Scott theorem

This section is most important for the description of the maximal subgroups we are dealing with as we are considering the primitive action of A_{2k} on $\Omega^{\{k\}}$.

The O'Nan-Scott theorem classifies the maximal subgroups of the alternating and symmetric groups. It says that every maximal subgroup of S_n or A_n is of a certain type. It does not state exactly what the maximal subgroups are, but it does provide the first step towards writing down the list of maximal subgroups of A_n or S_n for any particular reasonable value of n. The theorem is given by Wilson in [98].

Theorem 2.45. [98, Theorem 2.4] *If H is any proper subgroup of S_n other than A_n, then H is a subgroup of one or more of the following subgroups:*

(i) *an intransitive group $S_k \times S_m$, where $n = k + m$;*

(ii) *an imprimitive group $S_k \wr S_m$, where $n = km$;*

(iii) *a primitive wreath product, $S_k \wr S_m$, where $n = k^m$;*

(iv) *an affine group $AGL_d(p) \cong p^d : GL_d(p)$, where $n = p^d$;*

(v) *a group of shape $T^m.(Aut(T) \times S_m)$, where T is a non-abelian simple group, acting on the cosets of a subgroup $Aut(T) \times S_m$, where $n = |T|^{m-1}$;*

(vi) *an almost simple group acting on the cosets of a maximal subgroup of index n.*

2.8 Construction of 1-designs and codes from maximal subgroups

The method described here gives us the procedure for the construction of codes and designs defined by the primitive action of a group on a set of specified size. Our construction follows the same procedure by changing the sizes of the Ω and n in the classes of alternating groups we are considering.

Our construction for the symmetric 1-designs is based on the following results, mainly Theorem 2.46 below, which is a proposition by Key and Moori [61] with its corrected version in [62].

Theorem 2.46. [61, Proposition 1] *Let G be a finite primitive permutation group acting on the set Ω of size n. Let $\alpha \in \Omega$, and let $\Delta \neq \{\alpha\}$ be an orbit of the stabiliser G_α of α. If*

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

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

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

then $\mathcal{D} = (\Omega, \mathcal{B})$ forms a 1-$(n, |\Delta|, |\Delta|)$ *design with n blocks. Further, if Δ is a self-paired orbit of G_α, then $\Gamma = (\Omega, \varepsilon)$ is a regular connected graph of valency $|\Delta|, \mathcal{D}$ is self-dual, and G acts as an automorphism group on each of these structures, primitive on vertices of the graph, and on points and blocks of the design.*

Proof. The proof can be found in [62]. □

Lemma 2.47. [61, Lemma 2] *If the group G acts primitively on the points and the blocks of a symmetric 1-design $\mathcal{D}$, then the design can be obtained by orbiting a union of orbits of a point-stabilizer, as described in* Theorem 2.46.

Proof. The proof can be found in [62]. □

Lemma 2.48. *If G is a primitive simple group acting on Ω, then for any $\alpha \in \Omega$, the point stabilizer G_α has only one orbit of length 1.*

Proof. The proof can be found in [62]. □

Chapter 3

Codes and partial permutation decoding sets from biadjacency matrices of the bipartite graphs $\Gamma(2k, k, k+1, 1)$

3.1 Introduction

The code generated by biadjacency matrices of the bipartite graphs $\Gamma(2k, k, k+1, 1)$ and that generated by biadjacency matrices of the bipartite graphs $\Gamma(2k+1, k, k+2, 1)$ (at a lower level) are sub-codes of the code generated by an adjacency matrix of the uniform subset graph $\Gamma(2k, k, 1)$ which is the content of Chapter 6.

This chapter, therefore, considers codes generated by biadjacency matrices of the bipartite graphs $\Gamma(2k, k, k+1, 1)$. To facilitate such an enterprise, we first look at pertinent properties of the graph $\Gamma(2k, k, k+1, 1)$.

Succinctly, the main theme of this chapter is summarised in Theorem 3.1. Throughout this chapter it is assumed that $k \geq 3$ and Ω is a set of size $2k$, unless otherwise stated.

Theorem 3.1. *Let $C_B(\Gamma(2k, k, k+1, 1))$ denote the binary code from the row span of a $\binom{2k}{k} \times \binom{2k}{k+1}$ biadjacency matrix B of the bipartite graph $\Gamma(2k, k, k+1, 1)$ and $C_B(\Gamma(2k, k, k+1, 1))^{\perp}$ its dual. Then*

(a) *The code* $C_B(\Gamma(2k, k, k+1, 1))$ *is a* $[\binom{2k}{k+1}, \binom{2k-1}{k-1}, k]_2$*-code. Its dual* $C_B^{\perp}(\Gamma(2k, k, k+1, 1))$ *is the code from a* $\binom{2k}{k-2} \times \binom{2k}{k+1}$ *biadjacency matrix of the bipartite graph* $\Gamma(2k, k-2, k+1, 0)$ *and is a* $[\binom{2k}{k+1}, \binom{2k-1}{k-2}, k+2]_2$*-code.*

(b) *The code* $C_B(\Gamma(2k, k+1, k, 1))$ *is a* $[\binom{2k}{k}, \binom{2k-1}{k}, k+1]_2$*-code. Its dual* $C_B^{\perp}(\Gamma(2k, k+1, k, 1))$ *is the code from a* $\binom{2k}{k-1} \times \binom{2k}{k}$ *biadjacency matrix of the bipartite graph* $\Gamma(2k, k-1, k, 0)$ *and is a* $[\binom{2k}{k}, \binom{2k-1}{k-1}, k+1]_2$*-code.*

(c) $S_{2k} \cong$ *(a subgroup of)* $\mathrm{Aut}(\Gamma(2k, k, k+1, 1))$ *and* $S_{2k} \cong$ *(a subgroup of)* $\mathrm{Aut}(C_B(\Gamma(2k, k, k+1, 1)))$.

(d) $\mathcal{S} = \{1_{S_{2k}}\} \cup \{(1, j) : 1 < j \leq 2k\}$ *is a 2-PD-set for the dual code* $C_B(\Gamma(2k, k, k+1, 1))^{\perp}$.

Note that $C_B(\Gamma(2k, k+1, k, 1))$ is the row span of B^T for $C_B(\Gamma(2k, k, k+1, 1))$ and since $\mathrm{rank}_2(B) = \mathrm{rank}_2(B^T)$, the dimensions of the codes are equal as given by $\binom{2k-1}{k}$ and $\binom{2k-1}{k-1}$.

This chapter is organised as follows: In Section 3.2, we describe some basic properties and automorphism groups for the bipartite graphs $\Gamma(2k, k, k+1, 1)$. In Section 3.3, the main parameters of the binary code from the rows of the biadjacency matrix of the bipartite graphs $\Gamma(2k, k, k+1, 1)$ are determined. Finally, in Section 3.4, we give partial permutation decoding sets for the dual of the code under consideration.

Let $\boldsymbol{C_B(\Gamma(n, m, l, i))}$ denote the binary code from the row span of a $\binom{n}{m} \times \binom{n}{l}$ biadjacency matrix B of the bipartite graph $\Gamma(n, m, l, i)$ and $\boldsymbol{C_B(\Gamma(n, m, l, i))^{\perp}}$ its dual.

3.2 The bipartite graphs $\Gamma(2k, k, k+1, 1)$

We start with the following remark which is a direct implication from [36, Lemma 4.1, p. 1826].

Remark 3.2. $C_B(\Gamma(2k, k, k+1, 1)) \cong C_B(\Gamma(2k, k, k-1, 0))$ since by [36, Lemma 4.1, p. 1826] $\Gamma(2k, k, k+1, 1) \cong \Gamma(2k, k, k-1, 0)$.

We will first discuss the direct relationship between the distance between any two vertices and the size of their intersection as subsets of Ω. This will consequently determine the eccentricities of the vertices and the diameters of the graphs that we are examining.

Proposition 3.3. *Let u, v, x and y be distinct vertices of the bipartite graph $\Gamma(2k, k, k+1, 1)$ such that $u, v \in \Omega^{\{k\}}$ and $x, y \in \Omega^{\{k+1\}}$.*

(a) *For $0 \leq m \leq k-1$, $d(u,x) = 2m+1$ if and only if $|u \cap x| = m+1$.*

(b) *For $0 \leq m \leq k$, $d(u,v) = 2m$ if and only if $|u \cap v| = k-m$.*

(c) *For $0 \leq m \leq k-1$, $d(x,y) = 2m$ if and only if $|x \cap y| = k+1-m$.*

(d) *The diameter of the graph is $2k$.*

Proof. We proceed by induction on m in all three cases (a), (b) and (c) simultaneously with base $m = 0$.

(a) If $d(u,x) = 1$, by definition we have $|u \cap x| = 1$. Conversely, if $|u \cap x| = 1$ then $d(u,x) = 1$.

(b) If $d(u,v) = 0$, we have $|u \cap v| = k$. Conversely, if $|u \cap v| = k$ then $u = v$, and hence $d(u,v) = 0$.

(c) If $d(x,y) = 0$, we have $|x \cap y| = k+1$. Conversely, if $|x \cap y| = k+1$ then $x = y$, and hence $d(x,y) = 0$.

Suppose the statement holds for $m = r$. We need to show that in (a), (b) and (c) it also holds for $m = r+1$.

(a) We need to show that $d(u,x) = 2(r+1)+1 = 2r+3$ implies $|u \cap x| = r+2$. Let $d(u,x) = 2r+3$. Then there exists a path of length $2r+3$ from u to x. Let $uu_1u_2 \cdots u_{2r}u_{2r+1}u_{2r+2}x$ be such a path. Then since it is given that $|u \cap u_{2r}| = k-r, |u_{2r} \cap x| = 2, |u| = k, |u_{2r}| = k, |x| = k+1, |u \cup u_{2r} \cup x| = 2k-1$ and $|u \cap u_{2r} \cap x| = 0, 1,$ or 2.

We use the inclusion-exclusion principle and the three possibilities for $|u \cap u_{2r} \cap x|$.

When $|u \cap u_{2r} \cap x| = 0$ we get $|u \cap x| = r$, and this is a contradiction since that case does not arise. When $|u \cap u_{2r} \cap x| = 1$, we get $|u \cap x| = r+1$, and this is a contradiction according to the induction hypothesis. When $|u \cap u_{2r} \cap x| = 2$, we get $|u \cap x| = r+2$, and the result follows by induction.

Conversely, if $|u \cap x| = r+2$, we need to show that $d(u, x) = 2r+3$. Choose a vertex w which is on a path from u to x such that $d(w, x) = 3$. This implies that $|w \cap x| = 2$.

By the inclusion-exclusion principle we get $|u \cap w| = k - r$, and by the induction hypothesis, $d(u, w) = 2r$. This shows that $d(u, x) = d(u, w) + d(w, x) = 2r + 3$ as required.

(b) We need to show that $d(u, v) = 2(r+1) = 2r+2$ implies $|u \cap v| = k - (r+1)$. Let $d(u, v) = 2r+2$, it follows that there exists a path of length $2r+2$ from u to v. Let the path be $uu_1u_2 \cdots u_{2r}u_{2r+1}v$.

It is given that $|u \cap u_{2r+1}| = r+1, |u_{2r+1} \cap v| = 1, |u| = k, |u_{2r+1}| = k+1, |v| = k, u \cup u_{2r+1} \cup v = \Omega$ and $|u \cap u_{2r+1} \cap v| = 0$ or 1.

We use the inclusion-exclusion principle and the two possibilities for $|u \cap u_{2r+1} \cap v|$.

When $|u \cap u_{2r+1} \cap v| = 1$ we get $|u \cap v| = k - r$, and this is a contradiction according to the induction hypothesis. When $|u \cap u_{2r+1} \cap v| = 0$, we get $|u \cap v| = k - (r+1)$, and the result follows by induction.

Conversely, if $|u \cap v| = k - (r+1)$, we need to show that $d(u, v) = 2r+2$. Choose a vertex w which is on a path from u to v such that $d(w, v) = 1$. This implies that $|w \cap v| = 1$.

By the inclusion-exclusion principle, we get $|u \cap v| = r+1$, and by the induction hypothesis, $d(u, w) = 2r+1$. This shows that $d(u, v) = d(u, w) + d(w, v) = 2r+2$ as required.

(c) We need to show that $d(x, y) = 2(r+1) = 2r+2$ implies $|x \cap y| = k+1-(r+1) = k-r$. Let $d(x, y) = 2r+2$. It follows that there exists a path of length $2r+2$ from x to y. Let the path be $xx_1x_2 \cdots x_{2r}x_{2r+1}y$.

It is given that $|x \cap x_{2r+1}| = r+1, |x_{2r+1} \cap y| = 1, |x| = k+1, |x_{2r+1}| = k, |y| = k+1, x \cup x_{2r+1} \cup y = \Omega$ and $|x \cap x_{2r+1} \cap y| = 0$ or 1.

When $|x \cap x_{2r+1} \cap y| = 1$ we get $|x \cap y| = k + 1 - r$, and this is a contradiction according to the induction hypothesis. When $|x \cap x_{2r+1} \cap y| = 0$, we get $|x \cap y| = k - r$, and the result follows immediately by induction.

Conversely, if $|x \cap y| = k + 1 - (r + 1)$, we need to show that $d(x, y) = 2r + 2$. Choose a vertex w which is on a path from x to y such that $d(w, y) = 1$. This implies that $|w \cap y| = 1$.

Here, we get $|x \cap w| = r + 1$, and by the induction hypothesis, $d(x, w) = 2r + 1$. This shows that $d(x, y) = d(x, w) + d(w, y) = 2r + 2$ as required.

(d) This is a direct implication of (a), (b) and (c). The diameter is attained when $k = m$ in (b).

□

We now consider automorphisms of $\Gamma(2k, k, k+1, 1)$. Let $\alpha \in S_{2k}$. For $m = k$ or $k+1$, define a map $\sigma_\alpha : \Omega^{\{m\}} \to \Omega^{\{m\}}$ by

$$\sigma_\alpha(\{x_1, x_2, \ldots, x_m\}) = \{\alpha(x_1), \alpha(x_2), \ldots, \alpha(x_m)\},$$

the natural induced action of α on $\Omega^{\{m\}}$.

In Lemma 3.4 we show that $\sigma_\alpha \in \mathrm{Aut}(\Gamma(2k, k, k+1, 1))$.

Lemma 3.4. *Let* $\Gamma(2k, k, k+1, 1)$ *be a bipartite graph as defined in Equation* (2.1)*. Then* $\sigma_\alpha \in \mathrm{Aut}(\Gamma(2k, k, k+1, 1))$.

Proof. Since σ_α acts on both $\Omega^{\{k\}}$ and $\Omega^{\{k+1\}}$, it acts on the union. σ_α is clearly one-to-one and onto. It is also easy to see that σ_α preserves adjacency of the graph. Hence $\sigma_\alpha \in \mathrm{Aut}(\Gamma(2k, k, k+1, 1))$. □

Theorem 3.5. *Let k be an integer and* $\Omega = \{1, 2, \ldots, 2k\}$ *where* $2k \geq 6$*. Then* $S_{2k} \cong$ (*a subgroup of*) $\mathrm{Aut}(\Gamma(2k, k, k+1, 1))$.

Proof. Let $\alpha \in S_{2k}$. Recall that α induces a permutation σ_α of $V(\Gamma(2k, k, k+1, 1))$. Define a map $f : S_{2k} \to \mathrm{Aut}(\Gamma(2k, k, k+1, 1))$, given by $f(\alpha) = \sigma_\alpha$. Then f is a homomorphism. It suffices to show that f is also injective.

Let α and β be distinct permutations in S_{2k}. Then there exists an element $i \in \Omega$ such that $\alpha(x_i) \neq \beta(x_i)$. Let $x = \{x_1, x_2, \ldots, x_i, \ldots, x_m\} \in V(\Gamma(2k, k, k+1, 1))$. Then $\sigma_\alpha(x) = \{\alpha(x_1), \alpha(x_2), \ldots, \alpha(x_i), \ldots, \alpha(x_m)\}$ and $\sigma_\beta(x) = \{\beta(x_1), \beta(x_2), \ldots, \beta(x_i), \ldots, \beta(x_m)\}$. Since $\sigma_\alpha(x) \neq \sigma_\beta(x)$, f is injective. Therefore $S_{2k} \hookrightarrow \mathrm{Aut}(\Gamma(2k, k, k+1, 1))$. □

3.3 Binary codes from a biadjacency matrix of $\Gamma(2k, k, k+1, 1)$

As alluded in Chapter 2, Equation 2.6, the design that is used to generate the code has $\mathcal{P} = \Omega^{\{k+1\}}$ as the point set and each point $X \in \Omega^{\{k\}}$ has a block $\overline{X}$ corresponding to it. The block is defined by

$$\overline{X} = N(X) = \{Y \in \Omega^{\{k+1\}} : |Y \cap X| = 1\}.$$

The block set $\mathcal{B}$ is defined by

$$\mathcal{B} = \{\overline{X} : X \in \Omega^{\{k\}}\}.$$

The incidence vector associated with $\overline{X}$ is defined by

$$v^{\overline{X}} = \sum_{j \in X} v^{\{j\} \cup \complement X}, \tag{3.1}$$

where $\complement X = \Omega - X$.

The incidence vector $v^{\overline{X}}$ is the mapping

$$v^{\overline{X}} : \Omega^{\{k+1\}} \to \mathbb{F}_2, Y \mapsto v^{\overline{X}}(Y) = \begin{cases} 1 & \text{if} \quad \complement X \subset Y \\ 0 & \text{if} \quad \complement X \not\subset Y \end{cases}.$$

Hence for $Y \in \Omega^{\{k+1\}}$ we have $v^{\overline{X}}(Y) = 1$ if and only if there is a $j \in X$ with $Y = \{j\} \cup \complement X$.

For the labelling of the transpose B^T,

$$\overline{X} = N(X) = \{Y \in \Omega^{\{k\}} : |Y \cap X| = 1\}.$$

We now determine bases and dimensions for the codes.

Lemma 3.6. *Let k be an integer and $\Omega = \{1, 2, \ldots, 2k\}$. Then*

(a) $S := \{v^{\overline{X}} : X \in \Omega^{\{k\}}, 1 \in X\}$ *is a basis for the code* $C_B(\Gamma(2k,k,k+1,1))$ *and* $\dim(C_B(\Gamma(2k,k,k+1,1))) = \binom{2k-1}{k-1}$.

(b) $S := \{v^{\overline{X}} : X \in \Omega^{\{k+1\}}, 1 \in X\}$ *is a basis for the code* $C_B(\Gamma(2k,k+1,k,1))$ *and* $\dim(C_B(\Gamma(2k,k+1,k,1))) = \binom{2k-1}{k}$.

Proof. (a) The only set $Y \in \Omega^{\{k+1\}}$ with $1 \in Y$ and Y adjacent to X with $1 \in X$ is $\{1\} \cup \complement X$. Then the identity sub-matrix appears in the rows indexed by the X's with $1 \in X$ and the columns indexed by the Y's with $1 \in Y$. When the vectors of S are written in lexicographic order and the points of $\Omega^{\{k+1\}}$ are arranged as follows: first the points

$\{1,2,\ldots,k+1\}, \{1,2,\ldots,k,k+2\}, \ldots, \{1,2,\ldots,k,2k\}, \{1,2,\ldots,k-1,k+1,k+2\}, \ldots, \{1,2,\ldots,k-1,k+1,2k\}, \ldots, \{1,k+1,k+2,\ldots,2k\}$,

followed by the remaining points of $\Omega^{\{k+1\}}$ in arbitrary order, then a matrix of the form $[I_{\binom{2k-1}{k-1}}|A]$ results.

If $1 \notin X_0$ for $X_0 \in \Omega^{\{k\}}$, then since $\complement X_0 \subset Y$ when X_0 and Y are adjacent, $1 \in Y$, and all the non-zero entries for $v^{\overline{X_0}}$ are in those same columns. Such columns are indexed by the sets $\{x\} \cup \complement X_0, x \in X_0$.

We show that the $v^{\overline{X}}$'s with $X = (X_0 - \{x\}) \cup \{1\}$ with 1's where $v^{\overline{X_0}}$ has 1's span the code. The Y's of the form $((\complement X_0) \cup \{x, x'\}) - \{1\}$, with $x' \in X_0$ and $x \neq x'$, are the Y's with $1 \notin Y$ and Y adjacent to X. The other set X' with $1 \in X'$ and Y adjacent to X' is then $(X_0 - \{x'\}) \cup \{1\}$. So in the column labelled by the Y's, two 1's appear from the $\{v^{\overline{X}} : X \in \Omega^{\{k\}}, 1 \in X\}$ vectors corresponding to X and X' and they cancel out when these vectors are added. This shows that S spans $C_B(\Gamma(2k,k,k+1,1))$. Hence S is a basis for $C_B(\Gamma(2k,k,k+1,1))$, and $\dim(C_B(\Gamma(2k,k,k+1,1))) = \binom{2k-1}{k-1}$.

(b) The only set $Y \in \Omega^{\{k\}}$ with $1 \in Y$ and Y adjacent to X with $1 \in X$ is $\{1\} \cup \complement X$. Then the identity sub-matrix appears in the rows indexed by the X's with $1 \in X$ and the columns indexed by the Y's with $1 \in Y$. When the vectors of S are written in lexicographic order and the points of $\Omega^{\{k\}}$ are arranged as follows: first the points

$\{1, 2, \ldots, k\}, \{1, 2, \ldots, k-1, k+1\}, \ldots, \{1, 2, \ldots, k-1, 2k\}, \{1, 2, \ldots, k-2, k, k+1\}, \ldots, \{1, 2, \ldots, k-2, k, 2k\}, \ldots, \{1, k+2, k+3, \ldots, 2k\}$,

followed by the remaining points of $\Omega^{\{k\}}$ in arbitrary order, then a matrix of the form $[I_{\binom{2k-1}{k}}|A]$ results. The proof proceeds exactly as in (a) above.

□

We now investigate comparable results for $C^{\perp}$. To do that we consider binary codes generated by the rows of a biadjacency matrix of $\Gamma(2k, k-2, k+1, 0)$. Here, for $A \in \Omega^{\{k-2\}}$,

$$\overline{A} = N(A) = \{B \in \Omega^{\{k+1\}} : |A \cap B| = 0\}.$$

The block set $\mathcal{B}$ is defined by

$$\mathcal{B} = \{\overline{A} : A \in \Omega^{\{k-2\}}\}.$$

The incidence vector of the block $\overline{A}$ is defined by

$$v^{\overline{A}} \quad = \sum_{\substack{B \subseteq \complement A \\ |B|=k+1}} v^B, \tag{3.2}$$

where $\complement A = \Omega - A$.

It is clear that $\text{wt}(v^{\overline{A}}) = k+2$.

We also consider binary codes generated by the rows of a biadjacency matrix of $\Gamma(2k, k-1, k, 0)$. In this case, for $A \in \Omega^{\{k-1\}}$,

$$\overline{A} = N(A) = \{B \in \Omega^{\{k\}} : |B \cap A| = 0\}.$$

The incidence vector associated with $\overline{A}$ is defined by

$$v^{\overline{A}} \quad = \sum_{\substack{B \subseteq \complement A \\ |B|=k}} v^B. \tag{3.3}$$

We now identify the parameters for the codes.

Lemma 3.7. *Let* k *be an integer and* $\Omega = \{1,2,\dots,2k\}$*. Then*

(a) $R := \{v^{\overline{A}} : A \in \Omega^{\{k-2\}}, 1 \notin A\}$ *is a basis for the code* $C_B(\Gamma(2k,k-2,k+1,0))$ *and* $\dim(C_B(\Gamma(2k,k-2,k+1,0))) = \binom{2k-1}{k-2}$.

(b) $R := \{v^{\overline{A}} : A \in \Omega^{\{k-1\}}, 1 \notin A\}$ *is a basis for the code* $C_B(\Gamma(2k,k-1,k,0))$ *and* $\dim(C_B(\Gamma(2k,k-1,k,0))) = \binom{2k-1}{k-1}$.

Proof. (a) The only set $B \in \Omega^{\{k+1\}}$ with $1 \notin B$ and B adjacent to A with $1 \notin A$ is $\Omega - (A \cup \{1\})$. Then the identity sub-matrix appears in the rows indexed by the A's with $1 \notin A$ and the columns indexed by the B's with $1 \notin B$. When the vectors of R are written in lexicographic order and the points of $\Omega^{\{k+1\}}$ are arranged as follows: first the points

$\{2,3,\dots,k+2\}, \{2,3,\dots,k+1,k+3\},\dots,\{2,3,\dots,k+1,2k\},\{2,3,\dots,k,k+2,k+3\},\dots,\{2,3,\dots,k,2k-1,2k\},\dots,\{2,k+1,k+2,\dots,2k\},\{3,4,\dots,k+3\},\dots,\{3,k+1,k+2,\dots,2k\},\dots,\{k,k+1,\dots,2k\}$,

followed by the remaining points of $\Omega^{\{k+1\}}$ in arbitrary order, then a matrix of the form $[I_{\binom{2k-1}{k-2}}|E]$ results.

If $1 \in A_0$ for $A_0 \in \Omega^{\{k-2\}}$, then since $B \subset \complement A_0$ when A_0 and B are adjacent,$1 \notin B$, and all the non-zero entries for $v^{\overline{A_0}}$ are in those same columns. Such columns are indexed by the sets $\Omega - (A_0 \cup \{a\}), a \in \complement A_0$. We show that the $v^{\overline{A}}$'s with $A = (A_0 - \{1\}) \cup \{a\}$ with 1's where $v^{\overline{A_0}}$ has 1's span the code. The B's of the form $(\Omega - (A_0 \cup \{a, a'\})) \cup \{1\}$ with $a' \in \complement A_0$ and $a \neq a'$, are the B's with $1 \in B$ and B adjacent to A. The other set A' with $1 \notin X'$ and B adjacent to A' is then $(\Omega - A_0) - \{1\}$. So in the column labelled by the B's, two 1's appear from the $\{v^{\overline{A}} : A \in \Omega^{\{k-2\}}, 1 \notin A\}$ vectors corresponding to A and A' and they cancel out when these vectors are added. This shows that R spans $C_B(\Gamma(2k,k-2,k+1,0))$. Hence R is a basis for $C_B(\Gamma(2k,k-2,k+1,0))$. Clearly $\dim(C_B(\Gamma(2k,k-2,k+1,0))) = \binom{2k-1}{k-2}$.

(b) The only set $B \in \Omega^{\{k\}}$ with $1 \notin B$ and B adjacent to A with $1 \notin A$ is $\Omega - (A \cup \{1\})$. Then the identity sub-matrix appears in the rows indexed by the A's with $1 \notin A$ and the columns indexed by B's with

$1 \notin B$. When the vectors of R are written in lexicographic order and the points of $\Omega^{\{k\}}$ are arranged as follows: first the points

$\{2,3,\ldots,k+1\}, \{2,3,\ldots,k,k+2\}, \ldots, \{2,3,\ldots,k,2k\}, \{2,3,\ldots,k-1,k+1,k+2\}, \ldots, \{2,3,\ldots,k-1,2k-1,2k\}, \ldots, \{2,k+2,k+3,\ldots,2k\}$, $\{3,4,\ldots,k+2\}, \ldots, \{3,k+2,k+3,\ldots,2k\}, \ldots, \{k+1,k+2,\ldots,2k\}$,

followed by the remaining points of $\Omega^{\{k\}}$ in arbitrary order, then a matrix of the form $[I_{\binom{2k-1}{k-1}}|E]$ results. The proof proceeds in a similar way as in (a).

□

Lemma 3.8. *Let* $\Omega = \{1,2,\ldots,2k\}$. *Then*

(a) $C_B(\Gamma(2k,k,k+1,1))^{\perp} = C_B(\Gamma(2k,k-2,k+1,0))$.

(b) $C_B(\Gamma(2k,k+1,k,1))^{\perp} = C_B(\Gamma(2k,k-1,k,0))$ *and* $C_B(\Gamma(2k,k+1,k,1)) \cong C_B(\Gamma(2k,k-1,k,0))$.

Proof. (a) We first show that $C_B(\Gamma(2k,k-2,k+1,0)) \subseteq C_B(\Gamma(2k,k,k+1,1))^{\perp}$. To do this we consider the standard inner product $(v^{\overline{X}}, v^{\overline{A}}) = \left(\sum_{j\in X} v^{\{j\}\cup\complement X}, \sum_{B\subseteq\complement A,|B|=k+1} v^{B}\right)$ of any two incidence vectors in $C_B(\Gamma(2k,k,k+1,1))$ and $C_B(\Gamma(2k,k-2,k+1,0))$. If $|X\cap A| = k-2$ then the two vectors are only incident with the two points $X'\cup\{b\}$ and $X'\cup\{b'\}$ where $\{b,b'\} = X - A$ and $X' = \complement X$ and with no other points.

On the other hand, if $|X\cap A| \neq k-2$ then there are no points with which both vectors $v^{\overline{X}}$ and $v^{\overline{A}}$ are commonly incident.

Hence the standard inner product $(v^{\overline{X}}, v^{\overline{A}}) = 0$ in all the cases.

Finally, since $|R| = |\{v^{\overline{A}} : A \in \Omega^{\{k-2\}}, A \subseteq \complement\{1\}\}| = \binom{2k-1}{k-2}$, and $\dim(C_B(\Gamma(2k,k,k+1,1)))^{\perp} = \binom{2k}{k+1} - \binom{2k-1}{k-1}$ it follows that R is a basis for $C_B(\Gamma(2k,k,k+1,1))^{\perp}$. Hence $C_B(\Gamma(2k,k,k+1,1))^{\perp} = C_B(\Gamma(2k,k-2,k+1,0))$.

(b) By a similar argument as in (a) the first part of the result follows, and by Remark 3.2, it follows immediately that $C_B(\Gamma(2k,k+1,k,1)) \cong C_B(\Gamma(2k,k-1,k,0))$.

□

Lemma 3.9. (a) $C_B(\Gamma(2k, k, k+1, 1))$ *has minimum weight* k *and a basis of minimum weight vectors.*

(b) $C_B(\Gamma(2k, k+1, k, 1))$ *has minimum weight* $k+1$ *and a basis of minimum weight vectors.*

Proof. (a) Let $\mathcal{B} = \{\text{Supp}(v^{\overline{A}}) | v^{\overline{A}} \in C_B(\Gamma(2k, k, k+1, 1))^{\perp}\}$. Then $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is a 1-$(\binom{2k}{k+1}, k+2, k-1)$ design, where $k-1$ is the number of blocks through a point. The number of blocks of $\mathcal{B}$ through two distinct points P and Q can have one of $k-1$ values, $\lambda_2, \lambda_3, \ldots, \lambda_k$, depending on the size of $P \cap Q$. Note that the size of $P \cap Q$ cannot be less than two. For a given point $P \in \Omega^{\{k+1\}}$,

- if $2 \leq |P \cap Q| < k$, then there are no blocks $(\lambda_2, \lambda_3, \ldots, \lambda_{k-1} = 0)$ passing through P and Q.
- if $|P \cap Q| = k$, then there is one block $(\lambda_k = 1)$ passing through P and Q.

We will call a point Q distinct from P a point of type-i if $|P \cap Q| = i$, for $i = 2, 3, \ldots, k$. Now let S be the support of $c \in C_B(\Gamma(2k, k, k+1, 1))$, $|S| = s$, and let $P \in S$. Let z_i, for $i = 0$ to $k+2$, be the number of blocks of $\mathcal{B}$ that pass through P and meet S in i points. Then $z_0 = z_1 = 0$ and $\sum\limits_{i=2}^{k+2} z_i = k-1$. Suppose there are m_2 points of $S \setminus \{P\}$ of type-2, i.e on λ_2 blocks with P, m_3 points of type-3, i.e on λ_3 blocks with $P, \ldots, m_k$ points of type-k, i.e on λ_k blocks with P. Then counting incidences gives

$$\sum_{i=2}^{k+2} (i-1) z_i = \lambda_2 m_2 + \lambda_3 m_3 + \cdots + \lambda_k m_k,$$

where $s - 1 = m_2 + m_3 + \cdots + m_k$. Hence

$$\begin{aligned} k-1 = \sum_{i=2}^{k+2} z_i \leq \sum_{i=2}^{k+2} (i-1) z_i &\leq (m_2 + m_3 \cdots + m_k)\lambda_k \\ &= (s-1), \end{aligned}$$

and hence $s \geq k$.

Since the incidence vectors in $C_B(\Gamma(2k, k, k+1, 1))$ have weight k, the minimum weight is k, and $C_B(\Gamma(2k, k, k+1, 1))$ has a basis of minimum weight vectors.

(b) Let $\mathcal{B} = \{\text{Supp}(v^{\overline{A}}) | v^{\overline{A}} \in C_B(\Gamma(2k, k+1, k, 1))^{\perp}\}$. Then $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is a 1-$(\binom{2k}{k}, k+1, k)$ design, where k is the number of blocks through a point. The number of blocks of $\mathcal{B}$ through two distinct points P and Q can have one of k values, $\lambda_0, \lambda_1, \ldots, \lambda_{k-1}$, depending on the size of $P \cap Q$. For a given point $P \in \Omega^{\{k\}}$,

- if $0 \leq |P \cap Q| < k-1$, then there are no blocks ($\lambda_0, \lambda_1, \ldots, \lambda_{k-2} = 0$) passing through P and Q.
- if $|P \cap Q| = k-1$, then there is one block ($\lambda_{k-1} = 1$) passing through P and Q.

Then proof proceeds exactly as in (a).

□

Lemma 3.10. (a) *$C_B(\Gamma(2k, k-2, k+1, 0))$ has minimum weight $k+2$ and a basis of minimum weight vectors.*

(b) *$C_B(\Gamma(2k, k-1, k, 0))$ has minimum weight $k+1$ and a basis of minimum weight vectors.*

Proof. (a) Let $\mathcal{B} = \{\text{Supp}(v^{\overline{X}}) | v^{\overline{X}} \in C_B(\Gamma(2k, k-2, k+1, 0))^{\perp}\}$. Then $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is a 1-$(\binom{2k}{k+1}, k, k+1)$ design, where $k+1$ is the number of blocks through a point. Then the proof proceeds exactly as in 3.9(a).

(b) Using a similar argument as in (a), the result follows.

□

We now focus on the relationship between the codes and their duals by using the $\boldsymbol{j}$-vector.

Lemma 3.11. (a) *If k is even then $\boldsymbol{j} \in \mathrm{Hull}(C_B(\Gamma(2k, k, k+1, 1)))$; otherwise $\boldsymbol{j} \notin \mathrm{Hull}(C_B(\Gamma(2k, k, k+1, 1)))$. Moreover $C_B(\Gamma(2k, k, k+1, 1))$ is neither self-dual nor self-orthogonal.*

(b) *If k is odd then $\boldsymbol{j} \in \mathrm{Hull}(C_B(\Gamma(2k, k+1, k, 1)))$; otherwise $\boldsymbol{j} \notin \mathrm{Hull}(C_B(\Gamma(2k, k+1, k, 1)))$. Moreover $C_B(\Gamma(2k, k+1, k, 1))$ is neither self-dual nor self-orthogonal.*

Proof. (a)

By Equation 3.1

$$\begin{aligned}
\sum_{\substack{X\subseteq\Omega\setminus\{1\}\\|X|=k-1}} v^{\overline{\{1\}\cup X}} &= \sum_{\substack{X\subseteq\Omega\setminus\{1\}\\|X|=k-1}} \sum_{\substack{X'=\Omega\setminus(\{1\}\cup X)\\|X'|=k\\x'\in X}} v^{\{x'\}\cup X'} + \sum_{\substack{X\subseteq\Omega\setminus\{1\}\\|X|=k-1}} v^{\complement X} \\
&= \binom{k}{k-1} \sum_{\substack{X''\subseteq\Omega\setminus\{1\}\\|X''|=k+1}} v^{X''} + \sum_{\substack{X\subseteq\Omega\setminus\{1\}\\|X|=k-1}} v^{\complement X} \qquad (3.4)
\end{aligned}$$

where $\complement X = \Omega \setminus X$.

Similarly, by Equation 3.2

$$\begin{aligned}
\sum_{\substack{X\subseteq\Omega\setminus\{1\}\\|X|=k-2}} v^{\overline{X}} &= \sum_{\substack{X\subseteq\Omega\setminus\{1\}\\|X|=k-2}} \sum_{\substack{X'=\Omega\setminus(\{1\}\cup X)\\|X'|=k\\x'\in X}} v^{\{1\}\cup X'} + \sum_{\substack{X\subseteq\Omega\setminus\{1\}\\|X|=k-2}} v^{\complement(\{1\}\cup X)} \\
&= \binom{k+2}{k+1} \sum_{\substack{X''\subseteq\Omega\setminus\{1\}\\|X''|=k}} v^{\{1\}\cup X''} + \sum_{\substack{X\subseteq\Omega\setminus\{1\}\\|X|=k-2}} v^{\complement(\{1\}\cup X)} \qquad (3.5)
\end{aligned}$$

where $\complement(\{1\} \cup X) = \Omega \setminus (\{1\} \cup X)$.

Now if k is even, then $k+2$ is even too, and by Equations 3.4 and 3.5, $\boldsymbol{j} \in C_B(\Gamma(2k, k, k+1, 1))$ and $\boldsymbol{j} \in C_B(\Gamma(2k, k, k+1, 1))^{\perp}$. On the other hand if k is odd then $\boldsymbol{j} \notin C_B(\Gamma(2k, k, k+1, 1))$ and $\boldsymbol{j} \notin C_B(\Gamma(2k, k, k+1, 1))^{\perp}$.

Alternatively, we can argue that if k is even, then since each basis vector $v^{\overline{A}}, A \in \Omega^{\{k-2\}}, 1 \notin A$, in $C_B(\Gamma(2k, k, k+1, 1))^{\perp}$ has even weight, $\boldsymbol{j}$ is orthogonal to each, and by linearity of the standard inner product, to each vector in $C_B(\Gamma(2k, k, k+1, 1))^{\perp}$. Hence $\boldsymbol{j} \in C_B(\Gamma(2k, k, k+1, 1))$. Similarly if k is even, then $\boldsymbol{j} \in C_B(\Gamma(2k, k, k+1, 1))^{\perp}$. Hence $\boldsymbol{j} \in \mathrm{Hull}(C_B(\Gamma(2k, k, k+1, 1)))$.

In order to determine whether $C_B(\Gamma(2k, k, k+1, 1)) \subseteq C_B(\Gamma(2k, k, k+1, 1))^{\perp}$ consider $(v^{\overline{X}}, v^{\overline{X'}}), X, X' \in \Omega^{\{k\}}$ of any two incidence vectors $v^{\overline{X}}$ and $v^{\overline{X'}}$ in $C_B(\Gamma(2k, k, k+1, 1))$. Now if X and X' have $k-1$ elements in common, then $v^{\overline{X}}$ and $v^{\overline{X'}}$ are commonly incident at one point and hence $(v^{\overline{X}}, v^{\overline{X'}}) = 1$, and $C_B(\Gamma(2k, k, k+1, 1)) \nsubseteq C_B(\Gamma(2k, k, k+1, 1))^{\perp}$.

Neither is $C_B(\Gamma(2k, k, k+1, 1))^{\perp} \subseteq C_B(\Gamma(2k, k, k+1, 1))$, since $(v^{\overline{A}}, v^{\overline{A'}})$, $A, A' \in \Omega^{\{k-2\}} = 1$ if A and A' have $k-3$ elements in common.

Alternatively, it could be argued that $C_B(\Gamma(2k, k, k+1, 1)) \nsubseteq C_B(\Gamma(2k, k, k+1, 1))^{\perp}$ since $C_B(\Gamma(2k, k, k+1, 1))$ have vectors of weight k and $C_B(\Gamma(2k, k, k+1, 1))^{\perp}$ does not. It is clear from above that $C_B(\Gamma(2k, k, k+1, 1))$ is neither self-dual nor self-orthogonal.

(b) Using a similar argument as in (a), the result follows.

□

We now consider automorphisms of the code C. Let $\alpha \in S_{2k}$. For $q = k$ or $k+1$, define a map $\sigma_\alpha : \Omega^{\{q\}} \to \Omega^{\{q\}}$ by

$$\sigma_\alpha(\{x_1, x_2, \ldots, x_q\}) = \{\alpha(x_1), \alpha(x_2), \ldots \alpha(x_q)\}$$

to be the natural induced action of α on $\Omega^{\{q\}}$.

In Lemma 3.12 we show that $\sigma_\alpha \in \mathrm{Aut}(C_B(\Gamma(2k, k, k+1, 1)))$.

Lemma 3.12. *Let k be an integer and $\Omega = \{1, 2, \ldots, 2k\}$. Then $\sigma_\alpha \in \mathrm{Aut}(C_B(\Gamma(2k, k, k+1, 1)))$.*

Proof. Since σ_α acts on both $\Omega^{\{k\}}$ and $\Omega^{\{k+1\}}$, it acts on the union of these sets. σ_α is clearly one-to-one and onto. It is also easy to see that for $Y \in \Omega^{\{k+1\}}, X \in \Omega^{\{k\}}$, if $Y \in \mathrm{Supp}(v^{\overline{X}})$, then $\sigma_\alpha(Y) \in \mathrm{Supp}(v^{\overline{\sigma_\alpha(X)}})$. Hence $\sigma_\alpha \in \mathrm{Aut}(C_B(\Gamma(2k, k, k+1, 1)))$, and σ_α preserves the weight classes of $C_B(\Gamma(2k, k, k+1, 1))$. □

Theorem 3.13. $S_{2k+1} \cong$ (*a subgroup of*) $\mathrm{Aut}(C_B(\Gamma(2k+1,k,k+2,1)))$.

Proof. In this case $\alpha \in S_{2k+1}$ induces an automorphism σ_α of the code $C_B(\Gamma(2k+1,k,k+2,1))$. The proof then proceeds exactly as in Theorem 3.5.

Alternatively, we can argue that since the automorphism group of the graph is contained in the automorphism group of the corresponding code and we have shown in Theorem 3.5 that $S_{2k} \cong$ (a subgroup of) $\mathrm{Aut}(\Gamma(2k,k,k+1,1))$, we can conclude that $S_{2k} \cong$ (a subgroup of) $\mathrm{Aut}(C_B(\Gamma(2k+1,k,k+2,1)))$. □

We next consider permutation decoding sets for the codes.

3.4 Permutation decoding sets for the codes

While the automorphism group of the code provides the base for membership of a PD-set for the code, knowledge about the nature of the information positions and the subsequent action of the automorphism group is crucial in determining this membership.

In Lemma 3.6 (a) the set $S := \{v^X : X \in \Omega^{\{k\}}, 1 \in X\}$ has been identified as a basis for $C_B(\Gamma(2k,k,k+1,1))$. Using the information set from S, namely $\{X \in \Omega^{\{k\}}, 1 \in X\}$, the error-correcting capability for $C_B(\Gamma(2k,k,k+1,1))$ is limited: if errors occur at two information symbols where the union of the the symbols as $(k+1)$-subsets gives the whole set Ω, then there is no automorphism of $C_B(\Gamma(2k,k,k+1,1))$ which will map the errors into check positions. Hence we consider the error-correcting capability of $C_B(\Gamma(2k,k,k+1,1))^\perp = C_B(\Gamma(2k,k-2,k+1,0))$. Using the information set stated in Lemma 3.7 (a) and the fact that $C_B(\Gamma(2k,k-2,k+1,0))$ is able to correct $t = \lfloor \frac{k+1}{2} \rfloor$ errors, the automorphism group S_{2k} is a PD-set for $C_B(\Gamma(2k,k-2,k+1,0))$. The following theorem gives a 2-PD-set for $C_B(\Gamma(2k,k-2,k+1,0))$.

Proposition 3.14. *Let* $\Omega = \{1,2,\dots,2k\}$. *Let* $\mathcal{I}$ *denote the set*

$\{\{2,3,\dots,k{+}2\},\{2,3,\dots,k{+}1,k{+}3\},\dots,\{2,3,\dots,k{+}1,2k\},\{2,3,\dots,k,$ $k{+}2,k{+}3\},\dots,\{2,3,\dots,k,2k{-}1,2k\},\dots,\{2,k{+}1,k{+}2,\dots,2k\},\{3,4,\dots,k+$ $3\},\dots,\{3,k+1,k+2,\dots,2k\},\dots,P_{\binom{2k-1}{k+1}} = \{k,k+1,\dots,2k\}\}$.

Then

$$\mathcal{S} = \{1_{2k}\} \cup \{(1,j) : 1 < j \leq 2k\}$$

is a 2-PD-set for $C_B(\Gamma(2k,k-2,k+1,0))$ *with* $\mathcal{I}$ *as the information set.*

Proof. Let $\mathcal{C} = \mathcal{P} \backslash \mathcal{I}$ denote the check set for $C_B(\Gamma(2k,k-2,k+1,0))$. Then

$\mathcal{C} = \{\{1,2,\dots,k{+}1\},\{1,2,\dots,k,k{+}2\},\dots,\{1,2,\dots,k,2k\},\{1,2,\dots,k-1,k+1,k+2\},\dots,\{1,2,\dots,k-1,k+1,2k\},\dots,P_{\binom{2k-1}{k}} = \{1,k+1,k+2,\dots,2k\}\}$.

We need a set $\mathcal{S}$ of elements of $S_{2k} = \text{Aut}(C_B(\Gamma(2k,k-2,k+1,0)))$ such that every 2-set of elements of $\mathcal{P}$ is moved by some element of $\mathcal{S}$ into the check set.

Suppose that the $2 \leq \lfloor \frac{k+1}{2} \rfloor$ errors occur at $\mathcal{E} = \{\{e_1,e_2,\dots,e_{k+1}\},\{e'_1,e'_2,\dots,e'_{k+1}\} : e_1 < e_2 \dots < e_{k+1}, e'_1 < e'_2 \dots < e'_{k+1}\}$.

Case (i) $\mathcal{E} \subseteq \mathcal{C}$. Then we will use the identity element, 1_{2k}, to keep these fixed in the check positions.

Case (ii) $\mathcal{E} \subseteq \mathcal{I}$. Then we will use the transposition $\sigma = (1,j)$, for $j \in (\{e_1,e_2,\dots,e_{k+1}\} \cap \{e'_1,e'_2,\dots,e'_{k+1}\})$ to map the error positions to $\mathcal{C}$.

Case (iii) $\mathcal{E} \subseteq \mathcal{I} \cup \mathcal{C}$, $\mathcal{E} \cap \mathcal{I} \neq \emptyset$, $\mathcal{E} \cap \mathcal{C} \neq \emptyset$. The only possibility is that there is one error in the check set and one error in the information set. Then the transposition $\sigma = (1,j)$, for $j \in (\{e_1,e_2,\dots,e_{k+1}\} \cap \{e'_1,e'_2,\dots,e'_{k+1}\})$ will map the error position in $\mathcal{E} \cap \mathcal{I}$ to $\mathcal{C}$ and keep the one in $\mathcal{E} \cap \mathcal{C}$ fixed. □

Similarly in Lemma 3.6 (b) the set $S := \{v^{\overline{X}} : X \in \Omega^{\{k+1\}}, 1 \in X\}$ has been identified as a basis for $C_B(\Gamma(2k,k+1,k,1))$. The following theorem gives a 2-PD-set for $C_B(\Gamma(2k,k-1,k,0))$.

Proposition 3.15. *Let* $\Omega = \{1,2,\dots,2k\}$. *Let* $\mathcal{I}$ *denote the set*

$\{\{2,3,\dots,k+1\},\{2,3,\dots,k,k+2\},\dots,\{2,3,\dots,k,2k\},\{2,3,\dots,k-1,k{+}1,k{+}2\},\dots,\{2,3,\dots,k{-}1,2k{-}1,2k\},\dots,\{2,k{+}2,k{+}3,\dots,2k\},\{3,4,\dots,k+2\},\dots,\{3,k+2,k+3,\dots,2k\},\dots,\{k+1,k+2,\dots,2k\}\}$.

Then

$$\mathcal{S} = \{1_{2k}\} \cup \{(1,j) : 1 < j \leq 2k\}$$

is a 2-PD-set for $C_B(\Gamma(2k,k-1,k,0))$ *with* $\mathcal{I}$ *as the information set.*

Proof. Let $\mathcal{C} = \mathcal{P} \setminus \mathcal{I}$ denote the check set for $C_B(\Gamma(2k, k-1, k, 0))$. Then

$\mathcal{C} = \{\{1, 2, \ldots, k\}, \{1, 2, \ldots, k{-}1, k{+}1\}, \ldots, \{1, 2, \ldots, k{-}1, 2k\}, \{1, 2, \ldots, k-2, k, k+1\}, \ldots, \{1, 2, \ldots, k-2, k, 2k\}, \ldots, \{1, k+2, k+3, \ldots, 2k\}\}$.

We need a set $\mathcal{S}$ of elements of $S_{2k} = \mathrm{Aut}(C_B(\Gamma(2k, k-1, k, 0)))$ such that every 2-set of elements of $\mathcal{P}$ is moved by some element of $\mathcal{S}$ into the check set.

Suppose that the $2 \leq \lfloor \frac{k}{2} \rfloor$ errors occur at $\mathcal{E} = \{\{e_1, e_2, \ldots, e_k\}, \{e'_1, e'_2, \ldots, e'_k\} : e_1 < e_2 \ldots < e_k, e'_1 < e'_2 \ldots < e'_k\}$. Then the rest of the proof proceeds as in Proposition 3.14.

□

Chapter 4

Codes and partial permutation decoding sets from biadjacency matrices of the bipartite graphs $\Gamma(2k+1,k,k+2,1)$

4.1 Introduction

In this chapter we extend the work done in Chapter 3. The results found in this chapter are more interesting because in considering the codes and their duals from biadjacency matrices of these bipartite graphs, the adjacency matrix of the Odd graph $\mathbb{O}_k$ surfaces unexpectedly as one of the generators of the dual code.

We start by considering some specific properties of the bipartite graphs $\Gamma(2k+1,k,k+2,1)$. This is followed by the construction of binary codes from the row span of biadjacency matrices of these graphs.

The main results obtained are summarised in Theorem 4.1. Throughout this chapter it is assumed that $k \geq 3$ and Ω is a set of size $2k+1$, unless otherwise stated.

Theorem 4.1. *Let $C_B(\Gamma(2k+1,k,k+2,1))$ denote the binary code from the row span of a $\binom{2k+1}{k} \times \binom{2k+1}{k+2}$ biadjacency matrix B of the bipartite graph $\Gamma(2k+1,k,k+2,1)$ and $C_B(\Gamma(2k+1,k,k+2,1))^{\perp}$ its dual. Then*

(a) *$C_B(\Gamma(2k+1,k,k+2,1))$ is a $[\binom{2k+1}{k+2},\binom{2k}{k-1},k]_2$-code. $C_B(\Gamma(2k+1,k,k+2,1))^{\perp}$ is the code from a $\binom{2k+1}{k-2}\times\binom{2k+1}{k+2}$ biadjacency matrix of $\Gamma(2k+1,k-2,k+2,0)$ and is a $[\binom{2k+1}{k+2},\binom{2k}{k-2},k+3]_2$-code.*

(b) *$C_B(\Gamma(2k+1,k+2,k,1))$ is a $[\binom{2k+1}{k},\binom{2k}{k+1},k+2]_2$-code. $C_B(\Gamma(2k+1,k+2,k,1))^{\perp}$ is the code from an adjacency matrix of the* **odd graph** *$\Gamma(2k+1,k,0)$ and is a $[\binom{2k+1}{k},\binom{2k}{k},k+1]_2$-code.*

(c) *$S_{2k+1}\cong$ (a subgroup of) $\mathrm{Aut}(\Gamma(2k+1,k,k+2,1))$ and $S_{2k+1}\cong$ (a subgroup of) $\mathrm{Aut}(C_B(\Gamma(2k+1,k,k+2,1)))$.*

(d) *$\mathcal{S}=\{1_{S_{2k+1}}\}\cup\{(1,j):1<j\leq 2k+1\}$ is a 2-PD-set of size $2k+1$ for the dual code $C_B(\Gamma(2k+1,k,k+2,1))^{\perp}$.*

Note that $C_B(\Gamma(2k+1,k+2,k,1))$ is the row span of B^T for $C_B(\Gamma(2k+1,k,k+2,1))$ and since $\mathrm{rank}_2(B)=\mathrm{rank}_2(B^T)$, the dimensions of the codes are equal as given by $\binom{2k}{k+1}$ and $\binom{2k}{k-1}$.

The proof of Theorem 4.1, together with further results regarding the graphs we are considering and the codes from these graphs, are given in the sections to follow.

Let $\boldsymbol{C_B(\Gamma(n,m,l,i))}$ denote the binary code from the row span of a $\binom{n}{m}\times\binom{n}{l}$ biadjacency matrix B of the bipartite graph $\Gamma(n,m,l,i)$ and $\boldsymbol{C_B(\Gamma(n,m,l,i))^{\perp}}$ its dual. Further, let $\boldsymbol{C(\Gamma(2k+1,k,0))}$ denote the binary code from the row span of an adjacency matrix of the **odd graph** $\Gamma(2k+1,k,0)$.

4.2 The bipartite graphs $\Gamma(2k+1,k,k+2,1)$

As expressed in Chapter 3, the following proposition gives a direct relationship between the distance between any two vertices and the size of their intersection. This consequently determines the eccentricities of the vertices and the diameters of the graphs that we are examining.

Proposition 4.2. *Let p be a positive integer. Let u,v,x and y be distinct vertices of a bipartite graph $\Gamma(2k+1,k,k+2,1)$ such that $u,v\in\Omega^{\{k\}}$, $x,y\in\Omega^{\{k+2\}}$. Then the following hold:*

(a) *For* $0 \leq p \leq k-1$, $d(u,x) = 2p+1$ *if and only if* $|u \cap x| = p+1$;

(b) *For* $0 \leq p \leq k$, $d(u,v) = 2p$ *if and only if* $|u \cap v| = k-p$;

(c) *For* $0 \leq p \leq k-1$, $d(x,y) = 2p$ *if and only if* $|x \cap y| = k+2-p$;

(d) *The diameter of the graph is* $2k$.

Proof. Again, we proceed by induction on p for the first three cases simultaneously using $p = 0$ as a base case.

(a) If $d(u,x) = 1$, by definition, we have $|u \cap x| = 1$. Conversely, if $|u \cap x| = 1$ then $d(u,x) = 1$.

(b) If $d(u,v) = 0$, we have $|u \cap v| = k$. Conversely, if $|u \cap v| = k$ then $u = v$, and hence $d(u,v) = 0$.

(c) If $d(x,y) = 0$, we have $|x \cap y| = k+2$. Conversely, if $|x \cap y| = k+2$ then $x = y$, and hence $d(x,y) = 0$.

Suppose the statement holds for $p = r$. We need to show that in (a), (b) and (c) it also holds for $p = r+1$.

(a) We need to show that $d(u,x) = 2(r+1)+1 = 2r+3$ implies $|u \cap x| = r+2$. Let $d(u,x) = 2r+3$. It follows that there exists a path of length $2r+3$ from u to x. Let the path be $uu_1u_2 \cdots u_{2r}u_{2r+1}u_{2r+2}x$. Since it is given that $|u \cap u_{2r}| = k-r, |u_{2r} \cap x| = 2, |u| = k, |u_{2r}| = k, |x| = k+2, |u \cup u_{2r} \cup x| = 2k$, and hence $|u \cap u_{2r} \cap x|$ is 0, 1 or 2.

We use the inclusion-exclusion principle and the three possibilities for $|u \cap u_{2r} \cap x|$.

When $|u \cap u_{2r} \cap x| = 0$, we get $|u \cap x| = r$, and this is a contradiction since that case does not arise. When $|u \cap u_{2r} \cap x| = 1$, we get $|u \cap x| = r+1$, and this is a contradiction according to the induction hypothesis. When $|u \cap u_{2r} \cap x| = 2$, we get $|u \cap x| = r+2$, and the result follows by induction.

Conversely, if $|u \cap x| = r+2$, we need to show that $d(u,x) = 2r+3$. Choose a vertex w which is on a path from u to x such that $d(w,x) = 3$. This implies that $|w \cap x| = 2$.

By the inclusion-exclusion principle we get $|u \cap w| = k - r$, and by the induction hypothesis, $d(u, w) = 2r$. This shows that $d(u, x) = d(u, w) + d(w, x) = 2r + 3$ as required.

(b) We need to show that $d(u, v) = 2(r + 1) = 2r + 2$ implies $|u \cap v| = k - (r + 1)$. Let $d(u, v) = 2r + 2$. It follows that there exists a path of length $2r + 2$ from u to v. Let the path be $uu_1u_2 \cdots u_{2r}u_{2r+1}v$.

It is given that $|u \cap u_{2r+1}| = r + 1, |u_{2r+1} \cap v| = 1, |u| = k, |u_{2r+1}| = k + 2, |v| = k, u \cup u_{2r+1} \cup v = \Omega$, and hence $|u \cap u_{2r+1} \cap v|$ is either 0 or 1.

We now use the inclusion-exclusion principle and the two possibilities for $|u \cap u_{2r+1} \cap v|$.

When $|u \cap u_{2r+1} \cap v| = 1$, we get $|u \cap v| = k - r$, and this is a contradiction according to the induction hypothesis. When $|u \cap u_{2r+1} \cap v| = 0$, we get $|u \cap v| = k - (r + 1)$, and the result follows by induction.

Conversely, if $|u \cap v| = k - (r + 1)$, we need to show that $d(u, v) = 2r + 2$. Choose a vertex w which is on a path from u to v such that $d(w, v) = 1$. This implies that $|w \cap v| = 1$.

By the inclusion-exclusion principle we get $|u \cap v| = r + 1$, and by the induction hypothesis $d(u, w) = 2r + 1$. This shows that $d(u, v) = d(u, w) + d(w, v) = 2r + 2$ as required.

(c) We need to show that $d(x, y) = 2(r + 1) = 2r + 2$ implies $|x \cap y| = k + 2 - (r + 1) = k + 1 - r$. Let $d(x, y) = 2r + 2$. It follows that there exists a path of length $2r + 2$ from x to y. Let the path be $xx_1x_2 \cdots x_{2r}x_{2r+1}y$.

It is given that $|x \cap x_{2r+1}| = r + 1, |x_{2r+1} \cap y| = 1, |x| = k + 2, |x_{2r+1}| = k, |y| = k + 2, x \cup x_{2r+1} \cup y = \Omega$, and hence $|x \cap x_{2r+1} \cap y|$ is either 0 or 1.

When $|x \cap x_{2r+1} \cap y| = 1$, we get $|x \cap y| = k + 2 - r$, and this is a contradiction according to the induction hypothesis. When $|x \cap x_{2r+1} \cap y| = 0$, we get $|x \cap y| = k + 1 - r$, and the result follows immediately by induction.

Conversely, if $|x \cap y| = k + 2 - (r + 1)$, we need to show that $d(x, y) = 2r + 2$. Choose a vertex w which is on a path from x to y such that $d(w, y) = 1$. This implies that $|w \cap y| = 1$.

Here we get $|x \cap y| = r + 1$, and by the induction hypothesis $d(x, w) = 2r+1$. This shows that $d(x, y) = d(x, w)+d(w, y) = 2r+2$ as required.

(d) This is a direct consequence of (a), (b) and (c). The diameter is attained when $k = p$ in (b).

□

We now consider automorphisms of $\Gamma(2k + 1, k, k + 2, 1)$. Let $\alpha \in S_{2k+1}$. For $q = k$ or $k + 2$, define a map $\sigma_\alpha : \Omega^{\{q\}} \to \Omega^{\{q\}}$ by

$$\sigma_\alpha(\{x_1, x_2, \ldots, x_q\}) = \{\alpha(x_1), \alpha(x_2), \ldots, \alpha(x_q)\}$$

to be the natural induced action of α on $\Omega^{\{q\}}$.

In Lemma 4.3 we show that $\sigma_\alpha \in \mathrm{Aut}(\Gamma(2k + 1, k, k + 2, 1))$.

Lemma 4.3. $\sigma_\alpha \in \mathrm{Aut}(\Gamma(2k + 1, k, k + 2, 1))$.

Proof. The proof proceeds similarly as the proof done in Lemma 3.4 in Chapter 3. □

Theorem 4.4. $S_{2k+1} \cong$ (*a subgroup of*) $\mathrm{Aut}(\Gamma(2k + 1, k, k + 2, 1))$.

Proof. The proof proceeds similarly as the proof in Theorem 3.5 in Chapter 3. □

In the following section, the main parameters of the binary codes from $\Gamma(2k + 1, k, k + 2, 1)$, and their duals, are obtained.

4.3 Binary codes from biadjacency matrices of the bipartite graphs $\Gamma(2k + 1, k, k + 2, 1)$

As alluded in Chapter 2, Equation 2.6, the design that is used to generate the code has $\mathcal{P} = \Omega^{\{k+2\}}$ as the point set and each point $X \in \Omega^{\{k\}}$ has a block $\overline{X}$ corresponding to it. The block is defined by

$$\overline{X} = N(X) = \{Y \in \Omega^{\{k+2\}} | |Y \cap X| = 1\} = \{\{j\} \cup \complement X | j \in X\},$$

where $\complement X = \Omega - X$.

The block set $\mathcal{B}$ is defined by

$$\mathcal{B} = \{\overline{X} | X \in \Omega^{\{k\}}\}.$$

The incidence vector of the block $\overline{X}$ is defined by

$$v^{\overline{X}} \;=\; \sum_{j \in X} v^{\{j\} \cup \complement X}. \tag{4.1}$$

The incidence vector $v^{\overline{X}}$ is the mapping

$$v^{\overline{X}} : \Omega^{\{k+2\}} \to \mathbb{F}_2, Y \mapsto v^{\overline{X}}(Y) = \begin{cases} 1 & \text{if} \quad \complement X \subset Y \\ 0 & \text{if} \quad \complement X \not\subset Y \end{cases}.$$

Hence for $Y \in \Omega^{\{k+2\}}$, we have $v^{\overline{X}}(Y) = 1$ if and only if there is a $j \in X$ with $Y = \{j\} \cup \complement X$.

For X labelling a row of the transpose B^T,

$$\overline{X} = N(X) = \{Y \in \Omega^{\{k\}} || Y \cap X| = 1\} = \{\{j\} \cup \complement X | j \in X\}.$$

We start by determining bases and dimensions for the codes.

Lemma 4.5. *Let* $\Omega = \{1, 2, \ldots, 2k+1\}$. *Then*

(a) $S := \{v^{\overline{X}} | X \in \Omega^{\{k\}}, 1 \in X\}$ *is a basis for* $C_B(\Gamma(2k+1,k,k+2,1))$ *and* $\dim(C_B(\Gamma(2k+1,k,k+2,1))) = \binom{2k}{k-1}$.

(b) $S := \{v^{\overline{X}} | X \in \Omega^{\{k+2\}}, 1 \in X\}$ *is a basis for* $C_B(\Gamma(2k+1,k+2,k,1))$ *and* $\dim(C_B(\Gamma(2k+1,k+2,k,1))) = \binom{2k}{k+1}$.

Proof. (a) The only set $Y \in \Omega^{\{k+2\}}$ with $1 \in Y$ and Y adjacent to X with $1 \in X$ is $\{1\} \cup \complement X$. Then the identity sub-matrix appears in the rows indexed by the X's with $1 \in X$ and the columns indexed by Y's with $1 \in Y$. When the vectors of S are written in lexicographic order and the points of $\Omega^{\{k+2\}}$ are arranged by placing first the points

$\{1,2,\ldots,k{+}2\},\{1,2,\ldots,k{+}1,k{+}3\},\ldots,\{1,2,\ldots,k{+}1,2k{+}1\},\{1,2,\ldots,k,k{+}1,k{+}2\},\ldots,\{1,2,\ldots,k,k{+}1,2k{+}1\},\ldots,\{1,k{+}1,k{+}2,\ldots,2k{+}1\}$,

followed by the remaining points of $\Omega^{\{k+2\}}$ in arbitrary order, then a matrix of the form $[I_{\binom{2k}{k-1}}|A]$ results.

If $1 \notin X_0$ for $X_0 \in \Omega^{\{k\}}$, then since $\complement X_0 \subset Y$ when X_0 and Y are adjacent, $1 \in Y$, and all the nonzero entries for $v^{\overline{X_0}}$ are in those same columns. Such columns are indexed by the sets $\{x\} \cup \complement X_0, x \in X_0$.

For $1 \notin X \in \Omega^{\{k\}}$, the reader can easily verify that $v^{\overline{X}} = \sum_{\substack{y\subset X\\ |y|=k-1}} v^{\overline{\{1\}\cup y}}$. This shows that S spans $C_B(\Gamma(2k+1,k,k+2,1))$. Hence S is a basis for $C_B(\Gamma(2k{+}1,k,k{+}2,1))$ and $\dim(C_B(\Gamma(2k{+}1,k,k{+}2,1))) = \binom{2k}{k-1}$.

(b) The only set $Y \in \Omega^{\{k\}}$ with $1 \in Y$ and Y adjacent to X with $1 \in X$ is $\{1\} \cup \complement X$. Then the identity sub-matrix appears in the rows indexed by the X's with $1 \in X$ and the columns indexed by Y's with $1 \in Y$. When the vectors of S are written in lexicographic order and the points of $\Omega^{\{k\}}$ are arranged by placing first the points

$\{1,2,\ldots,k\},\{1,2,\ldots,k{-}1,k{+}1\},\ldots,\{1,2,\ldots,k{-}1,2k{+}1\},\{1,2,\ldots,k{-}2,k,k{+}1\},\ldots,\{1,2,\ldots,k{-}2,k,2k{+}1\},\ldots,\{1,k{+}2,k{+}3,\ldots,2k{+}1\}$,

followed by the remaining points of $\Omega^{\{k\}}$ in arbitrary order, then a matrix of the form $[I_{\binom{2k}{k+1}}|A]$ results.

By a similar argument as in (a), the result follows.

□

We now investigate $C_B(\Gamma(2k{+}1,k,k{+}2,1))^{\perp}$ and for this we first consider binary codes generated by the rows of a biadjacency matrix of the bipartite graph $\Gamma(2k+1,k-2,k+2,0)$. We take $\mathcal{P} = \Omega^{\{k+2\}}$ as the point set of the 1-design $\mathcal{D} = (\mathcal{P},\mathcal{B})$. Each $A \in \Omega^{\{k-2\}}$ has a block $\overline{A}$ corresponding to it. The block is defined by

$$\overline{A} = N(A) = \{B \in \Omega^{\{k+2\}} | |A \cap B| = 0\} = \{B \in \Omega^{\{k+2\}} | B \subset \complement A\}.$$

The block set $\mathcal{B}$ is defined by

$$\mathcal{B} = \{\overline{A} | A \in \Omega^{\{k-2\}}\}.$$

The incidence vector of the block $\overline{A}$ is defined by

$$v^{\overline{A}} = \sum_{\substack{B \subset \complement A \\ |B|=k+2}} v^B. \tag{4.2}$$

We also investigate $C_B(\Gamma(2k+1,k+2,k,1))^{\perp}$. To do that we consider binary codes generated by the rows of an adjacency matrix of the odd graph $\Gamma(2k+1,k,0)$. Here, for $A \in \Omega^{\{k\}}$,

$$\overline{A} = N(A) = \{B \in \Omega^{\{k\}} || A \cap B| = 0\} = \{B \in \Omega^{\{k\}} | B \subset \complement A\}.$$

The incidence vector of the block $\overline{A}$ for $A \in \Omega^{\{k\}}$ is defined by

$$v^{\overline{A}} = \sum_{\substack{B \subset \complement A \\ |B|=k}} v^B. \tag{4.3}$$

The binary codes and their duals from the row span of an adjacency matrix of the odd graph $\Gamma(2k+1,k,0)$ were examined in [28] and [30].

We state the following result which gives a basis and the dimension for $C(\Gamma(2k+1,k,0))$. The proof can be found in [30].

Result 4.6. [30, Lemma 3.1] *Let* $k \geq 2$ *be an integer and* $\Omega = \{1,2,\ldots,2k+1\}$*. Then* $R := \{v^{\overline{A}} | A \in \Omega^{\{k\}}, A \subset \complement\{1\}\}$ *is a basis for* $C(\Gamma(2k+1,k,0))$ *and* $\dim(C(\Gamma(2k+1,k,0))) = \binom{2k}{k}$.

The following lemma gives a basis and the dimension for $C_B(\Gamma(2k+1,k-2,k+2,0))$.

Lemma 4.7. *Let* $\Omega = \{1,2,\ldots,2k+1\}$*. Then* $R := \{v^{\overline{A}} | A \in \Omega^{\{k-2\}}, A \subset \complement\{1\}\}$ *is a basis for* $C_B(\Gamma(2k+1,k-2,k+2,0))$ *and* $\dim(C_B(\Gamma(2k+1,k-2,k+2,0))) = \binom{2k}{k-2}$.

Proof. The only set $B \in \Omega^{\{k+2\}}$ with $1 \notin B$ and B adjacent to A with $1 \notin A$ is $\Omega - (A \cup \{1\})$. Then the identity sub-matrix appears in the rows indexed by the A's with $1 \notin A$ and the columns indexed by B's with $1 \notin B$. When the vectors of R are written in lexicographic order and the points of $\Omega^{\{k+2\}}$ are arranged by placing first the points

$\{2,3,\ldots,k{+}3\}, \{2,3,\ldots,k{+}2,k{+}4\}, \ldots, \{2,3,\ldots,k{+}2,2k{+}1\}, \{2,3,\ldots, k{+}1,k{+}2,k{+}3\}, \ldots, \{2,3,\ldots,k{+}1,2k,2k{+}1\}, \ldots, \{2,k{+}1,k{+}2,\ldots,2k{+}1\}, \{3,4,\ldots,k{+}4\}, \ldots, \{3,k{+}1,k{+}2,\ldots,2k{+}1\}, \ldots, \{k,k{+}1,\ldots,2k{+}1\}$,

followed by the remaining points of $\Omega^{\{k+2\}}$ in arbitrary order, then a matrix of the form $[I_{\binom{2k}{k-2}}|E]$ results.

If $1 \in A_0$ for $A_0 \in \Omega^{\{k-2\}}$, then since $B \subset \complement A_0$ when A_0 and B are adjacent, $1 \notin B$, and all the non-zero entries for $v^{\overline{A_0}}$ are in those same columns. Such columns are indexed by the sets $\Omega - (A_0 \cup \{a\}), a \in \complement A_0$.

For $1 \in A \in \Omega^{\{k-2\}}$, the reader can easily verify that $v^{\overline{A}} = \sum_{\substack{y=A-\{1\} \\ x \in \complement A}} v^{\overline{\{x\}\cup y}}$. This shows that R spans $C_B(\Gamma(2k+1,k-2,k+2,0))$. Hence R is a basis for $C_B(\Gamma(2k{+}1,k{-}2,k{+}2,0))$ and $\dim(C_B(\Gamma(2k{+}1,k{-}2,k{+}2,0))) = \binom{2k}{k-2}$. □

Lemma 4.8. (a) $C_B(\Gamma(2k{+}1,k,k{+}2,1))^{\perp} = C_B(\Gamma(2k{+}1,k{-}2,k{+}2,0))$.

(b) $C_B(\Gamma(2k+1,k+2,k,1))^{\perp} = C(\Gamma(2k+1,k,0))$.

Proof. (a) We first show that $C_B(\Gamma(2k{+}1,k{-}2,k{+}2,0)) \subseteq C_B(\Gamma(2k{+}1,k,k+2,1))^{\perp}$. To do this we consider the standard inner product $(v^{\overline{X}}, v^{\overline{A}}) = \left(\sum_{j \in X} v^{\{j\}\cup\complement X}, \sum_{B \subset \complement A, |B|=k+2} v^{B} \right)$ of any two incidence vectors in $C_B(\Gamma(2k{+}1,k,k{+}2,1))$ and $C_B(\Gamma(2k{+}1,k{-}2,k{+}2,0))$ respectively. If $|X \cap A| = k-2$, then the two vectors are only incident with the two points $X' \cup \{b\}$ and $X' \cup \{b'\}$ where $\{b,b'\} = X - A$ and $X' = \complement X$ and with no other points.

On the other hand, if $|X \cap A| \neq k-2$, then $v^{\overline{X}}$ and $v^{\overline{A}}$ are not commonly incident with any points.

Hence the standard inner product $(v^{\overline{X}}, v^{\overline{A}}) = 0$ in all cases. Hence $C_B(\Gamma(2k+1,k-2,k+2,0)) \subseteq C_B(\Gamma(2k+1,k,k+2,1))^{\perp}$. Since in addition, $\dim(C_B(\Gamma(2k+1,k-2,k+2,0))) = \binom{2k}{k-2} = \binom{2k+1}{k+2} - \binom{2k}{k-1} =$

$\binom{2k+1}{k+2} - \dim(C_B(\Gamma(2k+1,k,k+2,1)))$, it follows that $C_B(\Gamma(2k+1,k,k+2,1))^{\perp} = C_B(\Gamma(2k+1,k-2,k+2,0))$.

(b) By a similar argument as the one used in (a), the result follows.

□

The following result gives the minimum weight for $C(\Gamma(2k+1,k,0))$. The proof can be found in [30].

Result 4.9. [30, Lemma 3.2] *Let $k \geq 2$ be an integer. Then $C(\Gamma(2k+1,k,0)$ has minimum weight $k+1$.*

The following lemmas give the minimum weight for the codes $C_B(\Gamma(2k+1,k,k+2,1))$, $C_B(\Gamma(2k+1,k+2,k,1))$ and $C_B(\Gamma(2k+1,k,k+2,1))^{\perp}$. The proofs proceed as in [58, Proposition 4].

Lemma 4.10. (a) *$C_B(\Gamma(2k+1,k,k+2,1))$ has minimum weight k and a basis of minimum weight vectors.*

(b) *$C_B(\Gamma(2k+1,k+2,k,1))$ has minimum weight $k+2$ and a basis of minimum weight vectors.*

Proof. (a) Let $\mathcal{B} = \{\mathrm{Supp}(v^{\overline{A}}) | v^{\overline{A}} \in C_B(\Gamma(2k+1,k,k+2,1))^{\perp}\}$. Then $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is a 1-$(\binom{2k+1}{k+2}, k+3, k-1)$ design, where $k-1$ is the number of blocks through a point. The number of blocks of $\mathcal{B}$ through two distinct points P and Q can have one of $k-1$ values, $\lambda_3, \lambda_4, \ldots, \lambda_{k+1}$, depending on the size of $P \cap Q$. Note that the size of $P \cap Q$ cannot be less than three. For a given point $P \in \Omega^{\{k+2\}}$,

- if $3 \leq |P \cap Q| < k+1$, then there are no blocks ($\lambda_3, \lambda_4, \ldots, \lambda_k = 0$) passing through P and Q.
- if $|P \cap Q| = k+1$, then there is one block ($\lambda_{k+1} = 1$) passing through P and Q.

A point Q distinct from P a point is of type-i if $|P \cap Q| = i$, for $i = 3, 4, \ldots, k+1$. Now let S be the support of $c \in C_B(\Gamma(2k+1,k,k+2,1))$, $|S| = s$, and let $P \in S$. Let z_i, for $i = 0$ to $k+3$, be the number of blocks of $\mathcal{B}$ that pass through P and meet S in i points. Then $z_0 = z_1 = 0$ and $\sum_{i=2}^{k+3} z_i = k-1$. Suppose there are m_3 points of $S \setminus \{P\}$ of type-3, i.e on λ_3 blocks with P, m_4 points of type-4, i.e on λ_4 blocks with $P, \ldots, m_{k+1}$ points of type-$(k+1)$, i.e on λ_{k+1} blocks with P. Then counting incidences gives

$$\sum_{i=2}^{k+3}(i-1)z_i = \lambda_3 m_3 + \lambda_4 m_4 + \cdots + \lambda_{k+1}m_{k+1},$$

where $s-1 = m_3 + m_4 + \cdots + m_{k+1}$. Hence

$$\begin{aligned} k-1 = \sum_{i=2}^{k+3} z_i \leq \sum_{i=2}^{k+3}(i-1)z_i &\leq (m_3 + m_4 \cdots + m_{k+1})\lambda_{k+1} \\ &= (s-1), \end{aligned}$$

and hence $s \geq k$.

Since the incidence vectors in $C_B(\Gamma(2k+1,k,k+2,1))$ have weight k, the minimum weight is k, and $C_B(\Gamma(2k+1,k,k+2,1))$ has a basis of minimum weight vectors.

(b) Let $\mathcal{B} = \{\text{Supp}(v^{\overline{A}}) | v^{\overline{A}} \in C_B(\Gamma(2k+1,k+2,k,1))^{\perp}\}$. Then $\mathcal{D} = (\mathcal{P},\mathcal{B})$ is a 1-$(\binom{2k+1}{k}, k+1, k+1)$ design, where $k+1$ is the number of blocks through a point. The number of blocks of $\mathcal{B}$ through two distinct points P and Q can have one of k values, $\lambda_0, \lambda_1, \ldots, \lambda_{k-1}$, depending on the size of $P \cap Q$. For a given point $P \in \Omega^{\{k\}}$,

- if $0 \leq |P \cap Q| < k-1$, then there are no blocks ($\lambda_0, \lambda_1, \ldots, \lambda_{k-2} = 0$) passing through P and Q.
- if $|P \cap Q| = k-1$, then there is one block ($\lambda_{k-1} = 1$) passing through P and Q.

  The proof proceeds exactly as in (a).

□

Lemma 4.11. $C_B(\Gamma(2k+1,k,k+2,1))^{\perp}$ *has minimum weight* $k+3$ *and a basis of minimum weight vectors.*

Proof. Let $\mathcal{B} = \{\mathrm{Supp}(v^{\overline{X}}) | v^{\overline{X}} \in C_B(\Gamma(2k+1,k-2,k+2,0))^{\perp}\}$. Then $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is a 1-$(\binom{2k+1}{k+2}, k, k+2)$ design, where $k+2$ is the number of blocks through a point. The proof the proceeds exactly as in Lemma 4.10(a).

□

In the following lemma we focus on the relationship between the codes and their duals by using the $\boldsymbol{j}$-vector.

Result 4.12. [30, Lemma 3.8] *If* k *is even, then* $\boldsymbol{j} \in C(\Gamma(2k+1,k,0))$; *otherwise* $\boldsymbol{j} \in C(\Gamma(2k+1,k,0))^{\perp}$. *Moreover* $C(\Gamma(2k+1,k,0))$ *is neither self-dual or self-orthogonal for any* $k \geq 2$. *In fact,* $C(\Gamma(2k+1,k,0)) \oplus C(\Gamma(2k+1,k,0))^{\perp} = \mathbb{F}_2^{\binom{2k+1}{k}}$ *for all* $k \geq 2$.

Lemma 4.13. *If* k *is odd then* $\boldsymbol{j} \in C_B(\Gamma(2k+1,k,k+2,1))$; *otherwise* $\boldsymbol{j} \in C_B(\Gamma(2k+1,k,k+2,1))^{\perp}$. *Moreover* $C_B(\Gamma(2k+1,k,k+2,1))$ *is neither self-dual nor self-orthogonal.*

Proof. By Equation 4.1

$$\begin{aligned}
\sum_{\substack{X\subseteq\Omega\backslash\{1\}\\|X|=k-1}} v^{\overline{\{1\}\cup X}} &= \sum_{\substack{X\subseteq\Omega\backslash\{1\}\\|X|=k-1}} \sum_{\substack{X'=\Omega\backslash(\{1\}\cup X)\\|X'|=k+1\\x'\in X}} v^{\{x'\}\cup X'} + \sum_{\substack{X\subseteq\Omega\backslash\{1\}\\|X|=k-1}} v^{\complement X} \\
&= \binom{k}{k-1} \sum_{\substack{X''\subseteq\Omega\backslash\{1\}\\|X''|=k+2}} v^{X''} + \sum_{\substack{X\subseteq\Omega\backslash\{1\}\\|X|=k-1}} v^{\complement X} \qquad (4.4)
\end{aligned}$$

where $\complement X = \Omega \setminus X$.

Similarly, by Equation 4.2

$$\begin{aligned}
\sum_{\substack{X\subseteq\Omega\backslash\{1\}\\|X|=k-2}} v^{\overline{X}} &= \sum_{\substack{X\subseteq\Omega\backslash\{1\}\\|X|=k-2}} \sum_{\substack{X'=\Omega\backslash(\{1\}\cup X)\\|X'|=k+1\\x'\in X}} v^{\{1\}\cup X'} + \sum_{\substack{X\subseteq\Omega\backslash\{1\}\\|X|=k-2}} v^{\complement(\{1\}\cup X)} \\
&= \binom{k+2}{k+1} \sum_{\substack{X''\subseteq\Omega\backslash\{1\}\\|X''|=k+1}} v^{\{1\}\cup X''} + \sum_{\substack{X\subseteq\Omega\backslash\{1\}\\|X|=k-2}} v^{\complement(\{1\}\cup X)} \qquad (4.5)
\end{aligned}$$

where $\complement(\{1\}\cup X) = \Omega \setminus (\{1\}\cup X)$.

Now if k is odd, then $k+3$ is even, and by Equations 4.4 and 4.5, $\boldsymbol{j} \in C_B(\Gamma(2k+1,k,k+2,1))$. On the other hand if k is even then $\boldsymbol{j} \in C_B(\Gamma(2k+1,k,k+2,1))^{\perp}$.

Alternatively, if k is odd, then since each basis vector $v^{\overline{A}}, A \in \Omega^{\{k-2\}}, 1 \notin A$, in $C_B(\Gamma(2k+1,k,k+2,1))^{\perp}$ has even weight, $\boldsymbol{j}$ is orthogonal to each, and by linearity of the standard inner product, to each vector in $C_B(\Gamma(2k+1,k,k+2,1))^{\perp}$. Hence $\boldsymbol{j} \in C_B(\Gamma(2k+1,k,k+2,1))$. If k is even, then since each basis vector $v^{\overline{X}}, A \in \Omega^{\{k\}}, 1 \in X$, in $C_B(\Gamma(2k+1,k,k+2,1))$ has even weight, $\boldsymbol{j}$ is orthogonal to each vector in $C_B(\Gamma(2k+1,k,k+2,1))$. Hence $\boldsymbol{j} \in C_B(\Gamma(2k+1,k,k+2,1))^{\perp}$.

In order to determine whether $C_B(\Gamma(2k+1,k,k+2,1)) \subseteq C_B(\Gamma(2k+1,k,k+2,1))^{\perp}$ consider $(v^{\overline{X}}, v^{\overline{X'}}), X, X' \in \Omega^{\{k\}}$ of any two incidence vectors $v^{\overline{X}}$ and $v^{\overline{X'}}$ in $C_B(\Gamma(2k+1,k,k+2,1))$. Now if X and X' have $k-1$ elements in common, then $v^{\overline{X}}$ and $v^{\overline{X'}}$ are commonly incident at one point and hence $(v^{\overline{X}}, v^{\overline{X'}}) = 1$, and $C_B(\Gamma(2k+1,k,k+2,1)) \nsubseteq C_B(\Gamma(2k+1,k,k+2,1))^{\perp}$.

Neither is $C_B(\Gamma(2k+1,k,k+2,1))^{\perp} \subseteq C_B(\Gamma(2k+1,k,k+2,1))$, since for $A, A' \in \Omega^{\{k-2\}}$, $(v^{\overline{A}}, v^{\overline{A'}}) = 1$ if A and A' have $k-3$ elements in common.

Alternatively, it could be argued that $C_B(\Gamma(2k+1,k,k+2,1)) \nsubseteq C_B(\Gamma(2k+1,k,k+2,1))^{\perp}$ since $C_B(\Gamma(2k+1,k,k+2,1))$ have vectors of weight k and $C_B(\Gamma(2k+1,k,k+2,1))^{\perp}$ does not. It is clear from above that $\boldsymbol{j} \notin \mathrm{Hull}(C_B(\Gamma(2k+1,k,k+2,1)))$. □

The following result gives the automorphism group of $C(\Gamma(2k+1,k,0))$. The proof can be found in [30].

Result 4.14. [30, Proposition 3.11] *Let $k \geq 2$ be an integer. Then the automorphism group of $C(\Gamma(2k+1,k,0))$ is S_{2k+1}.*

We now consider automorphisms of the code $C_B(\Gamma(2k+1,k,k+2,1))$. We recall the definition of σ_α preceding Lemma 4.3 let $\alpha \in S_{2k+1}$, and for $q = k$ or $k+2$, $\sigma_\alpha : \Omega^{\{q\}} \to \Omega^{\{q\}}$ is defined by

$$\sigma_\alpha(\{x_1, x_2, \ldots, x_q\}) = \{\alpha(x_1), \alpha(x_2), \ldots, \alpha(x_q)\}.$$

The following are the analogies of Lemma 4.3 and Theorem 6.12.

Lemma 4.15. $\sigma_\alpha \in \mathrm{Aut}(C_B(\Gamma(2k+1,k,k+2,1)))$.

Proof. Since σ_α acts on both $\Omega^{\{k\}}$ and $\Omega^{\{k+2\}}$, it acts on the union of these sets. σ_α is clearly one-to-one and onto. It is also easy to see that for $Y \in \Omega^{\{k+2\}}, X \in \Omega^{\{k\}}$, if $Y \in \mathrm{Supp}(v^{\overline{X}})$, then $\sigma_\alpha(Y) \in \mathrm{Supp}(v^{\overline{\sigma_\alpha(X)}})$. Hence $\sigma_\alpha \in \mathrm{Aut}(C_B(\Gamma(2k+1,k,k+2,1)))$, and σ_α preserves the weight classes of $C_B(\Gamma(2k+1,k,k+2,1))$. □

Theorem 4.16. $S_{2k+1} \cong$ (*a subgroup of*) $\mathrm{Aut}(C_B(\Gamma(2k+1,k,k+2,1)))$.

Proof. In this case $\alpha \in S_{2k+1}$ induces an automorphism σ_α of the code $C_B(\Gamma(2k+1,k,k+2,1))$. The proof then proceeds exactly as in Theorem 4.4. □

In the next section, we consider permutation decoding sets for the codes and their duals.

4.4 Permutation decoding sets for the dual codes

We start by giving a result for a 2-PD-set for $C(\Gamma(2k+1,k,0))$. The proof can be found in [30].

Result 4.17. [30, Theorem 4.2] *Let* $k \geq 4$ *be an integer and* $\Omega = \{1,2,\ldots,2k+1\}$. *Let* $\mathcal{I}$ *denote the set*

$\{\{1,2,\ldots,k-1,k+1\},\{1,2,\ldots,k-1,k+2\},\ldots,\{1,2,\ldots,k-1,2k+1\},\ldots,\{1,2,\ldots,k-2,k,2k+1\},\ldots,\{1,2,\ldots,k-2,2k-1,2k+1\},\{1,2,\ldots,k-3,k-1,k,k+2\},\ldots,\{1,k+2,k+3,\ldots,2k-1,2k+1\},\ldots,\{k+1,k+2,\ldots,2k-1,2k+1\}\}$.

Then

$$\mathcal{S} = \{(k-1+i,k+j)(k-1+i',k+j') : 0 \leq i \leq j \leq k+1, 0 \leq i' \leq j' \leq k+1\}$$

is a 2-PD-set of size $\binom{k+3}{2}^2$ *for* $C(\Gamma(2k+1,k,0))$ *with* $\mathcal{I}$ *as the information set.*

In Lemma 4.5(a) the set $S := \{v^{\overline{X}} | X \in \Omega^{\{k\}}, 1 \in X\}$ has been identified as a basis for $C_B(\Gamma(2k+1,k,k+2,1))$. Using the information set from S, namely $\{Y \in \Omega^{\{k+2\}}, 1 \in X\}$, the error-correcting capability for $C_B(\Gamma(2k+1,k,k+2,1))$ is limited: if errors occur at two information symbols where the union of the the symbols as (k+2)-subsets gives the whole set Ω, then there is no automorphism of $C_B(\Gamma(2k+1,k,k+2,1))$ which will map the errors into the check positions. Alternatively, we consider the error-correcting capability of $C_B(\Gamma(2k+1,k,k+2,1))^{\perp} = C_B(\Gamma(2k+1,k-2,k+2,0))$. The information positions are given in Lemma 4.7. From Lemma 4.11 we deduce that the code is able to correct $t = \lfloor \frac{k+2}{2} \rfloor$ errors. The following proposition gives a 2-PD-set for $C_B(\Gamma(2k+1,k,k+2,1))^{\perp}$.

Proposition 4.18. *Let* $\Omega = \{1,2,\ldots,2k+1\}$*. Let* $\mathcal{I}$ *denote the set*

$\{\{2,3,\ldots,k+3\},\{2,3,\ldots,k+2,k+4\},\ldots,\{2,3,\ldots,k+2,2k+1\},\{2,3,\ldots,k+1,k+3,k+4\},\ldots,\{2,3,\ldots,k+1,2k,2k+1\},\ldots,\{2,k+1,k+2,\ldots,2k+1\},\{3,4,\ldots,k+3\},\ldots,\{3,k+1,k+2,\ldots,2k+1\},\ldots,P_{\binom{2k}{k+2}} = \{k,k+1,\ldots,2k+1\}\}$.

Then

$$\mathcal{S} = \{1_{S_{2k+1}}\} \cup \{(1,j) : 1 < j \leq 2k+1\}$$

is a 2-PD-set for $C_B(\Gamma(2k+1,k,k+2,1))^{\perp}$ *of size* $2k+1$ *with* $\mathcal{I}$ *as the information set.*

Proof. Let $\mathcal{C} = \mathcal{P} \setminus \mathcal{I}$ denote the check set for $C_B(\Gamma(2k+1,k,k+2,1))^{\perp}$. Then

$\mathcal{C} = \{\{1,2,\ldots,k+2\},\{1,2,\ldots,k+1,k+3\},\ldots,\{1,2,\ldots,k+1,2k+1\},\{1,2,\ldots,k,k+2,k+3\},\ldots,\{1,2,\ldots,k,k+2,2k+1\},\ldots,P_{\binom{2k}{k+1}} = \{1,k+1,k+2,\ldots,2k+1\}\}$.

We need a set $\mathcal{S}$ of elements of S_{2k+1} such that every 2-subset of $\mathcal{P}$ is moved by some element of $\mathcal{S}$ into the check set.

Suppose that the $2 \leq \lfloor \frac{k+2}{2} \rfloor$ errors occur at $\mathcal{E} = \{\{e_1,e_2,\ldots,e_{k+2}\},\{e'_1,e'_2,\ldots,e'_{k+2}\} : e_1 < e_2 \ldots < e_{k+2}, e'_1 < e'_2 \ldots < e'_{k+2}\}$.

Case (i) $\mathcal{E} \subseteq \mathcal{C}$. Then we will use the identity element $1_{S_{2k+1}}$ to keep the error positions fixed in the check set.

Case (ii) $\mathcal{E} \subseteq \mathcal{I}$. Then we will use the transposition $\sigma = (1, j)$ where $j \in \{e_1, e_2, \ldots, e_{k+2}\} \cap \{e'_1, e'_2, \ldots, e'_{k+2}\}$, to map the error positions to $\mathcal{C}$.

Case (iii) $\mathcal{E} \subseteq \mathcal{I} \cup \mathcal{C}$, $\mathcal{E} \cap \mathcal{I} \neq \emptyset$, $\mathcal{E} \cap \mathcal{C} \neq \emptyset$. Then the transposition $\sigma = (1, j)$ where $j \in \{e_1, e_2, \ldots, e_{k+2}\} \cap \{e'_1, e'_2, \ldots, e'_{k+2}\}$, will map the error position in $\mathcal{E} \cap \mathcal{I}$ to $\mathcal{C}$ and keep the one in $\mathcal{E} \cap \mathcal{C}$ fixed. □

Chapter 5

Automorphism groups of graph covers and uniform subset graphs

5.1 Introduction

The uniform subset graphs $\Gamma(2k, k, k-1)$ have been investigated elsewhere as Johnson graphs (see [85]). In this chapter, we determine the automorphism groups of the Johnson graph $\Gamma(2k, k, k-1)$ and that of the uniform subset graph $\Gamma(2k, k, 1)$. We apply the technique of graph covers and their corresponding quotients to determine the automorphism groups of these graphs. This answers a conjecture posed by Mark Ramras and Elizabeth Donovan in [85]. They conjectured that $\text{Aut}(\Gamma(2k, k, k-1)) \cong S_{2k} \times < T >$, where T is the complementation map $X \mapsto T(X) = X^c = \{1, 2, \ldots, 2k\} \setminus X$, and $X \in \Omega^{\{k\}}$.

It is essential to explore the automorphism group of the graph $\Gamma(2k, k, 1)$ since we consider codes from this graph in the next chapter. In addition we also consider the graph $\Gamma(2k, k, k-1)$ to resolve the conjecture above.

5.2 Some properties of the uniform subset graphs $\Gamma(2k,k,1)$ and $\Gamma(2k,k,k-1)$

It is easy to see that the uniform subset graphs $\Gamma(2k,k,1)$ and $\Gamma(2k,k,k-1)$ are regular with $\binom{2k}{k}$ vertices. In both cases, the valency is $\binom{k}{1}\binom{k}{k-1} = k^2$. In general, these graphs are not strongly regular as can be seen from their diameters. One exception is $\Gamma(4,2,1)$ in which any two adjacent vertices are commonly adjacent to two vertices, and any two non-adjacent vertices are commonly adjacent to four vertices. As it has been alluded to in Chapter 2, Proposition 2.26, uniform subset graphs are in general vertex- and edge-transitive, as the symmetric group S_n, in its natural action, induces a transitive action both on its vertex- and edge-set.

As alluded to, S_n in its natural action imbeds into the automorphism group of $\Gamma(n,k,i)$ in the following way:

Let $\alpha \in S_n$. Define a map $\sigma_\alpha : \Omega^{\{k\}} \rightarrow \Omega^{\{k\}}$ by

$$\sigma_\alpha(\{x_1, x_2, \ldots, x_k\}) = \{\alpha(x_1), \alpha(x_2), \ldots, \alpha(x_k)\},$$

the natural induced action of α on $\Omega^{\{k\}}$. As has been observed, this action induces automorphisms of the graphs.

Lemma 5.1. $\sigma_\alpha \in \mathrm{Aut}(\Gamma(n,k,i))$.

Proof. Since σ_α acts on $\Omega^{\{k\}}$, σ_α is clearly one-to-one and onto. It is also easy to see that σ_α preserves adjacency of the graph. Hence $\sigma_\alpha \in \mathrm{Aut}(\Gamma(n,k,i))$. □

Theorem 5.2. $S_n \cong$ (*a subgroup of*) $\mathrm{Aut}(\Gamma(n,k,i))$.

Proof. The proof is similar to one in Theorem 3.5 in Chapter 3. □

It is surprisingly difficult to determine the full automorphism groups of uniform subset graphs. Amongst its many classes, it has only been determined that $\mathrm{Aut}(\Gamma(2k+1,k,0))$, the automorphism group of the so called Odd graphs, is S_{2k+1}, and more recently, Ramras and Donovan [85] proved that $\mathrm{Aut}(\Gamma(n,k,k-1)), n \neq 2k$ coincides with S_n.

For a graph $\Gamma, x \in V(\Gamma)$, we set $\Gamma_i(x) := \{y \in V(\Gamma) | \delta(x,y) = i\}$ and $\epsilon(x) = \max\{\delta(x,y) | y \in V(\Gamma)\}$, where δ is the usual shortest distance path in Γ. Let $\mathcal{P}$ be a partition of $V(\Gamma)$. By the quotient graph $\Gamma/\mathcal{P}$ is meant the graph with

$$\begin{aligned} V(\Gamma/\mathcal{P}) &:= \mathcal{P}; \\ \{X,Y\} \in E(\Gamma/\mathcal{P}) &\iff X \neq Y \text{ and } \{x,y\} \in E(\Gamma) \text{ for some } x \in X, y \in Y. \end{aligned}$$

A graph Γ is said to be *antipodal* if the collection of sets $\{x\} \cup \Gamma_{\epsilon(x)}(x)$ is a partition of $V(\Gamma)$.

For a graph Γ and $A \subset V(\Gamma)$, the minimum distance of A is defined by $\delta(A) := \min_{x,y \in A, x \neq y} \delta(x,y)$.

5.3 Automorphisms of graph covers

In order to determine the automorphism groups of the graphs in question, we employ Hofmeister's [51] strategy. He determines the automorphism group of a graph cover by first looking at the quotient (folded) graph. The key observation in analysing the automorphism group of the cover is in understanding the interplay between automorphisms of the cover and their corresponding quotient.

Definition 5.3. Let Γ and Δ be graphs. Δ is called an r-cover of Γ if there is an epimorphism $\rho : \Delta \to \Gamma$, called the covering projection, such that

(i) $|\rho^{-1}(x)| = r$, for every $x \in V(\Gamma)$;

(ii) ρ bijectively sends $\Delta_1(x)$ to $\Gamma_1(\rho(x))$ for each $x \in V(\Gamma)$.

The graph Γ is called the **fold** of Δ.

Gross and Tucker [46] have shown that graph covers arise from permutation voltage graphs so that the consideration of the former amounts to focussing on the later. Permutation voltage graphs are defined as follows.

For a graph Γ, let $A(\Gamma)$ be the arc set of the corresponding symmetric digraph. A permutation voltage assignment in a symmetric group S_r for Γ

is a mapping $f : A(\Gamma) \to S_r$ such that $f((x, y)) = (f((y, x)))^{-1}$, for any arc (x, y) in $A(\Gamma)$.

Given a graph Γ and a permutation voltage assignment f, the derived graph Γ_f is the graph with

$$V(\Gamma_f) = V(\Gamma) \times \{1, 2, \ldots, r\};$$
$$\{(x, i), (y, j)\} \in E(\Gamma_f) \iff \{x, y\} \in E(\Gamma), (f(x, y))i = j.$$

Gross and Tucker's reductions, as alluded to, is the content of the following two results.

Theorem 5.4. [46] *Let Γ be a graph and $f : A(\Gamma) \to S_r$ a permutation voltage assignment. Then the natural projection $\rho_f : \Gamma_f \to \Gamma$ (sending vertex (u, i) of Γ_f to vertex u of Γ) is an r-fold covering projection.*

Theorem 5.5. [46] *Let $\rho : \Delta \to \Gamma$ be an r-fold covering projection. Then there is an assignment f of voltages in the symmetric group S_r for Γ such that the covering projections ρ and ρ_f are isomorphic with respect to the trivial automorphism.*

It is in the context of permutation voltage graphs that Hofmeister [51] considered the interplay between the automorphisms of graph covers and their corresponding quotient graphs. The essence of this interplay is in the following: Let $H \leq \mathrm{Aut}(\Gamma)$ be a group of automorphisms of the graph Γ. An H-automorphism of a covering projection $\rho : \Delta \to \Gamma$ is a pair (φ, ψ), consisting of an automorphism $\varphi \in H$ and an automorphism $\psi : \Delta \to \Delta$, such that $\varphi\rho = \rho\psi$.

As a generalisation, we consider r-coverings that are defined by semi-regular automorphisms in vertex-transitive graphs. A semi-regular element of an automorphism group of a graph is a non-identity element having all cycles of equal length in its cycle decomposition. In the case of vertex-transitive graphs admitting a semi-regular automorphism, the following generalises antipodal coverings.

Lemma 5.6. *Let Γ be a vertex-transitive graph. Let σ be a semi-regular automorphism of Γ such that the orbits of σ partition $V(\Gamma)$ in such a way that for each cell $X, \delta(X) > 2$. Then the natural projection $f : \Gamma \to \Gamma/\sigma$*

defined by $x \mapsto X, x \in X$, *is a covering, where* Γ/σ *is the partition induced by* σ.

Proof. That $|f^{-1}(x)| = r$, for some fixed positive integer r, is an immediate consequence of semi-regularity of σ.

For any $y, z \in N(x), y \neq z$, the cell containing y is distinct from the cell containing z, since $\delta(X) \geq 2$. Therefore $|N(X)| \geq |N(x)|$ and by vertex transitivity $|N(X)| = |N(x)|$. □

The critical issue Hofmeister [51] observed is the result we generalise to graph covers in Lemma 5.6. In this context, the result below follows from the fact that graph automorphisms are distance-preserving.

Theorem 5.7. *Let* Γ *be a vertex transitive graph. Let* σ *be a semi-regular automorphism of* Γ *such that the orbits of* σ *partition* $V(\Gamma)$ *in such a way that for each cell* $X, \delta(X) > 2$. *Let* $\rho : \Gamma \to \Gamma/\sigma$ *be a covering projection and* ψ *an automorphism of* Γ. *Then there is an automorphism* φ *of* Γ/σ *such that* $\varphi\rho = \rho\psi$, *where* Γ/σ *is the quotient induced by* σ.

Following Homeister [51], we let the group $S_r^{V(\Gamma)}$ act on the set of permutation voltage assignments in S_r for any Γ by $\Pi(f(x, y)) = \pi_y^{-1} f(x, y)\pi_x$ where $\Pi = (\pi_u)_{u \in V(\Gamma)}$. The stabilizer of f under this action will be denoted by $\mathrm{Fix}(\Gamma, f)$.

In this generalised context, we recoup Hofmeister's characterisation of the automorphism groups of graph covers with respect to those of the corresponding quotient graphs and furthermore the argument of the proof of Theorem 5 in [51] holds.

Theorem 5.8. *Let* Γ *be a vertex transitive graph. Let* σ *be a semi-regular automorphism of* Γ *such that the orbits of* σ *partition* $V(\Gamma)$ *in such a way that for each cell* $X, \delta(X) > 2$. *Then there is a short exact sequence*

$$1 \to \mathrm{Fix}(\Gamma, f) \to \mathrm{Aut}(\Gamma_f) \to \mathrm{Aut}(\Gamma)_f \to 1.$$

5.4 Automorphisms of $\Gamma(2k, k, k-1)$ and $\Gamma(2k, k, 1)$

We now show that the graphs $\Gamma(2k, k, k-1)$ and $\Gamma(2k, k, 1)$ are covers of a graph from which one can determine their automorphism groups. Using

Theorem 5.8, we determine these automorphism groups.

Now, consider $\sigma : V(\Gamma(2k, k, i)) \to V(\Gamma(2k, k, i)), i = 1, k-1$ defined by

$$\sigma(X) = \Omega \setminus X. \tag{5.1}$$

It is easy to see that σ is an automorphism of $\Gamma(2k, k, i)$. Moreover, $\delta(X, \Omega \setminus X) = \epsilon(X)$ if $i = k-1$ and $\delta(X, \Omega \setminus X) = 3$ if $i = 1$. Hence we have the following:

Corollary 5.9. $\Gamma(2k, k, i), i = 1, k-1$ *are covers of* $\Gamma(2k, k, i)/\sigma$.

To determine the automorphism groups of $\Gamma(2k, k, k-1)$ and $\Gamma(2k, k, 1)$, it is sufficient to determine the automorphism groups of $\Gamma(2k, k, i)/\sigma, i = 1, k-1$.

Now, as for $\Gamma(2k, k, i)/\sigma, i = 1, k-1$, we have the following.

Lemma 5.10. *Let σ be the map defined in Equation* 5.1. *Then*

(i) $S_{2k} \cong$ (*a subgroup of*) $\mathrm{Aut}(\Gamma(2k, k, i)/\sigma), i = 1, k-1$.

(ii) $\mathrm{Aut}(\Gamma(2k, k, i)/\sigma), i = 1, k-1$ *is vertex-transitive.*

Proof. (i) Let $X = \{A, B\} \in V(\Gamma(2k, k, i)/\sigma)$. The symmetric group S_{2k} acts on $V(\Gamma(2k, k, i)/\sigma)$ by $\theta(X) = \{\theta(A), \theta(B)\}$, where $\theta \in S_{2k}$. Moreover θ preserves the size of intersections. Hence $S_{2k} \cong$ (a subgroup of) $\mathrm{Aut}(\Gamma(2k, k, i)/\sigma), i = 1, k-1$.

(ii) Let $\{\{a_1, a_2, \ldots, a_k\}, \{b_1, b_2, \ldots, b_k\}\}, \{\{a'_1, a'_2, \ldots a'_k\}, \{b'_1, b'_2, \ldots, b'_k\}\}$ $\in V(\Gamma(2k, k, i)/\sigma)$. Then the permutation $\alpha = \begin{pmatrix} a_1 & a_2 & \cdots & a_k & b_1 & b_2 & \cdots & b_k \\ a'_1 & a'_2 & \cdots & a'_k & b'_1 & b'_2 & \cdots & b'_k \end{pmatrix}$ takes $\{\{a_1, a_2, \ldots, a_k\}, \{b_1, b_2, \ldots, b_k\}\}$ to $\{\{a'_1, a'_2, \ldots, a'_k\}, \{b'_1, b'_2, \ldots, b'_k\}\}$ and hence S_{2k} acts transitively on $\Gamma(2k, k, i)/\sigma, i = 1, k-1$. □

We now determine the automorphism group of $\Gamma(2k, k, i)/\sigma, i = 1, k-1$.

Theorem 5.11. $\mathrm{Aut}(\Gamma(2k, k, i)/\sigma) \cong S_{2k}$.

Proof. Let $X = \{\{1, 2, \ldots, k\}, \{k+1, k+2, \ldots, 2k\}\}$. Since the graph $\Gamma(2k, k, i)/\sigma$ is vertex-transitive, to determine the order of the group, by the orbit-stabilizer theorem, it is sufficient to determine the order of the stabilizer $\mathrm{Stab}(X)$ of X.

Set $A = \{1,2,\ldots,k\}, B = \{k+1,k+2,\ldots,2k\}$. Let $i \in A$ and $j \in B$. Then the set C_i of vertices of the form $C_i = \{\{i\} \cup (B \setminus \{j\}), (A \setminus \{i\}) \cup \{j\}\}$ defines a distinct clique for each fixed $i \in A$ in $\Gamma(2k,k,i)/\sigma$. Hence there is a 1-1 correspondence between the set of cliques $C = \{C_i : i = 1,2,\ldots,k\}$ and A.

Now any automorphism in $\mathrm{Stab}(X)$ that fixes $C = \{C_i : i = 1,2,\ldots,k\}$ induces a permutation of S_A.

Similarly the set D_j of k vertices of the form $D_j = \{\{j\} \cup (A \setminus \{i\}), (B \setminus \{j\}) \cup \{i\}\}$ defines a distinct clique for each fixed $j \in B$ in $\Gamma(2k,k,i)/\sigma$. By a similar argument any automorphism that fixes $D = \{D_i : i = k+1,k+2,\ldots,2k\}$ induces as well a permutation of S_B.

It is easy to see that any automorphism in $\mathrm{Stab}(X)$ must either fix cliques in C or interchange them with those in D. Hence $|\mathrm{Stab}(X)| = 2(k!)(k!)$.

Now, since $\Gamma(2k,k,i)/\sigma)$ has $\dfrac{(2k)!}{2(k)!(k)!}$ vertices then $|\mathrm{Aut}(\Gamma(2k,k,i)/\sigma))| = (2k)!$ So, in view of Lemma 5.10 $\mathrm{Aut}(\Gamma(2k,k,i)/\sigma) \cong S_{2k}$. □

Theorem 5.12. $\mathrm{Aut}(\Gamma(2k,k,i)) \cong S_{2k} \times S_2, i = 1, k-1$.

Proof. $\mathrm{Fix}(\Gamma(2k,k,i),f) \cong S_2, i = 1, k-1$ and by Theorem 5.8 the result follows. □

Now that we have looked at the automorphism group of $\Gamma(2k,k,i), i = 1, k-1$, we turn to the determination of the codes generated by the graph $\Gamma(2k,k,1)$.

As alluded to Chapter 2, Section 2.8, these graphs as constructed by Key and Moori method has the maximal subgroup $S_k \times S_k$ acting on the set Ω of size $2k$.

Chapter 6

Codes from maximal subgroups of alternating group A_{2k}

6.1 Introduction

In this chapter, we focus on the graphs, codes and design from maximal subgroups of alternating group A_{2k}.

We look at primitive action of the alternating group A_{2k} on $\Omega^{\{k\}}$, the k-subsets of $\Omega = \{1, 2, \ldots, 2k\}$. The alternating group A_{2k} where $k \geq 2$, acts transitively on $\Omega^{\{k\}}$. In view of this fact, it is enough to consider the stabilizer of the subset $\{1, 2, \ldots, k\}$. It is observed that the stabilizer is $S_k \times A_k$. Since the stabilizer is maximal in A_{2k}, the action of the group is primitive. According to Theorem 2.45, in Chapter 2, the maximal subgroups are known to be of the form $S_k \times S_k$.

We construct the permutation group, then form the orbits of the stabilizer of k-subset from Ω. For each of the non-trivial orbits we formed the symmetric 1-design as described in Theorem 2.46 in Chapter 2. Because of the maximality of the point stabilizer, there is only the one orbit of length 1.

The graphs obtained in this enterprise are the uniform subset graphs $\Gamma(2k, k, i)$ for $0 \leq i \leq k-1$. Specifically, we focus on the codes from adjacency matrices of the sub-class $\Gamma(2k, k, k-1)$ of the Johnson graph and the uniform subset graph $\Gamma(2k, k, 1)$. We show that these graphs are non-isomorphic but the corresponding codes from the row span of their adjacency matrices coincide.

Having determined the properties of $\Gamma(2k,k,k-1)$ and $\Gamma(2k,k,1)$, in turn, we focus on the binary code generated by adjacency matrices of $\Gamma(2k,k,1)$ and $\Gamma(2k,k,k-1)$. We show that adjacency matrices of $\Gamma(2k,k,1)$ and $\Gamma(2k,k,k-1)$ are equivalent.

The code from $\Gamma(2k,k,1)$ is also the code of the 1-$\left(\binom{2k}{k},k^2,k^2\right)$ design $\mathcal{D}$, which has the vertices of $\Gamma(2k,k,1)$ and the supports of the incidence vectors of its adjacency matrix as its point set $\mathcal{P}$ and its block set $\mathcal{B}$ respectively. We determine a basis for the code and show that it is equal to a basis for the code generated by an adjacency matrix of $\Gamma(2k,k,k-1)$. Hence the codes generated from the row span coincide. We further prove a general case that the codes generated by an adjacency matrix of $\Gamma(2k,k,i)$ and of $\Gamma(2k,k,k-i)$ for $i \neq 0, \frac{k}{2}$ coincide.

This chapter is organised as follows: In Section 6.2, we show that adjacency matrices of $\Gamma(2k,k,1)$ and $\Gamma(2k,k,k-1)$ are equivalent and hence the codes from the row span of their adjacency matrices coincide. We further give a proof of the general case.

Pertinent pertinent properties of the graphs $\Gamma(2k,k,1)$ and $\Gamma(2k,k,k-1)$ are given already in Chapter 5 and codes from the Johnson graph $\Gamma(2k,k,k-1)$ have been investigated in [29].

We start by stating a result which identifies isomorphic uniform subset graphs and from which we can deduce that $n \geq 2k$. The proof can be found in [28].

Result 6.1. [28, Lemma 4.1.1] *For* $n \geq k \geq i, \Gamma(n,k,i) \cong \Gamma(n,n-k,n-2k+i)$.

In $\Gamma(2k,k,1)$ and $\Gamma(2k,k,k-1)$ the size of the intersection between two vertices as k-sets determines their distance. This in turn determines the eccentricities of the vertices and the diameters of the graphs.

Result 6.2. [16, Lemma 3] *Let* $\Gamma(2k,k,1)$ *be a uniform subset graph with* $k \geq 5$. *Let* $u,v \in V(\Gamma(2k,k,1))$ *and* $|u \cap v| = m > 1$. *Then*

$$\delta(u,v) = \min\left\{2\left\lceil\frac{k-m}{2}\right\rceil, 2\left\lceil\frac{m-1}{2}\right\rceil + 1\right\}. \tag{6.1}$$

Result 6.3. [17, Lemma 2] *Let k, i, s be positive integers with $k > i$. Let $\Gamma(n, k, i)$ be a uniform subset graph with $n = 2k - i + s$. Let $\mathcal{V}$ denote the set of all the pairs (u, v) with $u, v \in V(\Gamma(n, k, i))$ and $|u \cap v| > i$. Then*

$$\max_{(u,v)\in\mathcal{V}} \delta(u,v) = \begin{cases} \lceil \frac{k-i-1}{i+s} \rceil + 1 & \text{if } 0 < s < k - 2i - 1; \\ 2 & \text{otherwise.} \end{cases} \tag{6.2}$$

Result 6.4. [17, Theorem 4] *Let k, i, s be positive integers with $k > i$. Let $\Gamma(n, k, i)$ be a uniform subset graph with $n = 2k - i + s$. Then*

$$\operatorname{diam}(\Gamma(n,k,i)) = \begin{cases} \lceil \frac{k-i-1}{i+s} \rceil + 1 & \text{if } k \geq s + 2i + 2; \\ 2 & \text{if } s \geq i \text{ and } 2i \leq k \leq i + s, \\ & \text{or } s < i \text{ and } i + s \leq k \leq 2i; \\ 3 & \text{otherwise.} \end{cases} \tag{6.3}$$

Result 6.5. [28, Lemma 7.1.1, p. 83] *Let u and v be vertices of the Johnson graph $\Gamma(2k, k, k-1)$. Then for $m \geq 0$,*

$$\delta(u, v) = m \text{ if and only if } |u \cap v| = k - m. \tag{6.4}$$

From Result 6.5 we can easily see that the diameter of the Johnson graph $\Gamma(2k, k, k-1)$ is k, and two vertices u and v are at a distance k if and only if they are disjoint.

From the foregoing, we have the following.

Theorem 6.6. *Let k, i, s be positive integers with $k > i$. Let $\Gamma(n, k, i)$ be a uniform subset graph with $n = 2k - i + s$. Let $\Gamma_i = \Gamma(2k, k, i)$ and $\Gamma_{k-i} = \Gamma(2k, k, k-i)$ for $i \neq 0, \frac{k}{2}$ with $k \geq 4$ and $k \geq s + 2i + 2$. Then $\Gamma_i \ncong \Gamma_{k-i}$.*

Proof. From Results 6.4 and 6.5 $\operatorname{diam}(\Gamma_i) \neq \operatorname{diam}(\Gamma_{k-i})$, and the result follows. □

In general the uniform subset graphs $\Gamma(2k, k, i)$ and $\Gamma(2k, k, k-i)$ are non isomorphic for $i \neq 0, \frac{k}{2}$. There are cases when $k < s + 2i + 2$ in Lemma 6.4 where the diameters of non-isomorphic graphs $\Gamma(2k, k, i)$ and $\Gamma(2k, k, k-i)$ coincide. We use Magma [10] to confirm this observation.

6.2 Binary codes from the uniform subset graphs $\Gamma(2k, k, 1)$ and $\Gamma(2k, k, k-1)$

We now state the following results which give the parameters for the binary code generated by an adjacency matrix of the Johnson graph $\Gamma(n, k, k-1)$ for n even. These results and their proofs can be found in [28] and [29].

Let C_1 denote the binary code from the row span of an adjacency matrix of the Johnson graph $\Gamma(n, k, k-1)$ and $C_1^{\perp}$ its dual.

Result 6.7. [29, Lemma 3.1] *If $k \geq 3$ is odd and $n \geq 6$ is even, then $C_1 = \mathbb{F}_2^{\binom{n}{k}}$, and* $\mathrm{Aut}(C_1) = S_{\binom{n}{k}}$.

Result 6.8. [29, Proposition 3.4] *If $k \geq 2$ and $n \geq 6$ are both even, then C_1 is an $[\binom{n}{k}, \binom{n-2}{k-1}, d]_2$ code where $k+2 \leq d \leq k(n-k)$, and $C_1^{\perp}$ is an $[\binom{n}{k}, \binom{n}{k} - \binom{n-2}{k-1}, k+1]_2$ code. If $n > 2k$, then $C_1^{\perp}$ does not have a basis of minimum weight vectors. $C_1 \subseteq C_1^{\perp}$ and C_1 is doubly-even. If $n > 2k$, then* $\mathrm{Aut}(C_1) = S_n$, *except when $k = 2$ and $n = 6$, in which case* $\mathrm{Aut}(C_1) = PGL_4(2) \cong A_8$. *If $n = 2k$, then* $\mathrm{Aut}(C_1) = S_n \times Z_2$.

We now discuss the binary code from an adjacency matrix of the uniform subset graph $\Gamma(2k, k, 1)$.

Using the method of construction described in Chapter 2, Equation 2.5, we take $\mathcal{P} = \Omega^{\{k\}}$ as the point set. Each $X \in \Omega^{\{k\}}$ has a block $\overline{X}$ corresponding to it. The block is defined by

$$\overline{X} = N(X) = \{Y \in \Omega^{\{k\}} : |Y \cap X| = 1\}.$$

The block set $\mathcal{B}$ is given by

$$\mathcal{B} = \{\overline{X} : X \in \Omega^{\{k\}}\},$$

and the incidence vector of the block $\overline{X}$ by

$$v^{\overline{X}} = \sum_{\substack{x \in X \\ X' \subseteq \complement X, |X'| = k-1}} v^{\{x\} \cup X'} \tag{6.5}$$

where $\complement X = \Omega \setminus X$.

The incidence vector $v^{\overline{X}}$ is the mapping

$$v^{\overline{X}} : \Omega^{\{k\}} \to \mathbb{F}_2, Y \mapsto v^{\overline{X}}(Y) = \begin{cases} 1 & \text{if } |Y \cap X| = 1 \\ 0 & \text{if } |Y \cap X| \neq 1 \end{cases}.$$

Hence for $Y \in \Omega^{\{k\}}$, we have $v^{\overline{X}}(Y) = 1$ if and only if $|Y \cap X| = 1$.

Let C_2 denote the binary code from the row span of an adjacency matrix of $\Gamma(2k,k,1)$.

Lemma 6.9. *If $k \geq 3$ is odd, then $C_2 = \mathbb{F}_2^{\binom{2k}{k}}$ and* $\mathrm{Aut}(C_2) = S_{\binom{2k}{k}}$.

Proof. Let $X \in \Omega^{\{k\}}$. It is sufficient to show that the unit vector v^X is in C_2. Consider the set of all incidence vectors $\{v^{\overline{Y}} : Y \in \Omega^{\{k\}}, |Y \cap X| = 1\}$, and in particular the sum, $\sum_{|Y \cap X|=1} v^{\overline{Y}}$ of such vectors.

The above sum reduces to

$$k^2 v^X + (2k-2) \sum_{\substack{x \in \complement X \\ X' \subseteq X, |X'|=k-1}} v^{\{x\} \cup X'}$$

$$+4 \sum_{\substack{\{x,x'\} \subseteq \complement X \\ X' \subseteq X, |X'|=k-2}} v^{\{x,x'\} \cup X'}.$$

Since k is odd,

$$\sum_{|Y \cap X|=1} v^{\overline{Y}} = v^X.$$

Clearly, $\mathrm{Aut}(C_2) = S_{\binom{2k}{k}}$. □

Lemma 6.10. *Let $\Omega = \{1,2,\ldots,2k\}$. If $k \geq 2$ is even, then $S := \{v^{\overline{X}} : 1 \in X, 2k \notin X\}$ is a basis for C_2 and* $\dim(C_2) = \binom{2k-2}{k-1}$.

Proof. For $X, Y \in \Omega^{\{k\}}$, if Y is adjacent to X, then $v^{\overline{X}}$ has a non-zero entry in the column indexed by Y.

If $1 \in X$ and $2k \notin X$, then such columns are indexed by the set $\{1\} \cup (\complement X \setminus \{2k\})$, the sets $\{1, 2k\} \cup X''$, where $X'' \subseteq \complement X \setminus \{2k\}$ with $|X''| = k-2$, and the sets $\{x\}\cup X'$, where $x\in X\setminus\{1\}$ and $X'\subseteq \complement X$ with $|X'|=k-1$. For $x\in X, x\neq 1$, it can easily be verified that

$$\sum_{\substack{X'=X\setminus\{x\}\\ x'\in\complement X'\setminus\{2k\}}} v^{\overline{X'\cup\{x'\}}} = v^{\overline{(X\cup\{2k\})\setminus\{x\}}}.$$

If $1\notin X$, then such columns are indexed by the sets $\{1,x\}\cup X'$, where $x\in X$, $X'\subseteq\complement X\setminus\{1\}$ with $|X'|=k-2$, and the sets $\{x\}\cup X''$, where $x\in X$ and $X''=\complement X\setminus\{1\}$. Again it can be verified that

$$\sum_{\substack{X'\subseteq X\\ |X'|=k-1}} v^{\overline{\{1\}\cup X'}} = v^{\overline{X}}.$$

This shows that $S:=\{v^{\overline{X}}:1\in X, 2k\notin X\}$ spans C_2.

When the vectors of S are written in lexicographic order and the points of $\Omega^{\{k\}}$ are arranged by placing first the points

$\{1,2,\ldots,k\},\{1,2,\ldots,k-1,k+1\},\ldots,\{1,2,\ldots,k-1,2k-1\},\{1,2,\ldots,k-2,k,k+1\},\ldots,\{1,2,\ldots,k-2,k,2k-1\},\ldots,\{1,k+1,k+2,\ldots,2k-1\}$

in reverse order, followed by the remaining points of $\Omega^{\{k\}}$ in arbitrary order, then a matrix of the form $[I_{\binom{2k-2}{k-1}}|A]$ results.

Hence S is a basis for C_2 and clearly $\dim(C_2)=\binom{2k-2}{k-1}$. □

We now give the main result.

Theorem 6.11. *Let C_1 denote the binary code from the row span of an adjacency matrix of the Johnson graph $\Gamma(2k,k,k-1)$ and C_2 denote the binary code from the row span of an adjacency matrix of the graph $\Gamma(2k,k,1)$. Then $C_1=C_2$.*

Proof. In the proof of Result 6.8 (see [29, Lemma 3.4]) it had been shown that S is a basis for C_1. So by Results 6.7 and 6.8 and Lemmas 6.9 and 6.10 we conclude that $C_1=C_2$. □

We further analyse adjacency matrices of the two graphs $\Gamma(2k,k,i)$ and $\Gamma(2k,k,k-i)$. It has been observed that the two matrices are equivalent by the row operation as given in the following theorem.

Theorem 6.12. *Let k, i be non-negative integers, $k > i, k \geq 2$. Let A_i and A_{k-i} be adjacency matrices of the non-isomorphic uniform subset graphs $\Gamma(2k,k,i)$ and $\Gamma(2k,k,k-i)$ respectively for $i \neq 0, \frac{k}{2}$, where the columns of A_i and A_{k-i} have the same order. Then $A_i \sim A_{k-i}$.*

Proof. The row operation $R_X^{A_i} \to R_{\widehat{X}}^{A_{k-i}}$ for the rows which are indexed by X and $\widehat{X}$ respectively for $X \in \Omega^{\{k\}}$, $\widehat{X} = \Omega \setminus X$, shows that the two matrices are equivalent. □

From Theorem 6.12 above, we have the following result.

Theorem 6.13. *Let C_i and C_{k-i} be the binary codes generated by the row span of adjacency matrices of the the non-isomorphic uniform subset graphs $\Gamma(2k,k,i)$ and $\Gamma(2k,k,k-i)$ respectively for $i \neq 0, \frac{k}{2}$. Then $C_i = C_{k-i}$.*

Proof. This is a direct consequence of Theorem 6.12. □

In the next chapter, we now consider codes from an adjacency matrix of the generalised uniform subset graph $\Gamma(2k,k,\{1,k-1\})$ as defined in Definition 2.22, Chapter 2.

Chapter 7

Codes from the generalised uniform subset graphs $\Gamma(2k, k, \{1, k-1\})$

7.1 Introduction

A key motivation for this chapter is the work done by Fish, Mwambene and Key in [39]. They considered codes from the row span of an adjacency matrix from the graph formed from the Odd graph and the Johnson graph for the case $n = 2k + 1$.

In this chapter we take a similar tweak on the construction of codes from adjacency matrices. In Chapter 6, by exploring the intrinsic properties of the graphs $\Gamma(2k, k, 1)$, it becomes apparent that these graphs are non-isomorphic to the Johnson graphs $\Gamma(2k, k, k-1)$ but their adjacency matrices generate equal codes. We now focus on codes from the row span of an adjacency matrix A, of a generalised uniform subset graph $\Gamma(2k, k, \{1, k-1\})$.

Having determined the properties of the new graph, i.e $\Gamma(2k, k, \{1, k-1\})$, in turn, we focus on the binary code generated by the row span of its adjacency matrix. We determine a basis for the new code. We also determine its minimum weight and show that it is equal to twice the minimum weight of the code from $\Gamma(2k, k, k-1)$. The results obtained are interesting in coding theory as it shows that we can generalise graphs to produce a graph that generates a code that has double the minimum weight of the original code while maintaining the length with half or less the size of the basis.

The main results are summarised in Theorem 7.1.

Theorem 7.1. *Let k be a positive integer where $2k \geq 4$. Let C denote the binary code from the row span of an adjacency matrix of the generalised uniform subset graphs $\Gamma(2k, k, \{1, k-1\})$ and $C^{\perp}$ its dual. Then the following hold:*

(a) *For $k \geq 5$ odd, C is a $[\binom{2k}{k}, \binom{2k-1}{k-1}, 2]_2$-code, and its dual $C^{\perp}$ is a $[\binom{2k}{k}, \binom{2k-1}{k-1}, 2]_2$-code. Furthermore, C is self-dual.*

(b) *For $k \geq 4$ even, C is a $[\binom{2k}{k}, \binom{2k-3}{k-2} - 2^{k-2}, 2k^2]_2$-code, and its dual $C^{\perp}$ is a $[\binom{2k}{k}, \binom{2k}{k} - \binom{2k-3}{k-2} + 2^{k-2}, 2]_2$-code.*

This chapter is organised as follows: In Section 7.2 pertinent properties of the generalised graphs $\Gamma(2k, k, \{1, k-1\})$ are given. We further prove the specific parameters for the code.

7.2 Some properties of the generalised uniform subset graphs $\Gamma(2k, k, \{1, k-1\})$

It is easy to see that a generalised uniform subset graph $\Gamma(2k, k, \{1, k-1\})$ f is regular with $\binom{2k}{k}$ vertices and its valency is $2k^2$. In general, these graphs are not strongly regular.

The codes from the graphs $\Gamma(2k, k, k-1)$ are the content of [29] and codes from the graphs $\Gamma(2k, k, 1)$ have been considered in [42].

As alluded to, S_n in its natural action imbeds into the automorphism group of uniform subset graphs $\Gamma(n, k, i)$ in the same way as described in Chapter 6.

7.3 Binary codes from the generalised uniform subset graphs $\Gamma(2k, k, \{1, k-1\})$

We first state the following results which give the parameters for the binary code generated by an adjacency matrix of the Johnson graph $\Gamma(n, k, k-1)$ for n even and that for $\Gamma(2k, k, 1)$. These results and their proofs can be found in [28] and [29].

Let C_1 and C_2 denote the binary codes from the row span of adjacency matrices of the graphs $\Gamma(n, k, k-1)$ and $\Gamma(2k, k, 1)$ respectively, and $C_1^{\perp}$ and $C_2^{\perp}$ their duals.

For convenience we again give the following results which are stated in 6.

Result 7.2. [29, Lemma 3.1] *If* $k \geq 3$ *is odd and* $n \geq 6$ *is even, then* $C_1 = \mathbb{F}_2^{\binom{n}{k}}$, *and* $\mathrm{Aut}(C_1) = S_{\binom{n}{k}}$.

Result 7.3. [29, Proposition 3.4] *If* $k \geq 2$ *and* $n \geq 6$ *are both even, then* C_1 *is an* $[\binom{n}{k}, \binom{n-2}{k-1}, d]_2$ *code where* $k+2 \leq d \leq k(n-k)$, *and* $C_1^{\perp}$ *is an* $[\binom{n}{k}, \binom{n}{k} - \binom{n-2}{k-1}, k+1]_2$ *code. If* $n > 2k$, *then* $C_1^{\perp}$ *does not have a basis of minimum weight vectors.* $C_1 \subseteq C_1^{\perp}$ *and* C_1 *is doubly-even. If* $n > 2k$, *then* $\mathrm{Aut}(C_1) = S_n$, *except when* $k = 2$ *and* $n = 6$, *in which case* $\mathrm{Aut}(C_1) = PGL_4(2) \cong A_8$. *If* $n = 2k$, *then* $\mathrm{Aut}(C_1) = S_n \times Z_2$.

Result 7.4. [81, Theorem 5] *Let* C_1 *and* C_2 *denote the binary codes from the row span of adjacency matrices of the Johnson graph* $\Gamma(n, k, k-1)$ *and the uniform subset graph* $\Gamma(2k, k, 1)$ *respectively. Then* $C_1 = C_2$.

We also state the following result which gives the parameters for the binary code generated by the row span of an adjacency matrix of the Odd graph $\Gamma(2k+1, k, 0)$ $(\mathcal{O}_k)$ and the Johnson graph $\Gamma(2k+1, k, k-1)$ (J_k). This graph is a graph $\Gamma(2k+1, k, i)$ for $i \in \{0, k-1\}$. The given results and their proofs can be found in [39].

Let OJ_k denote a graph formed from a combination of the Odd graph $\Gamma(2k+1, k, 0)$ and the Johnson graph $\Gamma(2k+1, k, k-1)$.

Result 7.5. [39, Theorem 1] *For* $k \geq 2$, *let* A_k *be an adjacency matrix for the odd graph* $\mathcal{O}_k$ *and* M_k *an adjacency matrix for* OJ_k. *Let* $I = I_{\binom{2k+1}{k}}$ *and*

$C = C_2(A_k + I)$, the row span over $\mathbb{F}_2$ of $A_k + I$. Then C is a

$$\left[\binom{2k+1}{k}, \binom{2k}{k-1} + \binom{2k-1}{k-1} - 2^{k-1}, k+2\right]_2$$

code with at least $\binom{2k+2}{k}$ vectors. $C^{\perp}$ is an even-weight code with minimum weight $d^{\perp}$, where $k+4 \leq d^{\perp} \leq \min\{2^k, (k+1)^2+1\}$ for k even, and $k+5 \leq d^{\perp} \leq \min\{2^k, (k+1)^2\}$ for k odd. Furthermore, for $k \geq 3$

$$\mathrm{Hull}(C) = C \cap C^{\perp} = \begin{cases} C_2(M_k) & \text{for } k \text{ odd} \\ C_2(M_k + I) & \text{for } k \text{ even} \end{cases},$$

of dimension $\binom{2k-1}{k-1} - 2^{k-1}$. For k even (respectively odd), M_k (respectively $M_k + I$), has full 2-rank. Hull(C) *is self-orthogonal with minimum weight d where $(k+1)^2 + 1 \geq d \geq k+4$ for k even, $(k+1)^2 \geq d \geq k+5$ for k odd.*

If s_x denotes the row of $A_k + I$ labelled by the vertex x, then the hull is spanned by the vectors $w_x = \sum_{y \sim x} s_y$, which give the corresponding rows of M_k, of weight $(k+1)^2$, for k odd, or rows of $(M_k + I)$, of weight $(k+1)^2 + 1$, for k even, where $\sim$ denotes adjacency in $\mathcal{O}_k$.

For $k \geq 3$, the symmetric group S_{2k+2} acts as a primitive automorphism group of OJ_k, C and Hull(C), *and is edge-transitive on OJ_k. For $k = 4$,* Hull$(C)^{\perp}$ *is the code of a 2-$(126, 6, 9)$ design on which S_{10} acts primitively on points, transitively on blocks.*

We now discuss the binary code from an adjacency matrix of the generalised uniform subset graph $\Gamma(2k, k, \{1, k-1\})$.

Recall from Chapter 6, Equation 6.5, the incidence vector of the block $\widetilde{X}$ associated with the design from the graph $\Gamma(2k, k, 1)$ is given by

$$v^{\widetilde{X}} = \sum_{\substack{x \in X \\ X' \subseteq \complement X, |X'| = k-1}} v^{\{x\} \cup X'} \tag{7.1}$$

where $\complement X = \Omega \setminus X$.

Similarly, the incidence vector of the block $\widehat{X}$ associated with the design from the graph $\Gamma(2k, k, 1)$ is given by

$$v^{\widehat{X}} \;=\; \sum_{\substack{X' \subseteq X, |X'|=k-1 \\ x \in \complement X}} v^{\{x\}\cup X'}. \tag{7.2}$$

Hence the incidence vector of the block $\overline{X}$ of the design formed from the generalised uniform subset graph $\Gamma(2k, k, i)$ for $i \in \{1, k-1\}$ is given by

$$v^{\overline{X}} = \sum_{\substack{x \in X \\ X' \subseteq \complement X, |X'|=k-1}} v^{\{x\}\cup X'} \;+\; \sum_{\substack{X' \subseteq X, |X'|=k-1 \\ x \in \complement X}} v^{\{x\}\cup X'}. \tag{7.3}$$

Let A be an adjacency matrix of the generalised uniform subset graph $\Gamma(2k, k, \{1, k-1\})$ and C denote the binary code generated by the row span of A.

Lemma 7.6. *Let* $\Omega = \{1, 2, \ldots, 2k\}$. *If* $k \geq 5$ *is odd, then* $S := \{v^{\overline{X}} : 1 \in X\}$ *is a basis for* C *and* $\dim(C) = \binom{2k-1}{k-1}$.

Proof. For $X, Y \in \Omega^{\{k\}}$, if Y is adjacent to X, then $v^{\overline{X}}$ has a non-zero entry in the column indexed by Y.

If $1 \notin X$, then such columns are indexed by the sets $\{1, x\} \cup X'$, where $x \in X$, $X' \subseteq \complement X \setminus \{1\}$ with $|X'| = k-2$, and the sets $\{x\} \cup X''$, where $x \in X$ and $X'' = \complement X \setminus \{1\}$. The remaining columns are indexed by the sets $\{x'\} \cup X'''$, where $X''' \subset X, x' \in \complement X$ with $|X'''| = k-1$. It can be verified that

$$\sum_{\substack{X' \subseteq X \\ |X'|=k-1}} v^{\overline{\{1\}\cup X'}} = v^{\overline{X}}.$$

This shows that $S := \{v^{\overline{X}} : 1 \in X\}$ spans C.

When the vectors of S are written in lexicographic order and the points of $\Omega^{\{k\}}$ are arranged by placing first the points

$\{1, 2, \ldots, k\}, \{1, 2, \ldots, k-1, k+1\}, \ldots, \{1, 2, \ldots, k-1, 2k\}, \{1, 2, \ldots, k-2, k, k+1\}, \ldots, \{1, 2, \ldots, k-2, k, 2k\}, \ldots, \{1, k+2, k+3, \ldots, 2k\}$

followed by the remaining points of $\Omega^{\{k\}}$ in arbitrary order, there is a one-to-one correspondence between these points that have intersection one.

Hence, a triangular matrix with ones on the main diagonal results. We can reduce the matrix to the diagonal case, whereby a matrix of the form $[I_{\binom{2k-1}{k-1}}|A]$ results through some elementary row operations. Hence S is a basis for C and $\dim(C) = \binom{2k-1}{k-1}$.

□

Lemma 7.7. *Let $\Omega = \{1, 2, \ldots, 2k\}$. If $k \geq 5$ is odd, then C has minimum weight 2.*

Proof. Let $X_1, X_2 \in \Omega^{\{k\}}$. It is sufficient to show that the weight 2 vector $v^{X_1} + v^{X_2}$ is in C_2. Consider the set of all incidence vectors $\{v^{\overline{Y}} : Y \in \Omega^{\{k\}}, |Y \cap X_1| = 1 \text{ and } |Y \cap X_2| = k-1\}$, and in particular the sum, $\sum_{\substack{|Y\cap X_1|=1\\|Y\cap X_2|=k-1}} v^{\overline{Y}}$ of such vectors.

The above sum reduces to

$$k^2 v^{X_1} + (2k-2) \sum_{\substack{x \in \complement X_1\\ X' \subseteq X_1, |X'|=k-1}} v^{\{x\}\cup X'} + 4 \sum_{\substack{\{x,x'\} \subseteq \complement X_1\\ X' \subseteq X_1, |X'|=k-2}} v^{\{x,x'\}\cup X'}$$
$$+ k^2 v^{X_2} + (2k-2) \sum_{\substack{x \in \complement X_2\\ X' \subseteq X_2, |X'|=k-1}} v^{\{x\}\cup X'} + 4 \sum_{\substack{\{x,x'\} \subseteq \complement X_2\\ X' \subseteq X_2, |X'|=k-2}} v^{\{x,x'\}\cup X'}.$$

Since k is odd,

$$\sum_{\substack{|Y\cap X_1|=1\\|Y\cap X_2|=k-1}} v^{\overline{Y}} \;=\; v^{X_1} + v^{X_2}.$$

Alternatively, in [29], it is shown that the code generated by an adjacency matrix of the Johnson graph $\Gamma(2k, k, k-1)$ for k odd is the full space and hence has minimum weight 1 according to Result 7.2. Using Result 7.4, we have the same scenario for the code generated by an adjacency matrix for the uniform subset graph $\Gamma(2k, k, 1)$. The same linear combinations that occur separately in the rows of the adjacency matrices of the graphs $\Gamma(2k, k, k-1)$ and $\Gamma(2k, k, 1)$ also occur in similar patterns in an adjacency matrix $A_1 + A_2$. Furthermore, the rows of $A_1 + A_2$ do not coincide at any point, hence the minimum weight of C is 2. □

Lemma 7.8. *Let* $\Omega = \{1, 2, \ldots, 2k\}$*. If* $k \geq 5$ *is odd, then* $R := \{v^{\overline{X}} : 1 \in X\}$ *is a basis for* $C^{\perp}$ *and* $\dim(C^{\perp}) = \binom{2k-1}{k-1}$*. Moreover* C *is self-dual.*

Proof. First consider the standard inner product $(v^{\overline{X}}, v^{\overline{X'}})$ of any two incidence vectors, where $v^{\overline{X}}$ is as defined in Equation 7.3. If $|X \cap X'| = k-1$, then $(v^{\overline{X}}, v^{\overline{X'}}) = 4k-4 \equiv 0 \pmod 2$. On the other hand if $|X \cap X'| = k-2$, then $(v^{\overline{X}}, v^{\overline{X'}}) = 8 \equiv 0 \pmod 2$. And finally if $|X \cap X'| < k-2$, then $(v^{\overline{X}}, v^{\overline{X'}}) = 0$. The standard inner product $(v^{\overline{X}}, v^{\overline{X'}}) = 0$ irrespective of whether $X \cap X' = \emptyset$ or not. Hence $C \subseteq C^{\perp}$.

By arranging the vectors of R in lexicographic order, and the points as follows: first the last $\binom{2k}{k} - \binom{2k-1}{k-1}$ points and then the first $\binom{2k-2}{k-1}$ points as ordered in the case of C above, an upper triangular matrix results, the rank of which is $\binom{2k-1}{k-1} = \binom{2k}{k} - \binom{2k-1}{k-1} = \binom{2k}{k} - \dim(C)$. It follows that R is a basis for $C^{\perp}$. Since $\dim(C) = \dim(C^{\perp})$, C is self-dual. □

Lemma 7.9. *Let* $\Omega = \{1, 2, \ldots, 2k\}$*. If* $k \geq 4$ *is even, then* $\dim(C) = \binom{2k-3}{k-2} - 2^{k-2}$*.*

Proof. For $X, Y \in \Omega^{\{k\}}$, if Y is adjacent to X, then $v^{\overline{X}}$ has a non-zero entry in the column indexed by Y.

If $1, 2, 2k \in X$ then such columns are indexed by the sets $\{1\} \cup X', \{2\} \cup X', \{2k\} \cup X', \{x'\} \cup X'$, where $X' \subseteq \complement X$ with $|X'| = k-1$ and $x' \in X \setminus \{1, 2, 2k\}$. The other columns are indexed by $\{x''\} \cup X''$ where $X'' \subset X$ and $x'' \in \complement X$ with $|X''| = k-1$. It can easily be verified that

$$\sum_{\substack{X'' \subseteq X \setminus \{1,2,2k\} \\ |X''| = k-2}} v^{\overline{\{1,2\} \cup X''}} = v^{\overline{X}}.$$

If $1, 2 \notin X$ and $2k \in X$, then such columns are indexed by the sets $\{2k\} \cup X', \{x'\} \cup X'$, where $X' \subseteq \complement X$ with $|X'| = k-1$ and $x' \in X \setminus \{2k\}$. The other columns are indexed by $\{x''\} \cup X''$ where $X'' \subset X$ and $x'' \in \complement X$ with $|X''| = k-1$. Again it can be verified that

$$\sum_{\substack{X'' \subseteq X \setminus \{1,2,2k\} \\ |X''| = k-2}} v^{\overline{\{1,2\} \cup X''}} = v^{\overline{X}}.$$

If $1,2,2k \notin X$, then such columns are indexed by the sets $\{x\}\cup X'$, where $x\in X, X'\subseteq \complement X$ with $|X'|=k-1$. The other columns are indexed by $\{x''\}\cup X''$ where $X''\subset X$ and $x''\in\complement X$ with $|X''|=k-1$. Similarly, it can be verified that

$$\sum_{\substack{X''\subseteq X\setminus\{1,2,2k\}\\ |X''|=k-2}} v^{\overline{\{1,2\}\cup X'}} = v^{\overline{X}}.$$

If $1\in X$ and $2,2k\notin X$, or if $2\in X$ and $1,2k\notin X$, the result is similar to the case if $1,2\notin X$ and $2k\in X$.

If $1,2k\in X$ and $2\notin X$, then such columns are indexed by the sets $\{1\}\cup X', \{2k\}\cup X', \{x'\}\cup X'$, where $X'\subseteq\complement X$ with $|X'|=k-1$ and $x'\in X\setminus\{1,2k\}$. The other columns are indexed by $\{x''\}\cup X''$ where $X''\subset X$ and $x''\in\complement X$ with $|X''|=k-1$. It can easily be verified that

$$\sum_{\substack{X''\subseteq X\setminus\{1,2,2k\}\\ |X''|=k-2}} v^{\overline{\{1,2\}\cup X''}} = v^{\overline{X}}.$$

If $2,2k\in X$ and $1\notin X$, we proceed with a similar argument as for the case if $1,2k\in X$ and $2\notin X$.

This shows that $S:=\{v^{\overline{X}}: 1,2\in X, 2k\notin X\}$ spans C_2.

We now arrange the incidence vectors of an adjacency matrix of the combined graph $\Gamma(2k,k,i)$ for $i\in\{1,k-1\}$ in lexicographic order and the points of $\Omega^{\{k\}}$ are arranged by placing first the points

$\{1,2,\ldots,k\},\{1,2,\ldots,k-1,k+1\},\ldots,\{1,2,\ldots,k-1,2k-1\},\{1,2,\ldots,k-2,k,k+1\},\ldots,\{1,2,\ldots,k-2,k,2k-1\},\ldots,\{1,k+1,k+2,\ldots,2k-1\},\ldots,\{k,k+1,k+2,\ldots,2k-1\}$,

followed by the points

$\{1,2,\ldots,k-1,2k\},\{1,2,\ldots,k-2,k,2k\},\ldots,\{1,2,\ldots,k-2,2k-1,2k\},\{1,2,\ldots,k-3,k-1,k,2k\},\ldots,\{1,2,\ldots,k-3,2k-2,2k-1,2k\},\ldots,\{1,k+2,k+3,\ldots,2k\},\ldots,\{k+1,k+2,k+3,\ldots,2k\}$.

For a better analysis we break up this adjacency matrix of $\Gamma(2k,k,i)$ for $i\in\{1,k-1\}$ in the following equivalent way:

$$\boldsymbol{A}_{\Gamma(2k,k,i)} = \left[\begin{array}{c|c} \boldsymbol{A}_{\Gamma(2k-1,k,i)} & \boldsymbol{B}_{\Gamma(2k-1,k,k-1,i)} \\ \hline \boldsymbol{B}_{\Gamma(2k-1,k-1,k,i)} & \boldsymbol{A}_{\Gamma(2k-1,k-1,i)} \end{array}\right], \qquad (7.4)$$

where

(a) $\boldsymbol{A}_{\Gamma(2k-1,k,i)}$ is an adjacency matrix of the combined uniform subset graph $\Gamma(2k-1, k, i)$, for $i \in \{1, k-1\}$ and is a matrix of order $\binom{2k-1}{k} \times \binom{2k-1}{k}$.

(b) $\boldsymbol{B}_{\Gamma(2k-1,k,k-1,i)}$ is a biadjacency matrix of the bipartite graph $\Gamma(2k-1, k, k-1, i)$, for $i \in \{1, k-1\}$ and is a matrix of order $\binom{2k-1}{k} \times \binom{2k-1}{k-1}$.

(c) $\boldsymbol{B}_{\Gamma(2k-1,k-1,k,i)}$ is a biadjacency matrix of the bipartite graph $\Gamma(2k-1, k-1, k, i)$, for $i \in \{1, k-1\}$ and is a matrix of order $\binom{2k-1}{k-1} \times \binom{2k-1}{k}$.

(d) $\boldsymbol{A}_{\Gamma(2k-1,k-1,i)}$ is an adjacency matrix of a combined uniform subset graph $\Gamma(2k-1, k-1, i)$, for $i \in \{0, k-2\}$ and is a matrix of order $\binom{2k-3}{k-1} \times \binom{2k-3}{k-1}$.

Note that $\Gamma(2k-1, k, i) \cong \Gamma(2k-1, k-1, i)$ for $i \in \{1, k-1\}$ and $i \in \{0, k-2\}$ respectively.

If we let $r = k-1, \Gamma(2k-1, k-1, i)$ for $i \in \{0, k-2\}$ becomes $\Gamma(2r+1, r, i)$ for $i \in \{0, r-1\}$ and this graph is called the OJ_r described in Result 7.5 extracted from [39]. The linear code generated by OJ_r has dimension $\binom{2r-1}{r-1} - 2^{r-1}$. Hence the code generated by an adjacency matrix of the combined $\Gamma(2k-1, k-1, i)$ for $i \in \{0, k-2\}$ has dimension $\binom{2k-3}{k-2} - 2^{k-2}$. By graph isomorphism the code generated by an adjacency matrix of the combined graph $\Gamma(2k-1, k, i)$ for $i \in \{1, k-1\}$ has dimension $\binom{2k-3}{k-2} - 2^{k-2}$.

If we consider the incidence vectors $S_1 := \{v^{\overline{X}} : 1 \in X\}$ that form the rows an adjacency matrix of the graph $\Gamma(2k-1, k-1, i)$ for $i \in \{0, k-2\}$, which is a subgraph of a graph $\Gamma(2k, k, i)$ for $i \in \{1, k-1\}$, they can be written as a linear combination of the vectors of $S := \{v^{\overline{X}} : 1, 2 \in X, 2k \notin X\}$. However $|S_1| > |S|$, hence $\dim(C) = \binom{2k-3}{k-2} - 2^{k-2}$.

□

Lemma 7.10. *Let* $\Omega = \{1, 2, \ldots, 2k\}$. *If* $k \geq 4$ *is even, then* C *has minimum weight* $2k^2$.

Proof. In [29], it is shown that the minimum weight of the code generated by an adjacency matrix for the Johnson graph $\Gamma(2k, k, k-1)$ is k^2 according to Result 7.3. Using Result 7.4, the proof follows by a similar argument to that used in the alternative part of the proof of Lemma 7.7. □

Lemma 7.11. *Let* $\Omega = \{1, 2, \ldots, 2k\}$. *If* $k \geq 4$ *is even, then* $C \subseteq C^{\perp}$.

Proof. First consider the standard inner product $(v^{\overline{X}}, v^{\overline{X'}})$ of any two incidence vectors, where $v^{\overline{X}}$ is as defined in Equation 7.3. If $|X \cap X'| = k-1$, then $(v^{\overline{X}}, v^{\overline{X'}}) = 4k - 4 \equiv 0 \pmod 2$. On the other hand if $|X \cap X'| = k-2$, then $(v^{\overline{X}}, v^{\overline{X'}}) = 8 \equiv 0 \pmod 2$. And finally if $|X \cap X'| < k-2$, then $(v^{\overline{X}}, v^{\overline{X'}}) = 0$. The standard inner product $(v^{\overline{X}}, v^{\overline{X'}}) = 0$ irrespective of whether $X \cap X' = \emptyset$ or not. Hence $C \subseteq C^{\perp}$. □

Chapter 8

Conclusion

In this thesis, the target has been to explore codes, graphs and design from maximal subgroups of alternating groups.

In that view, we looked at codes of the graphs $\Gamma(2k, k, 1)$. In the course, it was imperative that we look at the automorphism group of the graphs. We have determined the automorphism group of $\Gamma(2k, k, k-1)$ in addition to the question at hand, thereby addressing the conjecture of by Mark Ramras and Elizabeth Donovan in [85].

In order to determine the parameters of the graphs $\Gamma(2k, k, k-1)$, we needed to address the codes from biadjacency matrices of $\Gamma(2k, k, k+1, 1)$ and those of $\Gamma(2k+1, k, k+2, 1)$. As alluded in Chapters 3 and 4, these appear as sub-codes of the codes from $\Gamma(2k, k, 1)$.

As it turns out out, codes of the graphs $\Gamma(2k, k, 1)$ are equal to those of $\Gamma(2k, k, k-1)$. Surprisingly, the graphs in question are non-isomorphic. Their diameters are not even equal. We have generalised this phenomenon without actually fully determining the parameters.

In a twist of events, we also have determined codes of the generalised uniform subset graphs $\Gamma(2k, k, \{1, k-1\})$. It turns out that the minimum weights of the codes are a combination of the minimum weights of the code from $\Gamma(2k, k, 1)$ and those from $\Gamma(2k, k, k-1)$.

This is an interesting avenue for consideration. Whilst a lot has been done on the exploration of the codes of uniform subset graphs, the consideration of codes of generalised uniform subset graphs as done in Chapter 7 has been first been explored here.

Difficulties withstanding, we hope that generalised uniform subset graphs may provide codes with bigger minimum weights than those from traditional uniform subset graphs. This should be exploited further.

Appendix A

Computer programs

In this chapter we present some programs that were used to explore the codes and their parameters presented in this thesis.

A.1 Gordon bound

The program below is written in Python [26]. It calculates the Gordon bound (see Equation (2.4)) for the PD-set of a given linear code. They can be changed to calculate the Gordon bound for the PD-set of any code of one's interest.

```
From scipy import mod, ceil, product, floor

# Constants
n           = 5
length      = (n-1)*(n-1)*n/2.0  # length of code
dim         = n*(n-1)-1          # dimension of the codes
dist        = n-1                # minimum distance
r           = length - dim       # code redundancy
t           = int((dist-1)/2.0)  # number of correctable errors
errors      = range(t)           # range of correctable errors
fractions   = []

# The loop below calculates values of all fractions in the
# Gordon bound formula

for i in errors:
   num      = length - i
   den      = r-i
   fract    = num/den
   fractions.append(fract)
gordonbound = ceil(fractions[-1])

# Calculating Gordon bound
for i in range(1,len(fractions)):
   gordonbound = ceil(fractions[-i-1]*gordonbound)

# Gordon bound
print gordonbound
```

A.2 Codes from biadjacency matrices of a class of bipartite graphs

The Magma [10] program below examines the parameters of linear binary codes from biadjacency matrices of the bipartite graphs $\Gamma(2k, k, k+1, 1)$ considered in Chapter 3.

```
make_des:=function(n,r);
S := {1..n};
ss:=Subsets(S,r);
ss1:=Subsets(S,(r+1));
verts:=[i:i in ss1];
ss2:=[j:j in ss];

v:=#verts;
w:=#ss2;
blox:=[ ];
```

```
for j:=1 to w do
blok:= {};
a:=ss2[j];
for i:=1 to v do

b:=verts[i];

if #(a meet b) eq 1 then blok:=blok join {i};
end if;
end for;

blox:=Append(blox,blok);
end for;
des:=Design<1,v|blox>;
return des;
end function;

give_code:=function(n,r);
des1:=make_des(n,r);
code:=LinearCode(des1,GF(2));
return code;
end function;

dims:=Dimension(give_code(n,r));
min:=minimumweight(give_code(n,r));
Aut:=AutomorphismGroup(give_code(n,r));
```

A.3 Codes from biadjacency matrices of a class of bipartite graphs

The Magma [10] program below examines the parameters of linear binary codes from biadjacency matrices of the bipartite graphs $\Gamma(2k+1, k, k+2, 1)$

considered in Chapter 4.

```
make_des:=function(n,r);
S := {1..n};
ss:=Subsets(S,r);
ss1:=Subsets(S,(r+2));
verts:=[i:i in ss1];
ss2:=[j:j in ss];

v:=#verts;
w:=#ss2;
blox:=[ ];

for j:=1 to w do
blok:= {};
a:=ss2[j];
for i:=1 to v do

b:=verts[i];

if #(a meet b) eq 1 then blok:=blok join {i};
end if;
end for;

blox:=Append(blox,blok);
end for;
des:=Design<1,v|blox>;
return des;
end function;

give_code:=function(n,r);
des1:=make_des(n,r);
code:=LinearCode(des1,GF(2));
return code;
```

```
end function;

dims:=Dimension(give_code(n,r));
min:=minimumweight(give_code(n,r));
Aut:=AutomorphismGroup(give_code(n,r));
```

A.4 Codes from the uniform subset graphs

The Magma [10] program in this section investigates parameters of linear binary codes from the uniform subset graphs $\Gamma(2k, k, i)$ considered in Chapter 5.

```
>next vert:=function(a,n,r);
function> b:=a;
function> for i:=0 to r-1 do
function|for> if a[r-i] lt n-i then
function|for|if> for j:=0 to i do
function|for|if|for> b[r-i+j]:=a[r-i]+1+j;
function|for|if|for> end for;
function|for|if> break i;
function|for|if> else
function|for|if> end if;
function|for> end for;
function> return b;
function> end function;

>gen verts:=function(n,r);
function> a:=[1..r];
function> verts:=[a];
function> while a[1] ne n-r+1 do
function|while> a:=next vert(a,n,r);
function|while> verts:=Append(verts,a);
function|while> end while;
```

```
function> return verts;
function> end function;

> count verts:=function(n,r);
function> verts:=gen verts(n,r);
function> v:=#(gen verts(n,r));
function> return v;
function> end function;

> make des:=function(n,r,k);
function> verts:=gen verts(n,r);
function> v:=count verts(n,r);
function> blox:=[ ];
function> for i:=1 to v do
function|for> blok:= ;
function|for> a:=Seqset(verts[i]);
function|for> for j:=1 to v do
function|for|for> b:=Seqset(verts[j]);


function|for|for> if #(a meet b) eq k then
function|for|for|if> blok:=blok join j;
function|for|for|if> end if;
function|for|for> end for;
function|for> blox:=Append(blox,blok);
function|for> end for;
function> des:=Design<1,v|blox>;
function> return des;
function> end function;


give code:=function(n,r,k);
function> des1:=make des(n,r,k);
function> code:=LinearCode(des1,GF(2));
function> return code;
function> end function;
```

A.5 Automorphism groups of graph covers and uniform subset graphs

The Magma [10] program below examines the automorphism groups of distance preserving graph covers. We apply the technique to determine the automorphism groups of uniform subset graphs $\Gamma(2k, k, k-1)$ and $\Gamma(2k, k, 1)$. This has been addressed in Chapter 6

```
r:=8;
n:=2*r;
S := {1..n};
ss:=Subsets(S,r);

WD:={@@};
for A, B in ss do
if #(A meet B) eq 0 then;
Include(~WD,Setseq({A,B}));
end if;
end for;

V := WD;
E :=[];

for a, b in [1..#WD] do
w :={WD[a],WD[b]};

if (a ne b) and #(WD[a][1] meet WD[b][1]) eq 1  or #(WD[a][2] meet
WD[b][2]) eq 1 then
```

```
w :={WD[a],WD[b]};

Append(~E,w);
end if;
end for;

Edges:=SequenceToSet(E);
G:= Graph<V|Edges>;
Aut:=AutomorphismGroup(G);
O:=Order(Aut);
```

Bibliography

[1] B́. Andrásfai, *Graph Theory: Flows, Matrices*. New York: Taylor and Francis, 1991.

[2] R. Aravamudhan and B. Rajendran, On antipodal graphs, *Discrete Math.*, **49** (1984), 193–195.

[3] A. S. Asratian, T. M. J. Denley and R. Hggkvist *Bipartite graphs and their applications*. Cambridge: Cambridge University Press, Cambridge Tracts in Mathematics, 1998.

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

[5] R. Balakrishnan and K. Ranganathan, *A Textbook of Graph Theory*. New York: Springer-Verlag, 2000.

[6] L. D. Baumert, R. J. McEliece and G. Solomon, Decoding with mulipliers, *JPL Deep Space Network Progress Report 42-34,* (1976), 43–46.

[7] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*. Cambridge: Cambridge University Press, 1993.

[8] N. L. Biggs and A. T. White, Permutation Groups and Combinatorial Structures, *Cambridge University Press, London, Cambridge.*, **33**, (1979).

[9] J. A. Bondy and U. S. R. Murty, *Graph Theory*, Vol. 244, Graduate Texts in Mathematics, Springer, 2008.

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

[11] A. E. Brouwer and J. H. van Eijl, On the p-rank of the adjacency matrices of strongly regular graphs, *J. Algebraic Combin.*, **1** (1992), 329–346.

[12] A. E. Brouwer, Packing and covering of $\binom{k}{t}$-sets, in: A. Schrijver (ed.), *Packing and Covering in Combinatorics.* Amsterdam: Mathematical Centre Tracts 106, 89–97, 1979.

[13] P. J. Cameron and J. H. van Lint, *Designs, Graphs, Codes and their Links.* Cambridge: Cambridge University Press, 1991.

[14] A. H. Chan and R. A. Games, (n, k, t)-covering systems and error-trapping decoding, *IEEE Trans. Inform. Theory*, **IT-27** (1981), 643–646.

[15] B-L. Chen and K-W. Lih, Hamiltonian uniform subset graphs, *J. Combin. Theory Ser. B*, **42** (1987), 257–263.

[16] Y. Chen and Y. Wang, On the diameter of generalised Kneser graphs, *Discrete Math.*, **308** (2008), 4276–4279.

[17] Y. Chen and W. Wang, Diameters of uniform subset graphs, *Discrete Math.*, **308** (2008), 6645–6649.

[18] G. C. Clark, Jr. and J. B. Cain, *Error-correction for digital communications.* New York: Plenum Press, 1981.

[19] J. T. Coffey and R. M. Goodman, The complexity of information set decoding, *IEEE Trans. Inform. Theory*, **36** (1990), 1031–1037.

[20] R. T. Curtis, On graphs and codes, *Geom.Dedicata*, **41** (1992), 127–134.

[21] P. Dankelman, J. D. Key and B. G. Rodrigues, A characterisation of graphs by codes from their incidence matrices, *Electron. J. Combin.*, **20 (3)** (2013), # P18.

[22] ———, Codes incidence matrices of graphs, *Des. Codes Cryptogr.*, **68** (2013), 373–393.

[23] R. Diestel, *Graph Theory.* New York: Springer, 2005.

[24] J. D. Dixon and B. Mortimer, *Permutation Groups.* Graduate Texts in Mathematics, 1996.

[25] D. Ž. Djoković, Automorphisms of graphs and coverings, *J. Combin. Theory Ser. B*, **16** (1974), 243–247.

[26] A. Downey, J. Elkner and C. Meyers, *How to think like a computer scientist: Learning with Python.* Massachusetts: Green Tea Press, 2002.

[27] M. Farzan, Automorphisms of double covers of a graph, in: *Problèmes combinatoires et théorie des graphes*, Publ. CNRS 260, Paris 1976, pp. 137–138.

[28] W. Fish, Codes from uniform subset graphs and cycle products, Ph.D. Thesis, University of the Western Cape, 2007.

[29] ———, Binary Codes and Partial Permutation Decoding Sets from the Johnson Graphs, *Graphs Combin.*, **31** (2015), 1381–1396.

[30] W. Fish, R. Fray and E. Mwambene, Binary codes and partial permutation decoding sets from the odd graphs, *Cent. Eur. J. Math.*, **12** (2014), 1362–1371.

[31] ———, Binary codes from the complements of the triangular graphs, *Quaest. Math.*, **33** (2010), 399–408.

[32] W. Fish, J. D. Key and E. Mwambene, Codes, designs and groups from the Hamming graphs, *J. Comb. Inf. Syst. Sci.*, **34** (1-4) (2009),169–182.

[33] ———, Graphs, designs and codes related to the n-cube, *Discrete Math.*, **309** (2009), 3255–3269.

[34] ———, Binary codes from the line graph of the n-cube, *J. Symbolic Comput.*, **45** (7) (2010), 800–812.

[35] ———, Codes from incidence matrices and line graphs of Hamming graphs, *Discrete Math.*, **310** (2010), 1884–1897.

[36] ———, Codes from the incidence matrices of graphs on 3-sets, *Discrete Math.*, **311** (2011), 1823–1840.

[37] ———, Codes from the incidence matrices and line graphs of Hamming graphs $H^k(n, 2)$ for $k \geq 2$, *Adv. Math. Commun.*, **5** (2011), 373–394.

[38] ———, Codes from the incidence matrices of graphs on 3-sets, *Discrete Math.*, **311** (2011), 1823-1840.

[39] ———, Self-orthogonal binary codes from odd graphs, *Util. Math.*, **103** (2017), 73–97.

[40] W. Fish, N. B. Mumba, E. Mwambene and B. G. Rodrigues, Binary codes and partial permutation decoding sets from biadjacency matrices of bipartite graphs $\Gamma(2k + 1, k, k + 2, 1)$, *Graphs Combin.*, **33** (2017), 357–368.

[41] ————, Binary codes and partial permutation decoding sets from biadjacency matrices of bipartite graphs $\Gamma(2k, k, k + 1, 1)$. (revised and resubmitted).

[42] ————, Equality of codes in the face of non-isomorphism in uniform subset graphs, submitted.

[43] Z. Füredi, Graphs of diameter 3 with the minimum number of edges, *Graphs Combin.*, **6** (1990) 333–337.

[44] C. Godsil and G. Royle, *Algebraic Graph Theory*. New York: Springer, Vol. 207 of Graduate Texts in Mathematics, 2001.

[45] D. M. Gordon, Minimal permutation sets for decoding the binary Golay codes, *IEEE Trans. Inform. Theory*, **28** (1982), 541–543.

[46] J. L. Gross and T. W. Tucker, Generating all graph coverings by permutation voltage assignments, *Discrete Math.*, **18** (1977), 273–283.

[47] W. H. Haemers, Matrices for graphs, designs and codes, *NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur.*, **29** (1981), 253–277.

[48] W. H. Haemers, R. Peeters and J. M. van Rijckevorsel, Binary codes of strongly regular graphs, *Des. Codes Cryptogr.*, **17** (1999), 187–209.

[49] R. L. Hemminger, On Whitney's line graph theorem, *Amer. Math. Monthly*, **79** (4) (1972) 374–378.

[50] R. Hill, *A First Course in Coding Theory*. Oxford: Oxford University Press, 1986.

[51] M. Hofmeister, Isomorphisms and automorphisms of graph coverings, *Discrete Math.*, **98** (1991), 175–183.

[52] W. C. Huffman, Codes and groups, in: *Handbook of Coding Theory* (V.S. Pless and W.C. Huffman, ed.), Amsterdam, Elsevier, 1998, pp. 1345–1440.

[53] W. C. Huffman and V. S. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge: Cambridge University Press, 2003.

[54] W. Imrich and H. Izbicki, Associative products of graphs, *Monatsh. Math*, **80** (1975) 277–281.

[55] T. W. Judson, *Abstract Algebra, Theory and Applications*. Stephan F. Austin State university, 2013.

[56] T. Kasami, A decoding procedure for multiple-error-correcting cyclic codes, *IEEE Trans. Inform. Theory*, **IT-10** (1964) 134–138.

[57] J. D. Key, J. Moori and B. G. Rodrigues, Permutation decoding sets for the binary codes from triangular graphs, *European J. Combin.*, **25** (2004), 113–123.

[58] ———, Ternary codes from graphs on triples, *Discrete Math.*, **309** (2009), 4663–4681.

[59] ———, Codes associated with triangular graphs and permutation decoding, *Int. J. Inform. and Coding Theory*, **1** (2010), 334–349.

[60] J. D. Key and B. G. Rodrigues, Codes associated with lattice graphs, and permutation decoding, *Discrete Appl. Math.*, **158** (2010), 1807–1815.

[61] J. D. Key and J. Moori, Codes, Designs and Graphs from the Janko Groups J_1 and J_2, *J. Combin. Math. Combin. Comput.*, **40**, (2002), 143–160.

[62] J. D. Key and J. Moori, Correction to: "Codes, Designs and Graphs from the Janko Groups J_1 and J_2, [*J. Combin. Math. Combin. Comput.*, **40**, (2002), 143–160]", *J. Combin. Math. Combin. Comput.*, **64**, (2008), 153.

[63] J. D. Key, Permutation decoding: An update. Available from `http://www.ces.clemson.edu/~keyj/Key/PDupdate.pdf`, 2003.

[64] J. D. Key, Permutation decoding of codes from designs and graphs, presented at Combinatorics 2008, available from `http://www.ces.clemson.edu/~keyj/Key/c2008.pdf`.

[65] J. D. Key, Recent developments in permutation decoding, available from `http://www.ces.clemson.edu/~keyj/Key/SAMS05b.pdf`.

[66] J. D. Key, T. P. McDonough and V. C. Mavron, Partial permutation decoding for codes from finite planes, *European J. Combin.*, **26** (2005), 665–682.

[67] J. D. Key, T. P. McDonough and V. C. Mavron, Information sets and partial permutation decoding for codes from finite geometries, *Finite Fields Appl.*, **12** (2006), 232–247.

[68] J. D. Key and P. Seneviratne, Permutation decoding for binary codes from lattice graphs, *Discrete Math.*, **308** (2008), 2862–2867.

[69] J. D. Key and P. Seneviratne, Binary codes from rectangular lattice graphs and permutation decoding, *European J. Combin.*, **28** (1) (2007), 121–126.

[70] J. D. Key and 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 Cryptography*, in: Vol. 3 of *Series on Coding Theory and Cryptology.* Hackensack: World Scientific Publishing Co. Pte. Ltd., (2007), 152–159.

[71] H-J. Kroll and R. Vincent, PD-sets related to the codes of some classical variates, *Discrete Appl. Math.*, **301** (2005), 89–105.

[72] H-J. Kroll and R. Vincenti, Antiblocking decoding, *Discrete Appl. Math.*,**158** (2010), 1461–1464.

[73] K. Kumwenda, *Codes, Graphs and Designs Related to Iterated Line Graphs of Complete Graphs*, Ph.D. Thesis, University of the Western Cape, 2011.

[74] J. Limbupasiriporn, *Partial permutation decoding for codes from designs and finite geometries*, Ph.D Thesis, Clemson University, 2005.

[75] S. Ling and C. Xing, *Coding Theory-A First Course*, Cambridge University Press, 2003.

[76] C. H. C. Little, D. D. Grant and D. A. Holton, On defect-d matchings in graphs, *Discrete Math.*, **13** (1975), 41–54.

[77] F. J. MacWilliams, Permuation decoding of systematic codes, *Bell System Tech. J.*, **43** (1964), 485–505.

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

[79] A. Maroti, *Orders, Conjugacy Classes, and coverings of Permutation Groups*, Ph.D. Thesis, University of Szeged, 2007.

[80] J. L. Massey, Reversible codes, *Inform. and Control*, **7** (1964), 369–380.

[81] N. B. Mumba and E. Mwambene, Automorphism groups of graph covers and uniform subset graphs, submitted.

[82] C. Peters, Information-set decoding for linear codes over F_q, in: Post-Quantum Cryptography, *Lecture Notes in Computer Science*, vol. 6061, pp. 81–94, Springer, 2010.

[83] E. Prange, The use of information sets in decoding cyclic codes, *IRE Trans.*, **8** (1962), S5-S9.

[84] M. Quick, *Topics in groups lecture notes, for MT 5824*, 2013, available from `http://www-groups.mcs.st-andrews.ac.uk/~martyn/5824/5824lecturenotes.pdf`.

[85] M. Ramras and E. Donovan, The automorphism group of a Johnson graph, *SIAM J. Discrete Math.*, **25** (2011), 267–270.

[86] B. G. Rodrigues, *Codes of Designs and Graphs from Finite Simple Groups*, PhD Thesis, University of Natal, 2002.

[87] G. Sabidussi, Graphs without dead ends, *European J. Combin.*, **17** (1996), 69–87.

[88] G. Sabidussi, Graph multiplication, *Math. Z.*, **72** (1) (1960), 446-457.

[89] J. Schönheim, On coverings, *Pacific J. Math.*, **14** (1964), 1405–1411.

[90] P. Seneviratne, *Permutation Decoding of Codes from Graphs and Designs*, PhD Thesis, Clemson University, 2007.

[91] C. C. Sims, Graphs and finite permutation groups, *Math.z*, **95** (1967), 76–86.

[92] J. Stern, A method for finding codewords of small weight, in G.D. Cohen and J. Wolfmann (Eds.), *Lecture Notes in Computer Science*, Vol. 388, pp.106-113, Springer, 1989.

[93] V. D. Tonchev, *Combinatorial Configurations, Designs, Codes, Graphs*, Pitman Monographs and Surveys in Pure and Applied Mathematics, No. 40. New York: Longman, 1988. Translated from the Bulgarian by Robert A. Melter.

[94] M. Valencia-Pabon and J-C. Vera, On the diameter of Kneser graphs, *Discrete Math.*, **305** (2005), 383–385.

[95] V. G. Vizing, The cartesian product of graphs (Russian), *Vychisl. Sistemy*, **9** (1963) 30–43.

[96] D. B. West, *Introduction to Graph Theory* (Second Edition). Patparganj: Pearson Education Pte. Ltd., 2001.

[97] H. Whitney, Congruent graphs and the connectivity of graphs, *Amer. J. Math.*, **54** (1932), 150–168.

[98] R. A. Wilson, *The Finite Simple Groups*, Springer-Verlag London Limited, Graduate Texts in Mathematics, **251**, 2009.

Index