Codes, graphs and designs related to iterated line graphs of complete graphs

Khumbo Kumwenda

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

Supervisor
Prof Eric Mwambene

Co-supervisor
Dr Washiela Fish

August, 2011

Codes, graphs and designs related to iterated line graphs of complete graphs

Khumbo Kumwenda

KEYWORDS

Automorphism groups

Categorical product of graphs

Designs

Graphs

Incidence design

Iterated line graph

Linear code

Neighbourhood design

Permutation decoding

PD-sets

Strong product of graphs

Abstract

In this thesis, we describe linear codes over prime fields obtained from incidence designs of iterated line graphs of complete graphs $L^i(K_n)$ where $i = 1, 2$. In the binary case, results are extended to codes from neighbourhood designs of the line graphs $L^{i+1}(K_n)$ using certain elementary relations. Codes from incidence designs of complete graphs, K_n, and neighbourhood designs of their line graphs, $L^1(K_n)$ (the so-called triangular graphs), have been considered elsewhere by others. We consider codes from incidence designs of $L^1(K_n)$ and $L^2(K_n)$, and neighbourhood designs of $L^2(K_n)$ and $L^3(K_n)$. In each case, basic parameters of the codes are determined.

Further, we introduce a family of vertex-transitive graphs Γ_n that are embeddable into the strong product $L^1(K_n) \boxtimes K_2$, of triangular graphs and K_2, a class which at first sight may seem unnatural but, on closer look, is a repository of graphs rich with combinatorial structures. For instance, unlike most regular graphs considered here and elsewhere that only come with incidence and neighbourhood designs, Γ_n also has what we have termed as 6-cycle designs. These are designs in which the point set contains vertices of the graph and every block contains vertices of a 6-cycle in the graph. Also, binary codes from incidence matrices of these graphs have other minimum words in addition to incidence vectors of the blocks. In addition, these graphs have induced subgraphs isomorphic to the family H_n of complete porcupines (see Definition 4.11). We describe codes from incidence matrices of Γ_n and H_n and determine their parameters.

The discussion is concluded with a look at complements of Γ_n and H_n, respectively denoted by $\overline{\Gamma}_n$ and $\overline{H}_n$. Among others, the complements $\overline{\Gamma}_n$ are contained in the union of the categorical product $L^1(K_n) \times K_n$, and the categorical product $\overline{L^1(K_n)} \times K_n$ (where $\overline{L^1(K_n)}$ is the complement of the triangular graph $L^1(K_n)$). As with the other graphs, we have also considered codes from the span of incidence matrices of $\overline{\Gamma}_n$ and $\overline{H}_n$ and determined some of their properties.

In each case, automorphisms of the graphs, designs and codes have been determined. For the codes from incidence designs of triangular graphs, embeddings of $L^1(K_n) \times K_2$ and complements of complete porcupines, we have exhibited permutation decoding sets (PD-sets) for correcting up to t errors where t is the full error-correcting capacity of the codes. For the remaining codes, we have only been able to determine PD-sets for which it is possible to correct a fraction of t errors (partial permutation decoding). For these codes we have also determined the number of errors that can be corrected by permutation decoding in the worst-case.

Declaration

I declare that *Codes, graphs and designs related to iterated line graphs of complete graphs* 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 complete references.

Khumbo Kumwenda August 2011

Signed: . . . .

List of symbols

$\mathrm{Aut}(C)$	automorphism group of a linear code C
$\mathrm{Aut}(\mathcal{D})$	automorphism group of a design $\mathcal{D}$
$\mathrm{Aut}(\Gamma)$	automorphism group of a graph Γ
$\mathcal{B}$	block set of a design
C	linear code
$C_p(M)$	p-ary linear code generated by a matrix M over $\mathbb{F}_p$
$C^{\perp}$	dual code of C
$C_p(M)^{\perp}$	dual code of $C_p(M)$
$\mathrm{d}(C)$	minimum distance of C
$\dim(C)$	dimension of C
$d(x, y)$	Hamming distance between codewords x and y
$\mathcal{D}$	design
$\mathbb{F}_q$	finite field of order q where $q = p^t$, p a prime
$\mathbb{F}_q^n$	vector space of n-tuples over $\mathbb{F}_q$
G	automorphism group
Γ	graph
Γ_n	embedding of $L^1(K_n) \boxtimes K_2$
$\overline{\Gamma}$	complement of a given graph Γ
H	parity-check matrix of C
H_n	complete porcupine
I_k	identity matrix of rank k
$\mathcal{I}$	incidence relation
$\mathcal{I}_n$	information set
$\cong$	isomorphism of two structures
$\jmath$	all-one vector in a given code

$\jmath_n$	all-one vector of length n in a given code
K_X	complete graph with vertex-set X
K_n	complete graph with n vertices
$K_{m,n}$	complete bipartite graph with bipartition (X, Y) where $\|X\| = m$ and $\|Y\| = n$
$L(\Gamma)$	line graph of a graph Γ
$L^i(\Gamma)$	i-iterated line graph of a graph Γ
M	generator matrix
$N(v)$	open neighbourhood of a vertex v
$N[v]$	closed neighbourhood of a vertex v
Ω	the set $\{1, \cdots, n\}$
$\Omega^{\{k\}}$	set of subsets of Ω of size k
$\mathcal{P}$	point set of a design
$\text{Supp}(x)$	support of a vector x
S_n	symmetric group on a set of n elements
$\Gamma_1 \square \Gamma_2$	cartesian product of graphs Γ_1 and Γ_2
$\Gamma_1 \boxtimes \Gamma_2$	strong product of graphs Γ_1 and Γ_2
$\Gamma_1 \times \Gamma_2$	categorical product of graphs Γ_1 and Γ_2
$\overline{v}$	block of $\mathcal{D}$ indexed by a vertex v of a graph Γ
$v^{\overline{v}}$	incidence vector of $\overline{v}$
$G_1 \wr G_2$	wreath product of groups G_1 and G_2
$\text{wt}(x)$	Hamming weight of a vector x

Acknowledgement

I have benefited a lot from

- Two supervisors who gave a lot of time to this work and kept their doors open at all times to equally get their hands dirty with the work. Eric and Washiela paid a lot of attention to details and pointed me in interesting directions right from the start. They are also the very reason I became interested in studying codes from graphs and designs.

- An understanding, patient and caring fiancée in Zelipha for letting me lean on her shoulder whenever I needed one.

- The support of my family members, particularly Temwa, Esther and Leonard, and a great friend Paul, for taking care of my home during the lengthy periods I was away.

- Friends who lightened the stress with the many lighter moments we shared, in person and online. Thanks a lot to Atipatsa, Aubrey, Brown, Didrick, Ezekiel, Mapopa, Paul, Precious, Tiyamika, Trevor, Walter and Ziolire. And to everybody in the mathematics postgraduate laboratories at the University of the Western Cape.

- The support of my employers, Mzuzu University. In particular, I acknowledge the role played by the Deputy Vice Chancellor Prof. Orton Msiska, the Coordinator of the MSc programme in Information Theory, Coding and Cryptography Prof. John Ryan, the Head of Department (Mathematics) at the time of my departure Dr. Busiso Chisala and the entire Mathematics Department.

- The postgraduate scholarship I got from German Academic Exchange Service (Deutscher Akademischer Austausch Dienst - DAAD). To this end, I acknowledge the role played by the African Mathematical Sciences Institute through Gudrun Schirge and Liesl Jones in facilitating the scholarship.

To Mum and Dad,
and to Zelipha.

Contents

List of Figures

Chapter 1

Introduction

Significant effort with considerable success has been directed towards the description of linear codes from neighbourhood and incidence designs of various regular graphs. A neighbourhood design of a regular graph is formed by taking points to be vertices of the graph and each block consists of neighbours of a given vertex. In the incidence design, points are edges of the graph and each block consists of edges incident with a given vertex. In most cases, these codes have been decoded using permutation decoding, a method due to MacWilliams [52]. This is because combinatorial properties of the graphs and designs are intimately linked to important properties of the codes including minimum weight, minimum words, information sets and automorphism groups which are pertinent for successful permutation decoding.

Incidence matrices of the neighbourhood designs are also adjacency matrices of the graphs and incidence vectors are rows of the matrices. Linear codes have since been studied from neighbourhood designs of triangular graphs [56, 41, 29, 61], complements of triangular graphs [16, 17], n-cubes [20, 16, 45, 59], line graphs of n-cubes [21], Hamming graphs [18], line graphs of Hamming graphs [19], lattice graphs [44, 43, 59], complete multipartite graphs [59] and various uniform subset graphs [16, 56], among others. In all these cases, permutation decoding has been employed with varying success. PD-sets for full permutation decoding have been exhibited for some of the codes including the binary codes from triangular graphs in [41, 56]. For some codes, partial permutation decoding, a concept introduced in [39], has been used. Here, one corrects $s \leq t$ errors where t is the full error-correcting capacity of the code. Examples where only partial permutation decoding has been done include binary codes from adjacency matrices of n-cubes [16, 45], the Johnson graphs and the Odd graphs considered in [16].

A lot of focus has recently been on codes from incidence designs of regular graphs. Incidence matrices of these designs are also incidence matrices of the graphs. Examples include codes from incidence matrices of complete graphs examined in [42], n-cubes in [21] and Hamming graphs in [19]. As with codes from the neighbourhood designs, PD-sets for full and partial permutation decoding have been obtained. For instance, full permutation decoding has been achieved for the codes from incidence matrices of complete graphs [42] and Hamming graphs [19]. In [21], a regular subgroup of the automorphism group of the binary codes associated with the line graph of the n-cube, for any information set, is given that can be used for full or partial permutation decoding.

Let Γ be a graph with incidence matrix B. Consider the binary code from the row span of an adjacency matrix A of the line graph $L(\Gamma)$. Over $\mathbb{F}_2$, it is well known that $A = B^T B$. Given the binary code $C_2(B)$ from the row span of B, it is therefore possible to predict some properties of the subcode $C_2(A)$, the binary code from the row span of A. This link between A and B has been exploited in [21] where binary codes from incidence matrices of the n-cube and adjacency matrices of their line graphs have been considered. In our case, we have used the relationship to determine parameters of the binary codes $C_2(A)$ where A is an adjacency matrix of the iterated line graph $L^i(K_n)$ for $i = 2, 3$, given the binary code from an incidence matrix of $L^{i-1}(K_n)$. A detailed discussion on these and other relationships between graphs, designs and codes is given in Section 2.4.

In this thesis, we examine linear codes over all prime fields obtained from incidence matrices of the line graphs $L^1(K_n)$ and $L^2(K_n)$ (triangular graphs and their line graphs, respectively). This is a follow-up on work reported in [42] on non-binary codes from incidence matrices of complete graphs K_n and in [29, 41, 56, 61] on binary codes from adjacency matrices of triangular graphs. To an extent, our approach is similar to that used in [21] for codes from line graphs of the n-cube and in [19] where codes from incidence matrices and line graphs of Hamming graphs have been examined. We use results on the binary codes from incidence matrices of $L^1(K_n)$ and $L^2(K_n)$, and the relationship between A and B referred to above, to describe binary codes from adjacency matrices of $L^2(K_n)$ and $L^3(K_n)$, respectively. In the non-binary case, we examine codes spanned by differences of rows of incidence matrices of $L^1(K_n)$.

We also consider codes from graphs embeddable into graph products involving triangular graphs, their complements and K_n. To this end, we introduce a family of graphs Γ_n that is an embedding of the strong product $L^1(K_n) \boxtimes K_2$, of triangular graphs and K_2. Complements of these graphs are contained in the union $(L^1(K_n) \times K_n) \cup \left(\overline{L^1(K_n)} \times K_n\right)$, where × denotes the categorical product of graphs and $\overline{L^1(K_n)}$ is the complement of the triangular graph $L^1(K_n)$. It is shown that these graphs are isomorphic to certain induced subgraphs of $L^2(K_n)$ and its complement $\overline{L^2(K_n)}$, respectively. Complete porcupines H_n (also simply known as porcupines, see [26]) are induced subgraphs of Γ_n. We have determined various properties including automorphism groups of Γ_n, $\overline{\Gamma}_n$, H_n and $\overline{H}_n$.

As with triangular graphs and their line graphs, we have described binary and non-binary codes from incidence matrices of Γ_n, $\overline{\Gamma}_n$, H_n and $\overline{H}_n$. We have determined their parameters, minimum words and automorphism groups. Binary codes from Γ_n are the only ones we have examined that have more minimum words than just the rows of the matrices. This is also in contrast with most binary codes obtained from other regular graphs elsewhere. Codes from H_n are interesting in their own right having unit minimum weight in as much as they are not full spaces. However, codes from complements of the complete porcupines are less trivial.

For each class of codes considered, permutation decoding has been employed. We have exhibited PD-sets for full permutation decoding of codes from incidence matrices of triangular graphs, Γ_n and $\overline{H}_n$. For the other codes we have determined PD-sets for partial permutation decoding. These include codes from incidence matrices of $\overline{\Gamma}_n$ and $L^2(K_n)$.

1.1 Thesis outline

We begin by presenting preliminaries related to codes, graphs and designs in Chapter 2. The material is standard. However, to aid the discussion, some results are given in Lemma 2.25, Corollary 2.26 and Proposition 2.30. Lemma 2.25 has also been used to give an alternative proof to Corollary 2.27, a result that appears in [42]. This result gives an upper bound on the minimum weight of non-binary codes from adjacency matrices of graphs with a 4-cycle. A discussion on information set and permutation decoding follows in Section 2.5. The chapter concludes with a presentation of some results on codes from complete graphs and triangular graphs in Section 2.6 and codes from a bipartite uniform subset graph (see Definition 2.4) in Section 2.7.

Chapter 3 focusses on codes from incidence matrices of triangular graphs $L^1(K_n)$, differences of rows of the matrices and adjacency matrices of their line graphs $L^2(K_n)$. Let B_n be an incidence matrix of $L^1(K_n)$ and A_n an adjacency matrix of $L^2(K_n)$. For any prime p, let $C_p(B_n)$ and $C_p(A_n)$ be the linear codes obtained from the row span over $\mathbb{F}_p$ of B_n and A_n, respectively. Let $E_p(B_n)$ be the code spanned over $\mathbb{F}_p$ by differences of rows of B_n. We investigate various properties of $C_p(B_n)$ and present results that extend to the binary codes $C_2(A_n)$. In particular, it is shown that $C_2(B_n) = C_2(A_n)$ if $n \equiv 2, 3 \pmod 4$ and that $C_2(A_n) = E_2(B_n)$ for all n. Parameters of $C_p(B_n)$, $C_2(A_n)$ and $E_p(B_n)$ are established for any prime p and $n \geq 3$. We also determine automorphism groups of $C_p(B_n)$. Using a specific information set, a PD-set for full permutation decoding of $C_p(B_n)$ is exhibited for any prime p.

In Chapter 4, we introduce vertex-transitive graphs Γ_n that are also embeddings of the strong product $L^1(K_n) \boxtimes K_2$ of triangular graphs and K_2 where $n \geq 3$. The graph Γ_n is isomorphic to certain induced subgraphs of $L^2(K_n)$ and it contains the complete porcupine, H_n. Some properties of Γ_n including automorphism groups are determined. Unlike other regular graphs considered in this thesis and elsewhere for which one may only associate neighbourhood and incidence designs, we show that Γ_n also has what we have termed as 6-*cycle designs*. These are 1-designs in which every block is incident with vertices of a 6-cycle in the graph. Codes from incidence matrices of Γ_n and H_n are studied and parameters determined. Unlike most codes from incidence matrices of regular graphs reported here and elsewhere, binary codes from Γ_n are shown to have n more minimum words in addition to the rows of the matrices. Since the codes from complete porcupines have minimum weight one, permutation decoding is only considered for the codes from Γ_n. We have exhibited PD-sets for full permutation decoding of both binary and non-binary codes.

In Chapter 5, we consider the complements $\overline{\Gamma}_n$ of embeddings of the strong product $L^1(K_n) \boxtimes K_2$ referred to above. These graphs correspond to certain induced subgraphs of the complements $\overline{L^2(K_n)}$. $\overline{\Gamma}_n$ is contained in the union $(L^1(K_n) \times K_n) \cup (\overline{L^1(K_n)} \times K_n)$. As may have been noted from the discussion above, complements of complete porcupines $\overline{H}_n$ are induced subgraphs of $\overline{\Gamma}_n$. These graphs and their codes are considered first. Automorphism groups of the graphs and codes are determined and shown to be isomorphic. One observation on some PD-sets presented here and elsewhere in literature is that, in most cases, their size is much larger than the lower bound predicted by Gordon [28]. This is despite that permutation decoding is obviously more efficient the smaller the size of the PD-sets. The PD-sets we have exhibited for the codes from incidence matrices of complements of complete porcupines are only twice the Gordon bound. We also examine codes from incidence matrices of $\overline{\Gamma}_n$ and determine their main parameters, automorphism groups and PD-sets for partial permutation decoding. The size of this PD-set is also only twice the Gordon bound.

Since Γ_n corresponds to certain induced subgraphs of $L^2(K_n)$, results obtained for the codes of Γ_n in Chapter 4 are used to describe properties of codes from incidence matrices of $L^2(K_n)$ in Chapter 6. These codes also have some properties which seem to be characteristic of codes from the iterated line graphs $L^i(K_n)$ in general. For instance, the minimum words are scalar multiples of the rows of the matrices and their automorphism group is isomorphic to that of the graphs, the symmetric group S_n. As with the codes from incidence matrices of $L^1(K_n)$, results from codes of incidence matrices of $L^2(K_n)$ have been used to describe codes from adjacency matrices of $L^3(K_n)$. For these codes we have only considered partial permutation decoding.

1.2 Papers from this thesis

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

1. K. Kumwenda and E. Mwambene, Codes from graphs related to the categorical product of triangular graphs and K_n, *Proceedings of 2010 IEEE Information Theory Workshop*, Dublin, August 30-September 3, 2010, 1-5, `dx.doi.org/10.1109/CIG.2010.5592662`.

2. W. Fish, K. Kumwenda and E. Mwambene, Codes and designs from triangular graphs and their line graphs, *Cent. Eur. J. Math.*, `dx.doi.org/10.2478/s11533-011-0072-5`.

3. W. Fish, K. Kumwenda and E. Mwambene, Permutation decoding sets for codes from incidence matrices of triangular graphs, *submitted.*

4. W. Fish, K. Kumwenda and E. Mwambene, Codes from embeddings of the strong product of triangular graphs and K_2 and certain induced subgraphs, *Ars Combin.*, accepted.

5. W. Fish, K. Kumwenda and E. Mwambene, Codes related to line graphs of triangular graphs and permutation decoding, *submitted.*

Chapter 2

Preliminaries

This chapter is a presentation of terminology, notation and an overview of results related to codes, designs and graphs that will be used. The reader is referred to the textbooks [2, 5, 6, 9, 14, 27, 31, 33, 51, 63] for more information.

The chapter is arranged as follows. In Sections 2.1, 2.2 and 2.3, we present elementary definitions related to codes, designs and graphs, respectively. In Section 2.4, we discuss links between codes, designs and graphs. We also describe properties of codes obtained from graphs and designs. Information set and permutation decoding are discussed in Section 2.5. Some known results on non-binary codes from incidence matrices of complete graphs and binary codes from adjacency matrices of triangular graphs are presented in Section 2.6.

2.1 Codes

Let p be a prime and let $q = p^t$ where t is a positive integer. Denote by $\mathbb{F}_q^n$ the vector space of n-tuples over $\mathbb{F}_q$, the finite field of order q.

In the context of coding theory, a q-ary *linear code* C is a subspace of $\mathbb{F}_q^n$. If C has dimension k then it is said to be an $[n, k]_q$ code. Elements of C are its *codewords*. The *Hamming distance* between two codewords $c_1, c_2 \in C$, written $d(c_1, c_2)$, is the number of coordinate positions in which they differ. The *minimum distance* d of C, also written as $d(C)$, is the minimum of the

Hamming distances between any two distinct codewords. If C has dimension k and minimum distance d then it is said to be an $[n,k,d]_q$ code. We will write this as $C = [n,k,d]_q$.

The minimum distance of a given code determines its error-detecting and error-correcting capability as stated in the theorem below.

Theorem 2.1. [2, Theorem 2.1.1] *Let C be a code with minimum distance d. If $d \geq s+1 > 1$ then C can be used to detect up to s errors in any received vector. If $d \geq 2t+1$ then C can be used to correct up to t errors in any received vector.*

The *Hamming weight* of a codeword $c \in C$, written $\mathrm{wt}(c)$, is the number of non-zero coordinate entries of c. Hence $\mathrm{wt}(c) = d(c, \mathbf{0})$. The *support* of c, $\mathrm{Supp}(c)$, is the set of all coordinate positions at which coordinate entries of c are non-zero, i.e.,

$$\mathrm{Supp}(c) = \{i : c_i \neq 0\}.$$

Hence $\mathrm{wt}(c) = |\mathrm{Supp}(c)|$. As with the minimum distance of C, one may also define the *minimum weight* of the code. A *minimum word* of C is a codeword of minimum weight. The following proposition is easily seen to hold.

Proposition 2.2. [9, Proposition 9.7] *The minimum distance of a linear code is equal to the minimum weight of all its non-zero codewords.*

The two most common ways to represent a linear code are with either a generator matrix or a parity check matrix.

A *generator matrix* M of a linear $[n,k]_q$ code C is a $k \times n$ matrix whose rows form a basis for C. The matrix M corresponds to a map $\mathbb{F}_q^k \to \mathbb{F}_q^n$, sending a message x of length k to a codeword $c = xM$ in C. Any set of k coordinate positions corresponding to k independent columns of M forms an *information set* for the code. The remaining $r = n-k$ positions form a *redundancy set* (also called a *check set*). r is also called the redundancy of the code.

In general, there are many generator matrices for a given linear code. Using elementary row operations, a generator matrix M can be written in the *standard form* $[I_k|A]$ where I_k is the $k \times k$ identity matrix and A is a $k \times (n-k)$ matrix. In this form the first k coordinates of the code are information positions. A generator matrix is *systematic* if among its columns there are columns of the $k \times k$ identity matrix.

In many instances, properties of a given linear code C may be established using its orthogonal complement $C^{\perp}$, also called the dual code of C. The *dual code* $C^{\perp}$ of an $[n, k, d]_q$ linear code C is defined as the set of all vectors in $\mathbb{F}_q^n$ orthogonal to C, i.e.,

$$C^{\perp} = \{v \in \mathbb{F}_q^n : (c, v) = 0 \text{ for all } c \in C\} \tag{2.1}$$

where $(,)$ denotes the standard inner product in $\mathbb{F}_q^n$. In general, $C^{\perp}$ is linear regardless of the linearity of C.

A *parity-check matrix* for C is an $(n-k) \times n$ matrix whose rows form a basis for its dual code $C^{\perp}$. It has standard form $H = \left[-A^T | I_{n-k}\right]$. Any n-tuple c over $\mathbb{F}_q$ is a codeword in C if and only if $cH^T = \mathbf{0}$.

Let C_1 and C_2 be linear codes of length n. Then the codes are *permutation equivalent* if there is a permutation of coordinates mapping C_1 to C_2. The permutation can be described using a permutation matrix P, an $n \times n$ matrix with exactly one entry equal to 1 in each row and column and 0's elsewhere. Each such matrix represents a permutation of n elements. Suppose M_1 is a generator matrix of C_1. Then C_1 and C_2 are also said to be permutation equivalent if there exists a permutation matrix P such that M_1P is a generator matrix for C_2.

It is often convenient to use permutations in cycle form other than permutation matrices. Let S_n be the symmetric group on n elements and let $\sigma \in S_n$. Consider a vector $x = x_1 \cdots x_n$. Define $\sigma(x)$ by $\sigma(x) = x_{\sigma^{-1}(1)} \cdots x_{\sigma^{-1}(n)}$. This way, we have $\sigma(x) = xP$ where P is the permutation matrix given by $p_{ij} = 1$ if $\sigma(i) = j$ and 0 otherwise.

The set of coordinate permutations that map a linear code C to itself forms a group under composition called the *permutation automorphism group* of C, denoted $\mathrm{Aut}(C)$. We note that there are more general equivalences of codes when one considers fields other than $\mathbb{F}_2$. We will not consider these but the interested reader is referred to Huffman and Pless [33, Section 1.7] for a detailed discussion.

We now give a definition of the well-known class of reversible codes. A reversible code has been presented in Lemma 5.12. These codes were introduced by Massey in [53]. A block code C is *reversible* if the block of digits formed by reversing the order of the digits in a codeword is another codeword in the same code. That is, a code C is reversible if and only if $(c_n, c_{n-1}, \cdots, c_1) \in C$ whenever $(c_1, \cdots, c_n) \in C$.

2.2 Designs

The basic concept in the theory of designs is that of a *finite incidence structure*, a triple $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ where $\mathcal{P}$ and $\mathcal{B}$ are disjoint finite sets and $\mathcal{I}$ is a binary relation between $\mathcal{P}$ and $\mathcal{B}$, i.e., $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$. Members of $\mathcal{P}$ are called *points*, those of $\mathcal{B}$ are *blocks* and those of $\mathcal{I}$ *flags*. Points are denoted by lower case letters while blocks by capital letters. If $(p, B) \in \mathcal{I}$ then the point p is said to be *incident* with the block B or B contains the point p.

We only consider incidence structures with a particular degree of regularity. These are called *designs* or *t-designs* if the degree of regularity is to be emphasised. An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is called a $t-(v, k, \lambda)$ *design*, or simply a t-design, for some non-negative integers t, v, k and λ if $\mathcal{P}$ has v points, every block $B \in \mathcal{B}$ is incident with precisely k points and every subset of $\mathcal{P}$ of size t is incident with exactly λ blocks.

A design is *symmetric* if the number of points is equal to the number of blocks. Two distinct blocks are said to be *repeated* if they are incident with the same set of points. A design is *simple* if it has no repeated blocks. A *trivial design* is one in which every set of k points is incident with a block. Designs considered in this thesis are simple and non-trivial 1-designs.

An incidence structure may be represented by its incidence matrix. Let $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be an incidence structure with point set $\mathcal{P} = \{p_1, ..., p_v\}$ and block set $\mathcal{B} = \{B_1, ..., B_b\}$. An *incidence matrix* for $\mathcal{S}$ is the $b \times v$ matrix $M = (m_{ij})$ with (i, j)th entry 1 if and only if the ith block contains the jth point and 0 otherwise.

If $P \subseteq \mathcal{P}$ then the *incidence vector* of P, written v^P, is the characteristic vector of P, i.e., v^P is such that $v^P(i) = 1$ if $i \in P$ and $v^P(i) = 0$ otherwise. Each row of an incidence matrix M is an incidence vector of the corresponding block.

For any given design $\mathcal{D}$, there are related structures that yield designs in some cases. We are interested in the dual of a given design. Properties of the dual provide a way of determining dimensions of the codes considered in Sections 3.4, 3.5, and 6.4.3.

In general, the *dual* of an incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is the structure $\mathcal{S}^t = (\mathcal{P}^t, \mathcal{B}^t, \mathcal{I}^t)$ where $\mathcal{P}^t = \mathcal{B}$, $\mathcal{B}^t = \mathcal{P}$ and $(B, p) \in \mathcal{I}^t$ if and only if $(p, B) \in \mathcal{I}$. If B is an incidence matrix of $\mathcal{S}$ then B^T, the transpose of B, is an incidence matrix of the dual S^t.

Now that some basic definitions of designs have been introduced, let us consider the notion of isomorphisms of designs.

Let $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ and $\mathcal{S}' = (\mathcal{P}', \mathcal{B}', \mathcal{J}')$ be incidence structures and let $\phi : \mathcal{P} \cup \mathcal{B} \to \mathcal{P}' \cup \mathcal{B}'$ be a bijection. Then ϕ is an *isomorphism* if it satisfies the following conditions.

(a) $\phi(\mathcal{P}) = \mathcal{P}'$ and $\phi(\mathcal{B}) = \mathcal{B}'$;

(b) $(p, B) \in \mathcal{I}$ if and only if $(\phi(p), \phi(B)) \in \mathcal{I}'$ for all $p \in \mathcal{P}$ and $B \in \mathcal{B}$.

If there is an isomorphism between incidence structures $\mathcal{S}$ and $\mathcal{S}'$ then they are said to be *isomorphic*. If $\mathcal{S} = \mathcal{S}'$ then ϕ is an *automorphism*. The set of all automorphisms of $\mathcal{S}$ forms a group under composition called the *automorphism group* of $\mathcal{S}$, denoted $\text{Aut}(\mathcal{S})$.

Observe the following: In terms of incidence matrices M and M' of, respectively, $\mathcal{S}$ and $\mathcal{S}'$, the incidence structures are isomorphic if there exist row and column permutations transforming M into M', i.e, if there exist permutation matrices P and Q such that $PMQ = M'$.

Some classes of designs obtained from regular graphs are considered in Section 2.4.

2.3 Graphs

We now present terminology from graph theory. The definition of graphs below is as given in [14]. Such graphs are also termed *simple graphs* by others (cf. [63]).

A *graph* is a pair $\Gamma = (V, E)$ of sets such that $E \subseteq V^{\{2\}}$, i.e, E contains 2-element subsets of V. The elements of V are *vertices* of the graph and those of E are its *edges*. The vertex set of Γ is denoted $V(\Gamma)$ and its edge set by $E(\Gamma)$. If $e = \{u, v\} \in E$ then we write $e = [u, v]$. The vertices u and v are said to be *adjacent* or *neighbours*. The vertices u and v are also said to be *incident* with the edge e. Two distinct edges e and f are adjacent if they are incident with a common vertex. The parity of a graph $\Gamma = (V, E)$ is the parity of $|V(\Gamma)|$.

Let $\Gamma = (V, E)$ be a graph and consider a vertex $v \in V(\Gamma)$. The *open neighbourhood* of v, $N(v)$, is the set of all vertices adjacent to v; the set $N[v] = N(v) \cup \{v\}$ is the *closed neighbourhood* of v. When we must be explicit, the open and closed neighbourhoods will be denoted $N_\Gamma(v)$ and $N_\Gamma[v]$, respectively. When stated without qualification, the neighbourhood is assumed to be open. The *degree* (or *valency*) of a vertex v, denoted $\deg(v)$, is the order of the set $N(v)$. If all vertices of Γ have the same degree k then Γ is said to be *k-regular*, or simply *regular*. When the degrees of all vertices in a graph are counted, every edge is counted exactly twice, once from each of its ends. Hence the number of edges of a k-regular graph $\Gamma = (V, E)$ is $|E| = \frac{1}{2}k \cdot |V|$, a result which follows from the hand-shaking lemma.

A *walk* in a graph Γ is a sequence $v_0, v_1, \cdots, v_n$ of vertices such that $[v_{i-1}, v_i]$ is an edge for $1 \leq i \leq n$; n is the *length* of the walk. A walk is called a *trail* if all edges appearing in it are distinct. It is *closed* if $v_0 = v_n$. A walk is a *path* if all its vertices are distinct. If there exists a path between any two vertices of a graph Γ then the graph is *connected*. 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.

Let $\Gamma = (V, E)$ and $\Gamma' = (V', E')$ be two graphs such that $V' \subseteq V$ and $E' \subseteq E$. Then Γ' is a *subgraph* of Γ. If Γ' contains all edges of Γ that join two vertices in V' then Γ' is said to be an *induced subgraph* of Γ and this is written as $\Gamma' = \Gamma[V']$.

Let X be a non-empty set. A *complete graph* K_X is a graph on X in which every pair of distinct vertices is adjacent. If $X = \Omega = \{1, \cdots, n\}$

then K_X 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.* A clique is *maximal* if it is not properly contained in another clique, i.e., if u is any vertex not in the clique then there exists a vertex v in the clique such that u and v are not adjacent. A clique of the largest size is said to be *maximum.* The number of vertices in a maximum clique is the *clique number* of the graph.

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. Hence if $\Gamma = (V, E)$ then its complement is the graph $\overline{\Gamma} = (V, E(K_V) \setminus E)$ where $E(K_V)$ is the edge set of the complete graph on V. If a graph Γ is k-regular then its complement is $(|V| - k - 1)$-regular.

A graph Γ is *k-edge-connected* if any subgraph formed by removing any $k - 1$ edges is connected. The *edge-connectivity* of a graph is the minimum number of edges needed to disconnect it.

2.3.1 Bipartite graphs

The dimension of non-binary codes from incidence matrices of the graph will be determined by whether the graph is bipartite or not. Details of this are given in Lemma 2.23. We will also consider bipartite subgraphs of certain graphs examined in this thesis. Examples include bipartite subgraphs of triangular graphs in Chapter 3 and embeddings of strong products of triangular graphs and K_2 in Chapter 4.

A graph Γ is *bipartite* if its vertex set can be partitioned into two non-empty subsets U and V such that each edge of Γ has one end in U and the other end in V. The pair (U, V) is a *bipartition* of the graph. A bipartite graph with bipartition (U, V) is denoted $\Gamma(U, V)$. If each vertex of U is adjacent to all vertices of V then $\Gamma(U, V)$ is a *complete bipartite graph.* A complete bipartite graph $\Gamma(U, V)$ such that $|U| = m$ and $|V| = n$ is denoted $K_{m,n}$. The graph $K_{1,n}$ is called a *star.*

As defined, a bipartite graph has no odd cycles. In fact, bipartite graphs are characterised by this property:

Proposition 2.3. [14, Proposition 1.6.1] *A graph is bipartite if and only if* *it contains no odd cycle.*

Fish, Key and Mwambene introduced the family of bipartite uniform subset graphs in [22]. A bipartite uniform subset graph is an induced subgraph of the triangular graph $L^1(K_4)$ (as observed from an incidence matrix of the graph in Equation (3.4)).

Definition 2.4. [22] Let $\Omega = \{1, \cdots, n\}$ and let k, l and i be non-negative integers such that $n \geq k, l$ and $k, l \geq i$. Let $\Omega^{\{j\}}$ be the set of subsets of order j of Ω. The *bipartite uniform subset graph* $\Gamma(n, k, l, i)$ has bipartition $\left(\Omega^{\{k\}}, \Omega^{\{l\}}\right)$ such that vertices $u \in \Omega^{\{k\}}$ and $v \in \Omega^{\{l\}}$ are adjacent if and only if $|u \cap v| = i$.

Hence $\Gamma(n, k, l, i)$ 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 of each vertex in $\Omega^{\{l\}}$ is $\binom{l}{i}\binom{n-l}{k-i}$. The graph has $\binom{n}{k}\binom{k}{i}\binom{n-k}{l-i} = \binom{n}{l}\binom{l}{i}\binom{n-l}{k-i}$ edges.

For certain values of n, k, l and i, codes from incidence matrices of bipartite uniform subset graphs $\Gamma(n, k, l, i)$ have been considered in [22]. In Lemma 3.2, we need results on codes from incidence matrices of the graphs $\Gamma(3, 2, 1, 1)$. Parameters of codes from incidence matrices of the family of graphs $\Gamma(n, k, 1, 1)$ are summarised in Proposition 2.37.

2.3.2 Line graphs

As it has been alluded to in Chapter 1, our work focusses on codes from iterated line graphs of complete graphs. In this section, we give definitions of iterated line graphs and consider their pertinent properties.

Let $\Gamma = (V, E)$ be a graph. The *line graph* of Γ, denoted $L(\Gamma)$, is the graph whose vertex set consists of the set of edges of Γ and two vertices e and f are adjacent if and only if they are adjacent as edges of Γ. For $i \geq 1$, the iterated line graph $L^i(\Gamma)$ is formed by successive applications of the line graph operator, i.e., $L^i(\Gamma) = L(L^{i-1}(\Gamma))$ where $L^0(\Gamma) = \Gamma$.

In general, iterated line graphs grow exponentially regardless of the starting graph. Exceptional cases are the line graph of the path P_n and that of the cycle C_n. The line graph of P_n is P_{n-1} and $L(C_n) = C_n$. Figure 2.1 depicts iterated line graphs of the star $K_{1,4}$.

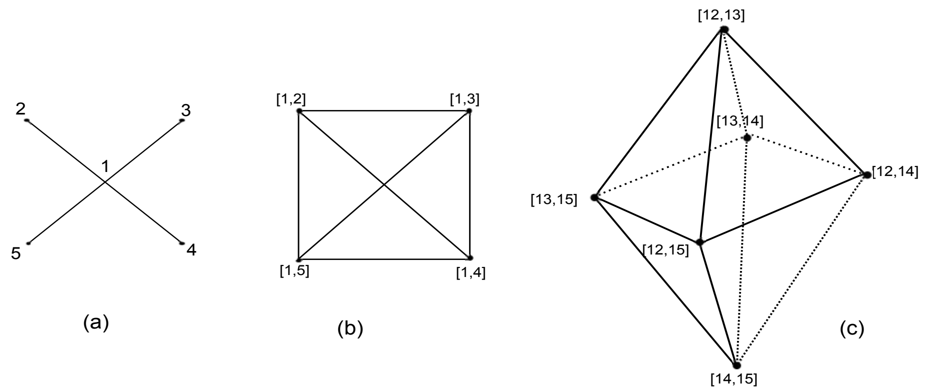

Figure 2.1: Iterated line graphs of $K_{1,4}$: (a) $K_{1,4}$, (b) $K_4 = L^1(K_{1,4})$ and (c) $L(K_4) = L^2(K_{1,4})$

Properties of a graph Γ that depend only on adjacency of edges may be translated into properties of its line graph that depend on the adjacency of vertices. For instance, if Γ is connected then it contains a path connecting any two edges. This translates to a path in the line graph $L(\Gamma)$ connecting any two vertices. Hence the line graph is also connected. The edges incident at a vertex of Γ give rise to a maximal clique in the line graph $L(\Gamma)$. Further properties of $L(\Gamma)$ that are relevant to our discussion are stated below.

Lemma 2.5. [27, Lemma 1.7.1] *If a graph* Γ *is* k*-regular then its line graph* $L(\Gamma)$ *is* $(2k-2)$*-regular.*

Proof. Let $e = [u, v] \in E(\Gamma)$. Then

$$\left|N_{L(\Gamma)}(e)\right| = |\{[u, x] : x \neq v\} \cup \{[y, v] : y \neq u\}| = 2k - 2$$

. □

Theorem 2.6. [3, Theorem 6.4.1, p. 118] *If a graph* Γ *is Eulerian then its line graph* $L(\Gamma)$ *is both Eulerian and Hamiltonian.*

Theorem 2.7. [3, Corollary 6.4.5, p. 119] *The line graph of a Hamiltonian graph is Hamiltonian.*

The *triangular graph* $L^1(K_n)$ is defined as the line graph of the complete graph K_n. The complete graph itself is the line graph of the star $K_{1,n}$ (see the example in Figure 2.1). Vertices of the triangular graph correspond to elements of $\Omega^{\{2\}}$. Hence $[u, v]$ is an edge of $L^1(K_n)$ if and only if $|u \cap v| = 1$. The triangular graph $L^1(K_4)$ is illustrated in Figure 2.2.

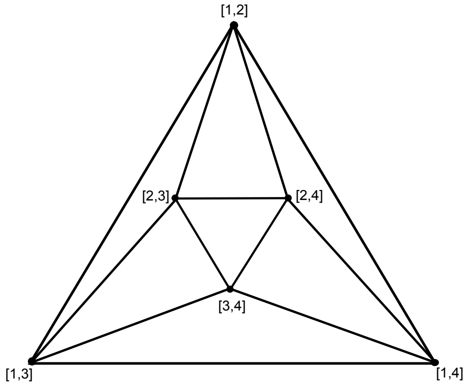

Figure 2.2: The triangular graph $L^1(K_4)$.

2.3.3 Graph homomorphisms

We now consider graph homomorphisms. These are used to characterise graphs considered in Chapter 4. Also, given two graphs Γ and H in Lemma 6.3, we need to determine if there is an isomorphism from Γ to H.

A *homomorphism* from a graph Γ to a graph H is a mapping $\alpha : V(\Gamma) \to V(H)$ such that $[u, v] \in E(\Gamma)$ implies that $[\alpha(u), \alpha(v)] \in E(H)$. If α is injective then it is an *embedding.* If α is bijective and α^{-1} is also a homomorphism then α is an *isomorphism.*

Two graphs Γ and H are *edge-isomorphic* if there exists a bijection σ between their edge sets that preserves adjacency of edges, i.e., $\sigma : E(\Gamma) \to E(H)$ is an edge-isomorphism if edges e and f are adjacent in Γ if and only if $\sigma(e)$ and $\sigma(f)$ are adjacent in H. 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 to H that induces σ. Whitney [64] proved that, with only four exceptions, edge isomorphisms between finite connected graphs are induced by graph isomorphisms. Exceptional cases have been illustrated by Hemminger in [30]. They include K_4. We state Whitney's result below as deduced from Hemminger [30].

Theorem 2.8. [30, Theorem 1] *Let α be a one-to-one function from the edge set of Γ onto the edge set of Γ' where Γ and Γ' are connected graphs. Then α is induced by an isomorphism of Γ onto Γ' if and only if α and α^{-1} preserve stars.*

Corollary 2.9. [30] (Whitney's Theorem for Line Graphs) *If Γ and Γ' are connected graphs with isomorphic line graphs then Γ and Γ' are isomorphic graphs unless one is isomorphic to K_3 and the other to $K_{1,3}$.*

An *automorphism* of a graph Γ is an isomorphism from the graph to itself. For a graph Γ, an automorphism α is just a permutation of its vertices that preserves adjacency, i.e., $[u, v] \in E(\Gamma)$ if and only if $[\alpha(u), \alpha(v)] \in E(\Gamma)$. We denote the group of automorphisms of a graph Γ by $\text{Aut}(\Gamma)$. Hence $\text{Aut}(\Gamma)$ is a subgroup of the symmetric group of all permutations of the vertex-set $V(\Gamma)$.

Since an automorphism α of a graph Γ maps edges to edges and non-edges to non-edges, we have the following.

Lemma 2.10. [27, Lemma 2.10] *The automorphism group of a graph is equal to the automorphism group of its complement.*

In general, it is not a trivial task to determine automorphisms of a given graph or whether a graph has non-trivial automorphisms. The case of K_n is rather obvious as any permutation of vertices is an automorphism. Hence $\text{Aut}(K_n) \cong S_n$ where S_n denotes the symmetric group on n elements. By Corollary 2.9, the automorphism group of a graph is isomorphic to that of its line graph. Hence,

Proposition 2.11. *For integers $i \geq 0$, $n \geq 3$ and $n \neq 4$, $\text{Aut}(L^i(K_n)) = S_n$ where $L^i(K_n)$ is the iterated line graph of K_n.*

A graph Γ is *vertex-transitive* if for any two vertices u and v, there is an automorphism $\alpha \in \text{Aut}(\Gamma)$ such that $\alpha(u) = v$. Hence, a vertex-transitive graph is one in which a given vertex cannot be distinguished from any other based on the vertices and edges surrounding it. Since the group actions on a graph and its complement are identical, a graph is vertex-transitive if and only if its complement is.

A graph Γ is *edge-transitive* if for any given two edges e and f there exists an automorphism $\alpha \in \mathrm{Aut}(\Gamma)$ such that $\alpha(e) = f$. It follows that the line graph of an edge-transitive graph is vertex-transitive. For example, it is clear that K_n is vertex- and edge-transitive. The vertex-transitivity of $L^1(K_n)$ is inherited from the edge-transitivity of K_n. It is also easily shown that $L^1(K_n)$ is edge-transitive and hence $L^2(K_n)$ is vertex-transitive. This phenomenon, however, does not continue *ad infinitum*. For instance, $L^2(K_n)$ is not, in general, edge-transitive as shown below.

Lemma 2.12. *If $n \geq 5$ then the iterated line graph $L^2(K_n)$ is not edge-transitive.*

Proof. Recall that edges of $L^2(K_n)$ have the form $[[A, B], [C, D]]$ where A, B, C and D are 2-element subsets of Ω such that $|A \cap B| = 1 = |C \cap D|$ and $|\{A, B\} \cap \{C, D\}| = 1$. By Proposition 2.11, $\mathrm{Aut}(L^2(K_n)) = S_n$ if $n \geq 5$. Let $\sigma \in S_n$. Then σ induces an edge-automorphism $\overline{\sigma} \in S_n$. Define a map $\overline{\sigma} : E(L^2(K_n)) \to E(L^2(K_n))$ by

$$\overline{\sigma}([[A, B], [C, D]]) = [[\overline{\sigma}(A), \overline{\sigma}(B)], [\overline{\sigma}(C), \overline{\sigma}(D)]]$$

where

$$\overline{\sigma}(\{a, b\}) = \{\overline{\sigma}(a), \overline{\sigma}(b)\}.$$

There is no automorphism $\overline{\sigma} \in S_n$ satisfying

$$\overline{\sigma}([[\{a, b\}, \{a, c\}], [\{a, b\}, \{a, d\}]]) = [[\{a, b\}, \{a, c\}], [\{a, b\}, \{b, d\}]].$$

□

2.3.4 Graph products

Graph products are used to construct new graphs ("products") from given ones ("factors"). Several graph products have been defined in literature. They are defined on the cartesian product of vertex sets of the factors. Adjacencies in the products depend on adjacencies in the factors. The graphs considered in Chapter 4 and Chapter 5 of this thesis are, respectively, *strong* and *categorical* products of triangular graphs and K_n. We give definitions of these products below including that of the *cartesian* product. In general, graph products take any number of graphs. We however restrict ourselves to products of two graphs. For the product taking any number of graphs, the interested reader is referred to Sabidussi [57].

Let Γ_1 and Γ_2 be graphs. A product $\Gamma_1 * \Gamma_2$ is a graph on the cartesian product $V(\Gamma_1) \times V(\Gamma_2)$. The definition of an edge $[(u_1, v_1), (u_2, v_2)] \in E(\Gamma_1 * \Gamma_2)$ depends on whether u_1 and u_2, and v_1 and v_2 are adjacent, identical or non-adjacent in their respective factors [34]. We give definitions of products of two graphs below by only specifying adjacency conditions.

Definition 2.13. [62, 57] The *cartesian product* of two graphs Γ_1 and Γ_2 is denoted $\Gamma_1 \Box \Gamma_2$ and

$$[(x,y),(x',y')] \in E(\Gamma_1 \Box \Gamma_2) \Longleftrightarrow x = x' \text{ and } [y,y'] \in E(\Gamma_2); \text{ or } \\ [x,x'] \in E(\Gamma_1) \text{ and } y = y'.$$

It follows that the cartesian product is both commutative and associative. In a remarkable result, Sabidussi [57] has shown that every connected graph can be expressed uniquely as a cartesian product of its prime factors. For example, the 4-cycle is the cartesian product $K_2 \Box K_2$.

Let Γ_1 and Γ_2 be graphs and let $v = (x, y) \in V(\Gamma_1 \Box \Gamma_2)$. Then

$$N(v) = (\{x\} \times N_{\Gamma_2}(y)) \cup (N_{\Gamma_1}(x) \times \{y\}).$$

Hence

$$\deg(v) = \deg_{\Gamma_1}(x) + \deg_{\Gamma_2}(y).$$

If Γ_1 is k-regular and Γ_2 is l-regular then $\Gamma_1 \Box \Gamma_2$ is $(k + l)$-regular.

Definition 2.14. [3] The *categorical product* (also called the *tensor product* or *Kronecker product*) of two graphs Γ_1 and Γ_2 is denoted $\Gamma_1 \times \Gamma_2$ and

$$[(u,v),(u',v')] \in E(\Gamma_1 \times \Gamma_2) \Leftrightarrow [u,u'] \in E(\Gamma_1) \text{ and } [v,v'] \in E(\Gamma_2).$$

The product is not necessarily commutative. It is equivalent to the Kronecker product of the adjacency matrices of the graphs. If $v = (x, y)$ is a vertex of $\Gamma_1 \times \Gamma_2$, then

$$N(v) = N_{\Gamma_1}(x) \times N_{\Gamma_2}(y).$$

Hence

$$\mathrm{d}(v) = \deg_{\Gamma_1}(v)\deg_{\Gamma_2}(v).$$

Definition 2.15. [3] The *strong product* of two graphs Γ_1 and Γ_2 is denoted $\Gamma_1 \boxtimes \Gamma_2$ and

$$\begin{aligned}[(u,v),(u',v')] \in E(\Gamma_1 \boxtimes \Gamma_2) \Longleftrightarrow & u = u' \text{ and } [v,v'] \in E(\Gamma_2);\ \text{or} \\ & [u,u'] \in E(\Gamma_1) \text{ and } v = v';\ \text{or} \\ & [u,u'] \in E(\Gamma_1) \text{ and } [v,v'] \in E(\Gamma_2).\end{aligned}$$

Equivalently,

$$\Gamma_1 \boxtimes \Gamma_2 = (\Gamma_1 \Box \Gamma_2) \cup (\Gamma_1 \times \Gamma_2).$$

The strong product is both commutative and associative.

2.3.5 Matchings and d-covered graphs

We now present definitions of independent sets, matchings and d-coveredness in graphs. Primarily, the focus is on sets of edges that are pairwise non-adjacent. Identifying such sets in a given graph provides a tool of determining if certain codes from the graph contain the all-one vector. This in turn is used to determine dimensions of the codes. These ideas are explored further in Section 2.4.

An *independent set* S in a graph $\Gamma = (V, E)$ is a subset of V in which no pair of vertices is adjacent, i.e., for any vertices u and v in S, $[u,v]$ is not an edge of Γ. Equivalently, each edge of Γ has at most one end point in S. If S is not a proper subset of another independent set then it is *maximal independent*. Adding any other vertex to a maximal independent set forces it to contain an edge. A maximal independent set of the largest size is *maximum*. One sees immediately that an independent set in a graph is a clique in the complement and vice-versa.

Let Γ be a graph. A subset $M \subseteq E(\Gamma)$ is a *matching* if no pair of edges is adjacent. M is a *perfect matching* if every vertex of the graph is incident with exactly one edge in M. Every graph with a perfect matching is even. A *defect-d* matching in a graph Γ is a matching M which covers all but d vertices of the graph. A graph is *d-covered* if for each edge e of Γ there exists a defect-d matching containing e. Thus a defect-0 matching is a perfect matching.

A characterisation of d-covered graphs is given by Little, Grant and Holton in [50]. They have shown that a k-regular graph Γ with edge-connectivity k or $k-1$ is 0-covered if $|V(\Gamma)|$ is even and 1-covered if $|V(\Gamma)|$ is odd. However, for any non-negative integers k and d, there exist k-regular graphs with edge-connectivity $k-2$ that have the parity of d but do not even have a defect-d matching. The following result has been used in Sections 3.4 and 6.4.3.

Theorem 2.16. [50, Theorem 4.4] *Every connected even vertex-transitive graph is* 0*-covered and every connected odd vertex-transitive graph is* 1*-covered.*

2.4 Codes from graphs and designs

Now that basics of codes, designs and graphs that are of interest to us have been considered in Sections 2.1, 2.2 and 2.3, respectively, we examine links between the three structures. The relationships are obtained through adjacency and incidence matrices of the graphs. If the graphs are regular, these matrices are also incidence matrices of certain designs from the graphs. The codes that we consider are generated by adjacency and incidence matrices of regular graphs.

2.4.1 Adjacency and incidence matrices of graphs; related designs and codes

In this section we define adjacency and incidence matrices of graphs. Corresponding neighbourhood and incidence designs are also described in the case of regular graphs. We also consider codes from the designs.

Let $\Gamma = (V, E)$ be a graph such that $|V(\Gamma)| = n$. An *adjacency matrix* $A = (a_{ij})$ of Γ is an $n \times n$ matrix with rows and columns indexed by vertices of Γ such that $a_{ij} = 1$ if vertices v_i and v_j are adjacent and $a_{ij} = 0$ otherwise. A is symmetric with zero diagonal.

An adjacency matrix of a graph is unique up to a permutation of rows and columns as it depends on the ordering of vertices. If the graph is regular, its adjacency matrix is also an incidence matrix of the neighbourhood design of the graph.

Definition 2.17. [19] The *neighbourhood design* $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ of a k-regular graph $\Gamma = (V, E)$ with n vertices is the $1-(n, k, k)$ design formed by taking points to be vertices of Γ and blocks to be sets of neighbours of a vertex, for each vertex.

Hence the neighbourhood design $\mathcal{D}$ is symmetric. The incidence vector of a block $\overline{u}$ of $\mathcal{D}$ corresponding to a vertex u of the graph is the vector

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

where v^u is the standard basis vector in $\mathbb{F}_p^n$ with entry 1 in the w-indexed coordinate position. $v^{\overline{u}}$ is also the row of A indexed by vertex u.

For any prime p, the p-ary linear code $C_p(A)$ is the span over $\mathbb{F}_p$ of rows of A, i.e.,

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

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

Another way of describing a graph is by using its incidence matrix. Let $\Gamma = (V, E)$ be a graph with n vertices and m edges. An *incidence matrix* $B = (b_{ij})$ of Γ is an $n \times m$ matrix such that $b_{ij} = 1$ if the ith vertex is an endpoint of the jth edge and $b_{ij} = 0$ otherwise. Rows and columns of B are indexed by, respectively, vertices and edges of the graph.

If Γ is regular then B is also an incidence matrix of the *incidence design* of the graph.

Definition 2.18. [19] The *incidence design* of a k-regular graph Γ with m edges is the $1-(m, k, 2)$ design formed by taking points to be edges of the graph and blocks to be sets of edges incident on a given vertex, for each vertex.

The block $\overline{u}$ of the incidence design contains edges incident with vertex u. It has incidence vector

$$v^{\overline{u}} = \sum_{[u,w] \in E(\Gamma)} v^{[u,w]}$$

where $v^{[u,w]}$ is the unit vector in $\mathbb{F}_p^m$ with coordinate entry 1 in the position indexed by $[u, w]$. $v^{\overline{u}}$ is also the row of B indexed by u. For any prime p, we denote by $C_p(B)$ the p-ary code spanned by rows of B. That is,

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

In Propositions 3.8 and 6.6, we will need the following relationship between an incidence matrix of a graph and an adjacency matrix of its line graph.

Proposition 2.19. [27, Lemma 8.2.2] *Let B be the incidence matrix of the graph Γ and let A be the adjacency matrix of the line graph $L(\Gamma)$. Then $B^T B = 2I + A$ where I is the $n \times n$ identity matrix.*

Over $\mathbb{F}_2$ we hence have

$$B^T B = A. \tag{2.2}$$

The following result gives a relationship between the automorphism group of a regular graph and that of the corresponding incidence design.

Lemma 2.20. [19, Lemma 1] *Let Γ be a k-regular graph with $m = |E|$ edges. Let $\mathcal{D}$ be the $1-(m, k, 2)$ incidence design from an incidence matrix of Γ. Then* $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\mathcal{D})$.

Let C be a code from an incidence matrix of a design $\mathcal{D}$. It is clear that every automorphism of $\mathcal{D}$ induces an automorphism of C. Hence $\mathrm{Aut}(\mathcal{D}) \subseteq \mathrm{Aut}(C)$.

2.4.2 Codes from incidence matrices of graphs

We now consider properties of codes from incidence matrices of graphs. We examine relationships between binary codes from these matrices and those from adjacency matrices of line graphs of the graphs. We also discuss properties of codes spanned by differences of rows of the incidence matrices.

Since an incidence matrix of a graph is made up of weight-2 column vectors, the following result is immediate.

Lemma 2.21. *If B is an incidence matrix of a graph $\Gamma = (V, E)$ then rows of B are linearly dependent over $\mathbb{F}_2$.*

If a graph Γ is connected, then the 2-rank of its incidence matrix B and hence the dimension of the binary code $C_2(B)$, is determined as follows.

Lemma 2.22. [1, Theorem 10, p. 140] *Let $\Gamma = (V, E)$ be a connected graph with $n = |V|$ vertices, $m = |E|$ edges and incidence matrix B. Then any $n-1$ rows of B are linearly independent over $\mathbb{F}_2$.*

Proof. Suppose $r_1, r_2, \cdots, r_d$ are $d \leq n-1$ linearly dependent rows of B. Then

$$r_1 + r_2 + \cdots + r_d = \mathbf{0}. \tag{2.3}$$

These rows correspond to d vertices of Γ. Because Γ is connected and each column of B has exactly two entries equal to 1, there is at least one edge e with one endpoint among these vertices and the other endpoint outside. The column corresponding to this edge has a single entry equal to one. The sum of the coordinates corresponding to this column cannot be zero, contradicting Equation (2.3). □

If any single row of an incidence matrix B of a graph is removed then the remaining $(n-1) \times m$ sub-matrix B^* has rank $n-1$. Hence only $n-1$ rows are needed to completely describe the corresponding graph. The vertex corresponding to the deleted row is a *reference vertex*. By Lemma 2.22, any vertex of Γ can be made a reference vertex.

For any odd prime p, if a given graph is connected then the p-rank of its incidence matrix B is determined using the following lemma, deduced from [46, Result 2].

Lemma 2.23. [46, Result 2] *Let $\Gamma = (V, E)$ be a connected graph with n vertices and incidence matrix B. For any odd prime p, if Γ is bipartite then* $\text{rank}_p(B) = n-1$ *while if Γ is not bipartite then* $\text{rank}_p(B) = n$*.*

In Lemma 2.24, some codewords in the duals of binary codes from incidence matrices of regular graphs are given. A similar result appears in [13].

Lemma 2.24. *Let $\Gamma = (V, E)$ be a regular graph with incidence matrix B. Let $C_2(B)$ be the binary code from the row span of B. If Γ has an l-cycle $C_l = (u_0, \cdots, u_{l-1})$ where $l \geq 3$, then*

$$c = v^{[u_0,u_1]} + v^{[u_1,u_2]} + \cdots + v^{[u_{l-2},u_{l-1}]} + v^{[u_{l-1},u_0]} \in C_2(B)^{\perp}.$$

Proof. For any $x \in V(\Gamma)$, we need to show that $(v^{\overline{x}}, c) = 0$ where $v^{\overline{x}}$ is the incidence vector of the block $\overline{x}$ in the incidence design of Γ.

Suppose $x \neq u_i$ for any $u_i \in C_l$. Then $v^{\overline{x}}$ and c are not commonly incident at any point. Hence $(v^{\overline{x}}, c) = 0$.

Suppose $x = u_i$ for some $u_i \in C_l$. Then $v^{\overline{x}}$ and c are commonly incident at $[u_{i-1}, u_i]$ and $[u_i, u_{i+1}]$ where the indices are added modulo l. Hence $(v^{\overline{x}}, c) = 2 \equiv 0 \pmod 2$. □

This result can be extended to codes over any prime field if $l \geq 4$ is even [13]. In this case, c takes the form

$$v^{[u_0,u_1]} - v^{[u_1,u_2]} + \cdots + v^{[u_{l-2},u_{l-1}]} - v^{[u_{l-1},u_0]}.$$

In Chapters 3 and 6, apart from codes from incidence designs $\mathcal{D}$ of the iterated line graphs $L^i(K_n)$, $i = 1, 2$, we have also considered the codes $E_F(\mathcal{D})$ obtained from the span of differences of incidence vectors of $\mathcal{D}$ over a field F. In general, this code has interesting properties. For instance, if a given graph Γ is connected and regular then the binary code from the span of differences of incidence vectors of $\mathcal{D}$ is equal to the binary code from the neighbourhood design of the line graph $L(\Gamma)$.

Formally, if $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is an incidence structure and F a field, the code $E_F(\mathcal{S})$ is obtained as follows.

$$\begin{aligned} E_F(\mathcal{S}) &= \left\langle v^C - v^D : C, D \in \mathcal{B} \right\rangle \\ &= \left\langle v^C - v^{C_0} : C \in \mathcal{B} \right\rangle \end{aligned} \tag{2.4}$$

where $C_0 \in \mathcal{B}$. The reader is referred to [2, p.44] for a thorough discussion on these codes and their properties. Since we consider codes over the prime field $\mathbb{F}_p$ and the design $\mathcal{D}$ has an incidence matrix B, $E_F(\mathcal{D})$ will be denoted $E_p(B)$.

Lemma 2.25. *Consider a regular graph Γ and its line graph $L(\Gamma)$. Let u and w be adjacent vertices of Γ, i.e, $[u, w]$ is a vertex of $L(\Gamma)$. Let $\overline{u}$ and $\overline{w}$ be blocks corresponding to vertices u and w in the incidence design of Γ and let $\overline{[u, w]}$ be the block in the neighbourhood design of $L(\Gamma)$ containing neighbours of vertex $[u, w]$ of $L(\Gamma)$. Then*

(a) $\overline{[u,w]} = \overline{u} \triangle \overline{w} = (\overline{u} \cup \overline{w}) \setminus \{[u,w]\}$;

(b) $v^{\overline{[u,w]}} = v^{\overline{u}} + v^{\overline{w}} - 2v^{[u,w]}$.

Proof. (a) In the neighbourhood design, the block $\overline{[u,w]}$ contains neighbours of $[u,w]$, i.e., elements of

$$\{[u,x] : x \neq w\} \cup \{[w,y] : y \neq u\}\,.$$

In the incidence design, this is equal to the set

$$\begin{aligned}&(\{[u,x] : x \neq u\} \cup \{[w,y] : y \neq w\}) \setminus \{[u,w]\}\\ &= (\overline{u} \cup \overline{w}) \setminus \{[u,w]\}.\end{aligned}$$

(b) Consider the incidence vector $v^{\overline{[u,w]}}$ in the neighbourhood design.

$$\begin{aligned}v^{\overline{[u,w]}} &= \sum_{x\neq u,w} v^{[u,x]} + \sum_{y\neq u,w} v^{[w,y]}\\ &= \sum_{x\neq u} v^{[u,x]} + \sum_{y\neq w} v^{[w,y]} - 2v^{[u,w]}\\ &= v^{\overline{u}} + v^{\overline{w}} - 2v^{[u,w]}.\end{aligned}$$

□

Over $\mathbb{F}_2$, Lemma 2.25(b) implies that $v^{\overline{[u,w]}} = v^{\overline{u}} + v^{\overline{w}}$, the difference of $v^{\overline{u}}$ and $v^{\overline{w}}$. Since $v^{\overline{[u,w]}}$ is also a row of an adjacency matrix of the line graph $L(\Gamma)$ of a graph Γ, we have the following result.

Corollary 2.26. *Let Γ be a regular graph with incidence matrix B and let $E_2(B)$ be the binary code spanned by differences of rows of B. Let $C_2(A)$ be the binary code from the row span of A, an adjacency matrix of the line graph $L(\Gamma)$. If Γ is connected then $C_2(A) = E_2(B)$.*

Proof. For any adjacent vertices u and w of Γ, we have $v^{\overline{[u,w]}} = v^{\overline{u}} + v^{\overline{w}} \in E_2(B)$ by Lemma 2.25(b). Hence $C_2(A) \subseteq E_2(B)$.

Conversely, suppose $v^{\overline{u}} + v^{\overline{w}} \in E_2(B)$. Since Γ is connected, there is a path connecting u and w. Let $u, u_1, u_2, \cdots, u_l, w$ be such a path. Then

$$\begin{aligned}v^{\overline{u}} + v^{\overline{w}} &= v^{\overline{u}} + v^{\overline{u_1}} + v^{\overline{u_1}} + \cdots + v^{\overline{u_l}} + v^{\overline{u_l}} + v^{\overline{w}}\\ &= v^{\overline{[u,u_1]}} + v^{\overline{[u_1,u_2]}} + \cdots + v^{\overline{[u_l,w]}},\end{aligned}$$

a sum of rows of A. Hence $v^{\overline{u}} + v^{\overline{w}} \in C_2(A)$. □

We now use Lemma 2.25(b) to give an alternative proof to Corollary 2.27, a result that also appears in [42]. The result holds for non-binary codes from adjacency matrices of line graphs of regular graphs with an l-cycle, l even.

Corollary 2.27. *Suppose a regular graph Γ has an l-cycle $(u_0, u_1, \cdots, u_{l-1})$ where $l \geq 4$ and l is even. Let A be an adjacency matrix of the line graph $L(\Gamma)$. Then, for any odd prime p, the code $C_p(A)$ from the row span of A over $\mathbb{F}_p$ has minimum weight l or less.*

Proof. Consider the codeword

$$v^{\overline{[u_0,u_1]}} - v^{\overline{[u_1,u_2]}} + \cdots + v^{\overline{[u_{l-2},u_{l-1}]}} - v^{\overline{[u_{l-1},u_0]}} \in C_p(A).$$

By Lemma 2.25(b),

$$\begin{aligned}
& v^{\overline{[u_0,u_1]}} - v^{\overline{[u_1,u_2]}} + \cdots + v^{\overline{[u_{l-2},u_{l-1}]}} - v^{\overline{[u_{l-1},u_0]}} \\
= \; & \left(v^{\overline{u}_0} + v^{\overline{u}_1} - 2v^{\overline{[u_0,u_1]}}\right) - \left(v^{\overline{u}_1} + v^{\overline{u}_2} - 2v^{\overline{[u_1,u_2]}}\right) + \cdots + \\
& \left(v^{\overline{u}_{l-2}} + v^{\overline{u}_{l-1}} - 2v^{\overline{[u_{l-2},u_{l-1}]}}\right) - \left(v^{\overline{u}_0} + v^{\overline{u}_{l-1}} - 2v^{\overline{[u_{l-1},u_0]}}\right) \\
= \; & -2v^{\overline{[u_0,u_1]}} + 2v^{\overline{[u_1,u_2]}} - \cdots + 2v^{\overline{[u_{l-1},u_0]}}.
\end{aligned}$$

Hence the minimum weight of $C_p(A)$ does not exceed l. □

The triangular graphs $L^1(K_n)$ and their line graphs $L^2(K_n)$ have 4-cycles. It hence follows that non-binary codes from the row span of adjacency matrices of $L^2(K_n)$ and $L^3(K_n)$ have minimum weight not exceeding 4. These codes are hence not examined in detail in Chapters 3 and 6, respectively.

Let $\mathcal{S}$ be an incidence structure with incidence matrix B. As has been noted, B^T is an incidence matrix of the dual structure $\mathcal{S}^t$. Let $E_F(B)$ be the code obtained from the span of differences of rows of B. The presence of the all-one vector $\jmath$ in $C_F(B^T)$, the code over F of $\mathcal{S}^t$, determines the dimension of $E_F(B)$ and whether $C_F(B) = E_F(B)$. Let $\jmath_{\mathcal{B}}$ be the all-one vector of length $|\mathcal{B}|$ and by $\jmath_{\mathcal{P}}$ the all-one vector of length $|\mathcal{P}|$.

Proposition 2.28. [2, Proposition 2.4.1, p. 46] *Let $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be an incidence structure with incidence matrix B and let F be a field. Then $E_F(B)$ has co-dimension at most 1 in $C_F(B)$ and $E_F(B) = C_F(B)$ if and only if $\jmath_{\mathcal{B}} \notin C_F(B^T)$. Dually, $E_F(B^T)$ has co-dimension at most 1 in $C_F(B^T)$ and $E_F(B^T) = C_F(B^T)$ if and only if $\jmath_{\mathcal{P}} \notin C_F(B)$.*

Proof. See [2, Proposition 2.4.1, p. 46]. □

Corollary 2.29. [2, Corollary 2.4.1, p. 46] *For any incidence structure S with incidence matrix B and any field F we have that $E_F(B)$ is of co-dimension 1 in $C_F(B)$ if and only if the all-one vector is in $C_F(B^T)$.*

If a regular graph Γ has a perfect matching then the presence of $\jmath$ in the code from the row span of the incidence matrix of the corresponding dual design is determined as follows.

Proposition 2.30. *Let $\Gamma = (V, E)$ be a regular graph with incidence matrix B. Let $C_p(B)$ be the p-ary code obtained from the row span of B over $\mathbb{F}_p$ where p is any prime. If Γ has a perfect matching then $\jmath \in C_p(B^T)$.*

Proof. Let $M = \{[u_1, w_1], \cdots, [u_k, w_k]\}$ be a perfect matching in Γ. Consider the dual design with incidence matrix B^T. Since no two edges in M have a common endpoint and each incidence vector $v^{\overline{[u_i,w_i]}}$ has weight two, we have $\sum_{1\le i\le k} v^{\overline{[u_i,w_i]}} = \jmath$, the all one vector of length $|V(\Gamma)|$. □

For example, since the complete graph is Hamiltonian, it has a perfect matching when it is even. By Theorem 2.7, the line graphs $L^i(K_n)$ are Hamiltonian. Hence the following result holds.

Corollary 2.31. *For $i \ge 0$, let $L^i(K_n)$ be the i-iterated line graph of the complete graph K_n. If $|V(L^i(K_n))|$ is even then $L^i(K_n)$ has a perfect matching.*

2.5 Information set decoding

The use of information sets as a basis for a decoding algorithm was introduced by Prange [55]. Since then variations of the principle have been introduced. These include decoding with multipliers [4], the use of covering polynomials [35], permutation decoding [52] and, more recently, antiblocking decoding [47]. Information set decoding is also used in code-based cryptography. The reader interested in this topic is referred to [54, 60] and references therein.

In general, information set decoding algorithms are designed to work for any linear code. They are based on the principle that if a received vector has no errors in information positions then the transmitted codeword can be reconstructed. Using a certain procedure and the fact that an information set of a given code is not unique, various information sets are identified until one is found such that there are no errors in information positions of a received vector. Hence all errors occurring outside information positions are correctable.

The following theorem is a basis for information set decoding techniques.

Theorem 2.32. [32, 33, 51] *Let C be an $[n, k, d]_q$ code with minimum distance $d \geq 2t + 1$. Let $H = [-A^T | I_{n-k}]$ be a parity check matrix for C in standard form. Suppose a codeword c is sent and a vector $y = c + e$ is received such that e has weight t or less. Then the information symbols of y are correct if and only if the syndrome Hy^T has weight t or less.*

Proof. See [32, Theorem 8.1, p. 1414] or [33, Theorem 10.2.1, p. 403]. □

In its basic form, information set decoding proceeds as follows. Suppose a t-error-correcting code C has a generator matrix M and an information set $\mathcal{I}$. Denote by $M_{\mathcal{I}}$ the restriction of M to its $\mathcal{I}$-indexed columns and by $y_{\mathcal{I}}$ the restriction of a vector $y \in \mathbb{F}_q^n$ to its $\mathcal{I}$-indexed coordinates. Note that M and $M_{\mathcal{I}}^{-1}M$ both generate C. Information set decoding takes as input a vector $y \in \mathbb{F}_q^n$ at a distance t or less from C. Suppose c is the codeword closest to y. If $y_{\mathcal{I}} = c_{\mathcal{I}}$ then y has no errors in $\mathcal{I}$. Hence $y_{\mathcal{I}}M_{\mathcal{I}}^{-1}$ is the original message and $y - (y_{\mathcal{I}}M_{\mathcal{I}}^{-1})M$ is the error vector.

By Theorem 2.32, if a parity check matrix H of a linear code is in standard form then information set decoding allows one to focus on the error pattern. If $\mathrm{wt}(Hy^T) \leq t$ then the error pattern is zero in $\mathcal{I}$ and the portion in the check positions is identical to the syndrome. Hence an error pattern is identified if a parity set completely containing it is found. Such a parity set is said to *cover* the error pattern. The collection of parity sets which covers all errors of a particular type is called a *covering*. Two questions arise at this point. The first one is, how can a covering be found? And the second is, what is the minimum number of parity sets in a covering? There is no obvious answer to the first question. It is however possible to obtain a lower bound on the minimum size of a covering.

Information set decoding is related to the combinatorial (n, l, t) *covering set problem* [10, 12] which is stated as follows. Given a set S of n objects, find the minimum number $N(n, l, t)$ of subsets of S of size l such that any subset of size t is contained in at least one of those of size l. With reference to an $[n, k, d]_q$ t-error-correcting code C, this is equivalent to finding the minimum size of the set of subsets of size $n - k$ covering every error pattern of size t, i.e., $l = n - k$. It is only necessary to concentrate on the t-error case since this also takes care of fewer than t errors. The total number of distinct error patterns in all positions is $\binom{n}{t}$. Since each covering set must have size t, the maximum number of t-tuples covered by a given parity set is $\binom{n-k}{t}$. Hence

$$\begin{aligned} N(n, n-k, t) &\geq \binom{n}{t} \Big/ \binom{n-k}{t} \\ &= \frac{n(n-1)\cdots(n-t+1)}{(n-k)(n-k-1)\cdots(n-k-t+1)}. \end{aligned}$$

Schonheim [58] showed that a tighter bound on N is given by

$$N(n, n-k, t) \geq \left\lceil \frac{n}{n-k} \left\lceil \frac{n-1}{n-k-1} \left\lceil \cdots \left\lceil \frac{n-t+1}{n-k-t+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil . \qquad (2.5)$$

This result is often referred to as the Gordon bound [41, 47]. It was used by Gordon [28] (using a result on coverings by Brouwer [8]) to find minimal PD-sets (see Section 2.5.1 for definition of PD-sets) for permutation decoding of binary Golay codes. In relation to the use of coverings in decoding, the result also appears in Clark and Cain [11, p. 110]. It is also stated and proved by Huffman [32, 33].

2.5.1 Permutation decoding

Permutation decoding was introduced by MacWilliams in [52]. It has been fully described in [51, Chapter 15], [32, Section 8] and [33, Section 10.2]. The technique uses a subset of the automorphism group of the code called a permutation decoding set.

A *permutation decoding set* (for short *PD-set*) S for a t-error-correcting code C is a set of automorphisms of C with the property that every error vector of weight at most t is mapped by at least one member of S into a vector where the error coordinates are only in check positions. The existence of a PD-set for a given code is not guaranteed. Much as PD-sets have been exhibited for some codes, there is no known general method of finding them.

Let C be a t-error-correcting linear code with PD-set $S = \{\sigma_1, \sigma_2, \cdots, \sigma_s\}$. Let H be a parity check matrix for C with I_{n-k} in redundancy positions. Hence the generator matrix M has I_k in the k information positions and the map $v \to vM$ for any length k vector v is a systematic encoder for C. If a vector y is received such that at most t errors occur, the permutation decoding algorithm, as stated in [32, 33], proceeds as follows.

- Compute the syndromes $H\sigma_i(y)^T$ for $i = 1, 2, \cdots$ until an i is found such that $\text{wt}(H\sigma_i(y)^T) \leq t$.
- Extract information symbols of $\sigma_i(y)$ and obtain the codeword $c \in C$ that has these information symbols.
- Decode y as $\sigma_i^{-1}(c)$.

The minimum size of a PD-set for a t-error-correcting $[n, k]_q$ code is given by the Gordon bound (see Equation (2.5)). In many cases, PD-sets that have been found are much larger than the Gordon bound. For examples, see the references at the end of this section.

The definition of PD-sets was generalised to that of *s-PD-sets* in [39] for purposes of correcting $s \leq t$ errors. An *s-PD-set S* for a t-error-correcting linear code C is a set of automorphisms of C with the property that every error vector of weight $s \leq t$ is mapped by at least one member of S into a vector where errors occur only in check positions. *Partial* permutation decoding is useful in cases where PD-sets for full error correction may not be found. It is also used in cases where the Gordon bound is greater than the size of the automorphism group of the code (cf. [39]). The minimum size of an s-PD-set is calculated by replacing t by s in the Gordon bound in Equation (2.5).

The following lemma finds a number s such that a code with an automorphism group G has G as an s-PD-set. The result depends only on the size of the information set.

Lemma 2.33. [40, Lemma 7] *Let C be a code with automorphism group G, information set $\mathcal{I}$, minimum distance d and check set $\mathcal{C}$. Denote by $\mathcal{O}$ a G-orbit and by n the maximum of $|\mathcal{O} \cap \mathcal{I}|/|\mathcal{O}|$. If $s = \min(\lceil \frac{1}{n} \rceil - 1, \lfloor \frac{d+1}{2} \rfloor)$ then G is an s-PD-set for C.*

The following theorem gives the worst-case time complexity of the permutation decoding algorithm. It is clear from the theorem that permutation decoding is more efficient the smaller the size of the PD-set.

Theorem 2.34. [49] *The worst-case time complexity of the permutation decoding algorithm can be expressed in terms of the size m of the s-PD set S, the dimension k and the length n of the code C. Permutation decoding requires at most $O(knm)$ operations in a worst-case situation.*

For a review of permutation decoding of various codes, the reader is referred to Huffman [32]. More recently, permutation decoding has been used for codes from graphs and designs. The reader is referred to [36, 37, 38] for Key's review of results on permutation decoding of codes from neighbourhood designs of various regular graphs. Other codes from graphs that permit permutation decoding but do not appear in these reviews include those examined in [17, 16, 21, 42].

2.6 Codes from complete graphs and triangular graphs

In this section we present pertinent results on non-binary codes from incidence matrices of complete graphs and binary codes from adjacency matrices of triangular graphs.

2.6.1 Codes from incidence matrices of complete graphs

Non-binary codes from the row span of incidence matrices of complete graphs have been considered by Key, Moori and Rodrigues in [42]. We will need results on these codes in Chapters 3, 4 and 5.

In [42], an incidence matrix G_n of K_n is written as follows. Rows are indexed by vertices of K_n in the order $1, \cdots, n$. Columns are ordered according to the following ordering of edges of K_n.

$$[1,2],[1,3],[2,3],[1,4],[2,4],[3,4],\cdots,[1,n],[2,n],\cdots,[n-1,n].$$

This way, G_n takes the form

$$\left[\begin{array}{c|c} G_{n-1} & I_{n-1} \\ \hline 0\cdots 0 & 1\cdots 1 \end{array}\right]. \tag{2.6}$$

where I_{n-1} is the identity matrix of rank $n-1$. We now summarise some properties of the p-ary linear codes $C_p(G_n)$ generated by G_n where p is any odd prime. Theorem 2.35 below can be deduced from Theorem 1 of [42].

Theorem 2.35. [42] *Denote by $C_p(G_n)$ the p-ary code from the row span of G_n, an incidence matrix of the complete graph K_n, where p is an odd prime and $n \geq 5$.*

(a) $C_p(G_n) = \left[\binom{n}{2}, n, n-1\right]_p$;

(b) *If $n \geq 6$ then the minimum words are the scalar multiples of the rows of G_n;*

(c) *For $n \geq 6$, $\mathrm{Aut}(C_p(G_n)) \cong S_n$, the symmetric group on $\Omega = \{1, \cdots, n\}$.*

2.6.2 Binary codes from triangular graphs

Binary codes from adjacency matrices of triangular graphs have been studied by Key, Moori and Rodrigues in [41] and [56]. Prior to this, they were examined by Tonchev [61] and later by Haemers, Peeters and van Rijckevorsel [29].

Let $C_2(A_n)$ be the binary code from the row span of an adjacency matrix A_n of the triangular graph. Let us first consider relationships between $C_2(A_n)$ and the binary codes $E_2(G_n)$ and $C_2(G_n)$ where $E_2(G_n)$ is obtained from the span of differences of rows of G_n, an incidence matrix of the complete graph K_n. The binary code $C_2(G_n)$ is obtained from the row span of G_n and it has parameters $[\binom{n}{2}, n-1, n-1]_2$ if n is odd.

By Lemma 2.26, $E_2(G_n) = C_2(A_n)$ for all n. By Proposition 2.28, if n is odd then $E_2(G_n) = C_2(G_n)$. By Corollary 2.29 and Lemma 2.30, if n is even then $E_2(G_n)$ has codimension 1 in $C_2(G_n)$. Relationships similar to these are also obtained in Chapter 3 between binary codes from incidence matrices of triangular graphs and those from adjacency matrices of their line graphs and in Chapter 6 between binary codes from incidence matrices of line graphs of triangular graphs and adjacency matrices of their line graphs.

We formally state some properties of $C_2(A_n)$ in Theorem 2.36 below. Notice that no particular ordering of rows or columns of A_n is assumed.

Theorem 2.36. [29, 41, 61] *Let $C_2(A_n)$ be the binary code obtained from the row span of an adjacency matrix A_n of the triangular graph $L^1(K_n)$ where $n \geq 5$.*

(a) $C_2(A_n) = [\binom{n}{2}, n-1, n-1]_2$ *if n is odd and* $C_2(A_n) = [\binom{n}{2}, n-1, 2(n-2)]_2$ *if n is even;*

(b) *If $n \geq 5$ and $n \neq 6$ then* $\mathrm{Aut}(C_2(A_n)) = S_n$. *If $n = 6$ then* $\mathrm{Aut}(C_2(A_n)) \cong A_8$*, the alternating group on* $\{1, \cdots, 8\}$.

2.7 Codes from the bipartite uniform subset graph $\Gamma(n, k, 1, 1)$

As has been mentioned in Section 2.3.1, codes from incidence matrices of the bipartite uniform subset graphs $\Gamma(n, k, l, i)$ (see Definition 2.4) for certain values of n, k, l and i have been considered in [22]. In Lemma 3.2, the following result on codes from incidence matrices $M(n, k, 1, 1)$ of $\Gamma(n, k, 1, 1)$, where $n \geq 4$ and $n \geq k$, will be used.

Proposition 2.37. [22, Proposition 2] *For all $n \geq 4$, $n \geq k$, all primes p, $C = C_p(M(n, k, 1, 1))$ has minimum weight k if $n > k$, 1 if $n = k$ and the minimum words are the non-zero scalar multiples of the rows of $M(n, k, 1, 1)$ of weight k or 1, respectively. For $n > k$, $C = \left[k\binom{n}{k}, \binom{n}{k} + n - 1, k\right]_p$ for all p.*

Chapter 3

Codes from incidence matrices of triangular graphs

3.1 Introduction

In this chapter we examine p-ary linear codes $C_p(B_n)$ from the row span of B_n, an incidence matrix of the triangular graph $L^1(K_n)$, where $n \geq 3$ and p is a prime. We also consider the codes $C_2(A_n)$ and $E_p(B_n)$ where $C_2(A_n)$ is the binary code from the row span of an adjacency matrix of the line graph of the triangular graph $L^2(K_n)$ and $E_p(B_n)$ is the p-ary code, p any prime, from the span of the differences of the rows of B_n. In all cases, parameters of the codes and their duals are obtained. We also determine permutation automorphisms for the codes and exhibit PD-sets for full permutation decoding.

Part of the work in this chapter is the content of [23]. Our main results are summarized in Theorem 3.1.

Theorem 3.1. *For $n \geq 4$, let B_n be an incidence matrix of $L^1(K_n)$, the line graph of the complete graph, i.e., the triangular graph. Let A_n be an adjacency matrix of $L^2(K_n)$, the line graph of the triangular graph. For any prime p, let $C_p(B_n)$ and $C_p(A_n)$ be the p-ary linear codes spanned by the rows of B_n and A_n, respectively. Let $E_p(B_n) = \langle r_i - r_j | r_i, r_j$ are rows of $B_n\rangle$ where the span is also taken over $\mathbb{F}_p$. Then we have the following:.*

(a) *If p is odd then $C_p(B_n)$ is an $\left[(n-2)\binom{n}{2}, \binom{n}{2}, 2(n-2)\right]_p$ code. If $p = 2$*

then $C_2(B_n)$ *is an* $\left[(n-2)\binom{n}{2}, \binom{n}{2}-1, 2(n-2)\right]_2$ *code. In both cases, the minimum words are the scalar multiples of the rows of* B_n*.*

(b) *If* $n \geq 5$ *then* $\mathrm{Aut}(C_p(B_n)) \cong \mathrm{Aut}(L^1(K_n)) = S_n$*.*

(c) *If* $n \equiv 0, 1 \pmod 4$ *then* $C_2(A_n)$ *is an* $\left[(n-2)\binom{n}{2}, \binom{n}{2}-2, 4n-10\right]_2$ *code and its minimum words are the rows of* A_n*. If* $n \equiv 2, 3 \pmod 4$ *then* $C_2(A_n) = E_2(B_n) = C_2(B_n)$*.*

(d) *If* p *is odd and* $n = 4$ *then* $E_p(B_4)$ *is a* $[12, 5, 4]_p$ *code and its minimum words include scalar multiples of vectors of the form* $u = v^{\overline{[a,b]}} + v^{\overline{[b,d]}} + v^{\overline{[c,d]}} - v^{\overline{[b,c]}} - v^{\overline{[a,d]}} - v^{\overline{[a,c]}}$ *where* $a, b, c, d \in \{1, 2, 3, 4\}$ *and* $v^{\overline{[i,j]}}$ *is the row of* B_4 *corresponding to the vertex* $[i, j]$*.*

(e) *If* p *is odd and* $n \geq 5$ *then* $E_p(B_n)$ *is an* $\left[(n-2)\binom{n}{2}, \binom{n}{2}-1, 4n-10\right]_p$ *code and its minimum words are the scalar multiples of the differences of the pairs of rows of* B_n *indexed by adjacent vertices of* $L^1(K_n)$*.*

(f) *If* $n \geq 5$ *then*

$$\mathcal{I}_n = \{[[1,2],[1,x]], [[1,y],[y,z]] : 3 \leq x \leq n, 2 \leq y < z \leq n\}$$

is an information set for $C_2(B_n)$*. The code has PD-set*

$$S = \{(1), (1, \check{z}), (1, \check{z}, \check{x}) : \check{x}, \check{z} \neq 1, 2\},$$

a set of $1 + \binom{n-1}{2}$ *elements of* S_n*.*

(g) *If* p *is odd and* $n \geq 5$ *then* $\mathcal{I}_n \cup \{[[1,3],[1,4]]\}$ *is an information set for* $C_p(B_n)$*. The set*

$$S \setminus \{(1,3), (1,4), (1,3,4), (1,4,3)\}$$

is a PD-set for the code.

The proof of the theorem follows from lemmas and propositions presented in various sections below. The rest of the chapter is organised as follows. In Section 3.2 an incidence matrix B_n of $L^1(K_n)$ is written inductively. A brief description is also given of how the codes $C_p(A_n)$ and $E_p(B_n)$ are obtained.

Results on the binary and non-binary codes $C_p(B_n)$, their duals and automorphisms are presented in Section 3.3. The codes $C_2(A_n)$ are considered in Section 3.4. We examine the non-binary codes $E_p(B_n)$ in Section 3.5. Permutation decoding for the codes is considered in Section 3.6.

3.2 The incidence matrix B_n of $L^1(K_n)$ and related codes

Let B_n be an incidence matrix of the triangular graph $L^1(K_n)$ where $n \geq 3$. We write B_n in inductive form as follows. Starting with $n = 3$, rows of B_3 are ordered according to the ordering

$$[1,2],[1,3],[2,3]$$

of vertices of the triangle $L^1(K_3)$. Columns are indexed by edges of $L^1(K_3)$ in the order

$$[[1,2],[1,3]],[[1,2],[2,3]],[[1,3],[2,3]].$$

Hence B_3 takes the form

$$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}. \tag{3.1}$$

For each $n > 3$ we add to B_{n-1} rows corresponding to the vertices

$$[1,n],[2,n],\cdots,[n-1,n],$$

in that order. Additional columns are indexed by edges connecting vertices of $L^1(K_{n-1})$ and the new vertices and, lastly, by edges between the new vertices. Hence B_n is an $\binom{n}{2} \times (n-2)\binom{n}{2}$ matrix of the form

$$\left[\begin{array}{c|c|c} B_{n-1} & L & \mathbf{0} \\ \hline \mathbf{0} & M & G_{n-1} \end{array}\right] \tag{3.2}$$

where

(a) B_{n-1} is an incidence matrix of the triangular graph $L^1(K_{n-1})$;

(b) L is an $\binom{n-1}{2} \times (n-2)(n-1)$ with only one entry 1 in each column. Each row has weight two and the two non-zero entries are consecutive;

(c) M is an $(n-1)\times(n-2)(n-1)$ matrix with one entry 1 in each column is a unit vector and each row has weight $n-2$;

(d) G_{n-1} is an incidence matrix of the complete graph K_{n-1}. Recall that linear codes from these matrices have been considered in [42] and discussed in Section 2.6.1.

The incidence design of $L^1(K_n)$ with incidence matrix B_n will be denoted $\mathcal{D}_n$ and the corresponding p-ary linear code by $C_p(B_n)$. If $[a,b]$ is any vertex of the graph then

$$\overline{[a,b]} = \{[[a,b],[a,x]],[[a,b],[b,x]] : x \neq a,b\}$$

is the block of $\mathcal{D}_n$ containing all edges incident with $[a,b]$. The incidence vector of the block is the weight-$(2n-4)$ vector

$$v^{\overline{[a,b]}} = \sum_{x\neq a,b} v^{[[a,b],[a,x]]} + \sum_{y\neq a,b} v^{[[a,b],[b,y]]}.$$

Let A_n be an adjacency matrix of $L^2(K_n)$, the line graph of the triangular graph. The neighbourhood design of $L^2(K_n)$ with incidence matrix A_n has incidence vectors of the form

$$v^{\overline{[[a,b],[b,c]]}} = \sum_{w\neq a,b} v^{[[a,b],[a,w]]} + \sum_{x\neq a,b,c} v^{[[a,b],[b,x]]} + \sum_{y\neq a,b,c} v^{[[b,c],[b,y]]} + \sum_{z\neq b,c} v^{[[b,c],[c,z]]}.$$

These vectors have weight $4n-10$ and they are also rows of A_n. The p-ary code with generator matrix A_n will be denoted $C_p(A_n)$.

We will also be interested in the p-ary code $E_p(B_n)$ obtained from the span over $\mathbb{F}_p$, p any prime, of the differences of rows of B_n. Hence by Equation (2.4),

$$\begin{aligned} E_p(B_n) &= \left\langle v^{\overline{[a,b]}} - v^{\overline{[c,d]}} : [a,b],[c,d] \in V(L^1(K_n)) \right\rangle \\ &= \left\langle v^{\overline{[a,b]}} - v^{\overline{[a_0,b_0]}} : [a,b] \in V(L^1(K_n)) \right\rangle \qquad (3.3) \end{aligned}$$

where $[a_0,b_0]$ is a fixed vertex of $L^1(K_n)$.

3.3 The code $C_p(B_n)$ from an incidence matrix of $L^1(K_n)$

We now discuss the main thrust of this chapter, namely, the codes $C_p(B_n)$ where p is a prime and $n \geq 3$.

The case of $n = 3$ follows rather easily. If $p = 2$ then $C_2(B_3) = [3, 2, 2]_2$. Because $C_2(B_3) = \{000, 110, 101, 011\}$, minimum words of the code are the rows of B_3. If p is odd then $C_p(B_3) = [3, 3, 1]_p$. Unit vectors are obtained from the difference between the sum of any two rows of B_3 and the third row.

3.3.1 The code $C_p(B_4)$

We now consider the case of $n = 4$. By Equation (3.2), $L^1(K_4)$ has incidence matrix

$$B_4 = \left[\begin{array}{c|c|c} 110 & 110000 & 000 \\ 101 & 001100 & 000 \\ 011 & 000011 & 000 \\ \hline 000 & 101000 & 110 \\ 000 & 010010 & 101 \\ 000 & 000101 & 011 \end{array}\right]. \tag{3.4}$$

Since $K_3 = L^i(K_3)$ for all i, we have $B_3 = G_3$ in B_4. Also observe that the submatrix $\left[\frac{L}{M}\right]$ of B_4 (where L and M are as in Equation (3.2)), is an incidence matrix of the bipartite uniform subset graph $\Gamma(3, 2, 1, 1)$ (see Definition 2.4).

Parameters of the p-ary codes $C_p(B_4)$, p any prime, are determined in Lemma 3.2. The lemma is used as an induction base in Proposition 3.3 to establish minimum weights and minimum words of $C_p(B_n)$ where $n \geq 5$.

Lemma 3.2. *Let B_4 be an incidence matrix of $L^1(K_4)$ and $C_p(B_4)$ the p-ary linear code from the row span of B_4 where p is any prime.*

(a) *If p is odd then $C_p(B_4) = [12, 6, 4]_p$ and its minimum words include the rows of B_4.*

(b) *If $p = 2$ then $C_2(B_4) = [12, 5, 4]_2$ and its minimum words are the rows of B_4.*

Proof. Dimensions of the non-binary and binary codes follow from Lemma 2.23 and Lemma 2.22, respectively, since the triangular graph $L^1(K_4)$ is connected and, having triangles, it is also non-bipartite.

Write B_4 as in Equation (3.4). Label the first three rows by R_1 and the last three rows by R_2. Let $c \in C_p(B_4)$. Then c is a concatenation of three vectors, c_1, c_2 and c_3, from the three column blocks of B_4 where $c_1 \in \mathbb{F}_p^3$, $c_2 \in \mathbb{F}_p^6$ and $c_3 \in \mathbb{F}_p^3$. We need to show that $\text{wt}(c) \geq 4$.

(a) Suppose c is a linear combination of r_1 rows of R_1. Then $\text{wt}(c_1) \geq 1$ since $C_p(B_3) = [3, 3, 1]_p$ if p is odd. Also, $\text{wt}(c_2) = 2r_1$. If $\text{wt}(c_1) = 1$ then $\text{wt}(c_2) = 6$ because the only linear combinations of the rows of B_3 giving a unit vector use all rows of R_1. Hence $\text{wt}(c) > 4$. If $\text{wt}(c_1) = 2$ then, since $\text{wt}(c_2) = 2r_1$, we have $\text{wt}(c) \geq 2 + 2r_1 \geq 4$. Equality occurs if c is a scalar multiple of a row of R_1. Similar observations are made if c is a linear combination of rows of R_2.

If c is a linear combination of r_1 rows of R_1 and r_2 rows of R_2 then $\text{wt}(c_1) \geq 1$ and $\text{wt}(c_3) \geq 1$. Since $\left[\frac{L}{M}\right]$ is an incidence matrix of the bipartite uniform subset graph $\Gamma(3, 2, 1, 1)$, $\text{wt}(c_2) \geq 2$ by Proposition 2.37. Hence $\text{wt}(c) \geq 4$. This completes the proof for the non-binary case.

(b) In the binary case, suppose c is a sum of rows of R_1. Then $\text{wt}(c_1) = 2$ since $C_2(B_3) = [3, 2, 2]_2$. Because $\text{wt}(c_2) \geq 2$, we have $\text{wt}(c) \geq 4$. From the form of B_4, it is clear that $\text{wt}(c) = 4$ if c is a row of R_1. A similar observation is made if c is a sum of rows of R_2.

Suppose c is a sum of r_1 rows of R_1 and r_2 rows of R_2. If $r_1 < 3$ and $r_2 < 3$ then $\text{wt}(c_1) = 2 = \text{wt}(c_3)$. By Proposition 2.37, $\text{wt}(c_2) \geq 2$. Hence $\text{wt}(c) > 4$.

We also need to consider cases when all rows of R_1 or R_2 are added since these give, respectively, $c_1 = \mathbf{0}$ and $c_3 = \mathbf{0}$. Suppose we add all rows of R_1 and $r_2 < 3$ rows of R_2. Then $c_1 = \mathbf{0}$, $\text{wt}(c_2) \geq 2$ and $\text{wt}(c_3) = 2$. Hence $\text{wt}(c) \geq 4$. It is possible to have $\text{wt}(c) = 4$ if $r_2 = 2$. In this case, c is the row of R_2 that is not added. The case of $r_1 < 3$ and $r_2 = 3$ is similar. This completes the proof for $n = 4$. □

If p is odd then, from the proof of Lemma 3.2(a), it is possible to have other minimum words in addition to the rows of B_4. These include scalar multiples of vectors of the form

$$\left(v^{\overline{[a,b]}} + v^{\overline{[b,d]}} + v^{\overline{[c,d]}}\right) - \left(v^{\overline{[b,c]}} + v^{\overline{[a,d]}} + v^{\overline{[a,c]}}\right) \tag{3.5}$$

$$= 2\left(v^{[[a,b],[b,d]]} + v^{[[b,d],[d,c]]} - v^{[[a,c],[a,d]]} - v^{[[a,c],[b,c]]}\right) \tag{3.6}$$

where $a, b, c, d \in \{1, 2, 3, 4\}$. These are the only codewords of minimum weight we have been able to determine apart from scalar multiples of the rows of B_4.

3.3.2 The code $C_p(B_n)$ where $n \geq 5$

We now consider the codes $C_p(B_n)$ where $n \geq 5$ and p is any prime. Minimum weights and minimum words of the codes are determined in Proposition 3.3 below.

Proposition 3.3. *Let B_n be an incidence matrix of $L^1(K_n)$ and let $C_p(B_n)$ be the p-ary code from the row span of B_n where $n \geq 5$ and p is any prime.*

(a) *If p is odd then $C_p(B_n) = \left[(n-2)\binom{n}{2}, \binom{n}{2}, 2(n-2)\right]_p$ and its minimum words are the scalar multiples of the rows of B_n.*

(b) *$C_2(B_n) = \left[(n-2)\binom{n}{2}, \binom{n}{2} - 1, 2(n-2)\right]_2$ and its minimum words are the rows of B_n.*

Proof. As in Lemma 3.2, dimensions of the codes are obtained using Lemmas 2.23 and 2.22. We therefore only need to prove the minimum weight of the codes.

Write B_n as in Equation (3.2). Label the first $\binom{n-1}{2}$ rows of the matrix by R_1, i.e., R_1 is the submatrix $[B_{n-1}|L|\mathbf{0}]$. Let R_2 be the submatrix $[\mathbf{0}|M|G_{n-1}]$ comprising the last $n-1$ rows of B_n. For any prime p, let $c \in C_p(B_n)$. Then c is a concatenation of three vectors $c_i \in \mathbb{F}_p^{k_i}$ from the three column blocks of B_n where $k_1 = (n-2)\binom{n-1}{2}$, $k_2 = 2\binom{n-1}{2}$ and $k_3 = \binom{n-1}{2}$.

We use induction to prove the assertion about the minimum weight and minimum words using the case of $C_p(B_4)$ considered in Lemma 3.2 as the induction base. We assume that the minimum weight holds up to $n-1$ and that minimum words are the rows of B_{n-1}.

(a) Suppose c is a non-zero linear combination of r_1 rows of R_1. Then $c_1 = \sum \alpha_i b_i$ and $c_2 = \sum \alpha_i l_i$ where $\alpha_i \in \mathbb{F}_p^*$ and b_i and l_i are ith rows of B_{n-1} and L, respectively. By the induction hypothesis, $\mathrm{wt}(c_1) \geq 2(n-3)$. Since $\mathrm{wt}(c_2) = 2r_1$, we have $\mathrm{wt}(c) \geq 2(n-3) + 2r_1 \geq 2(n-2)$. Equality occurs if $r_1 = 1$, i.e., if c is a scalar multiple of a row of R_1.

If c is a non-zero linear combination of r_2 rows of R_2 then $c_2 = \sum \alpha_i m_i$ and $c_3 = \sum \alpha_i g_i$ where $\alpha_i \in \mathbb{F}_p^*$ and m_i and g_i are ith rows of M and G_{n-1}, respectively. Since no two rows of M intersect, we have $\mathrm{wt}(c_2) = r_2(n-2)$. By Theorem 2.35, $\mathrm{wt}(c_3) \geq n-2$. Hence $\mathrm{wt}(c) \geq (r_2+1)(n-2) \geq 2(n-2)$. Equality occurs if $r_2 = 1$, i.e., if c is a scalar multiple of a row of R_2.

Lastly, suppose c is a linear combination of r_1 rows of R_1 and r_2 rows of R_2. Then $c_1 = \sum \alpha_i b_i$, $c_2 = \sum (\alpha_i l_i + \alpha_j m_j)$ and $c_3 = \sum \alpha_j g_j$ where b_i, l_i, m_j and g_j are, respectively, rows of B_{n-1}, L, M and G_{n-1}. By the induction hypothesis, $\mathrm{wt}(c_1) \geq 2(n-3)$. Since $\mathrm{wt}(c_3) \geq n-2$ by Theorem 2.35, we have $\mathrm{wt}(c) \geq 2(n-3) + (n-2) > 2(n-2)$.

(b) For the binary codes, in addition to what has been considered in (a) above when p is odd, we need to examine the weight of c if all rows of R_1 or R_2 are added since these give, respectively, $c_1 = \mathbf{0}$ and $c_3 = \mathbf{0}$.

Suppose c is a sum of all rows of R_1 and $r_2 < n-1$ rows of R_2. Then $\mathrm{wt}(c_2) = 2\binom{n-1}{2} - r_2(n-2)$. By Theorem 2.35, $\mathrm{wt}(c_3) \geq n-2$. Hence $\mathrm{wt}(c) \geq 2\binom{n-1}{2} - r_2(n-2) + (n-2) = (n-r_2)(n-2) \geq 2(n-2)$ where $1 \leq r_2 \leq n-2$. Equality holds if $r_2 = n-2$. In this case, c is the row of R_2 that is not added.

If c is a sum of all rows of R_2 and $r_1 < \binom{n-1}{2}$ rows of R_1 then $\mathrm{wt}(c_1) \geq 2(n-3)$ and $\mathrm{wt}(c_2) \geq (n-1)(n-2) - 2r_1$ where $1 \leq r_1 \leq \binom{n-1}{2} - 1$. Hence $\mathrm{wt}(c) \geq 2(n-3) + (n-1)(n-2) - 2r_1 \geq 2(n-2)$. Equality holds if $r_1 = \binom{n}{2} - 1$ in which case c is the row of R_1 that is not added. This completes the proof. □

3.3.3 The dual code $C_2(B_n)^\perp$

We now consider some properties of the duals of the binary codes. We first present weight-3 vectors of the dual in Lemma 3.4.

Lemma 3.4. *For* $n \geq 3$, *let* $\mathcal{D}_n$ *be the incidence design of the triangular graph* $L^1(K_n)$. *Let* $a, b, c, d \in \Omega$.

(a) *The weight-*3 *vectors of the form*

$$\begin{aligned} u(a,b,c) &= v^{[[a,b],[a,c]]} + v^{[[a,b],[b,c]]} + v^{[[a,c],[b,c]]}, \\ u(a,b,c,d) &= v^{[[a,b],[b,c]]} + v^{[[a,b],[b,d]]} + v^{[[b,c],[b,d]]}, \end{aligned} \tag{3.7}$$

are in $C_2(B_n)^\perp$.

(b) $C_2(B_n)^\perp$ *has minimum weight* 3.

Proof. That $u(a,b,c)$ and $u(a,b,c,d)$ are in $C_2(B_n)^\perp$ is a consequence of Lemma 2.24. We therefore only need to prove (b).

To show that $C_2(B_n)^\perp$ has minimum weight 3, we first observe that the dual has no codewords of weight 1. This is because for any incidence vector $v^{\overline{[a,b]}}$, there exists a unit codeword $v^{[[a,b],[a,c]]}$ such that $(v^{\overline{[a,b]}}, v^{[[a,b],[a,c]]}) \neq 0$. Hence $v^{[[a,b],[a,c]]} \notin C_2(B_n)^\perp$.

Also, for any incidence vector u of $\mathcal{D}_n$, there exists a weight-2 vector w such that $(u, w) \neq 0 \pmod 2$. For example, let $u = v^{\overline{[a,b]}}$ and $w = v^{[[a,b],[a,c]]} + v^{[[a,c],[a,d]}$. Since the dual has weight-3 codewords, the minimum weight follows. This completes the proof of the lemma. □

There are $\binom{n}{3}$ codewords of the form $u(a,b,c)$ and $4\binom{n}{4}$ of the form $v(a,b,c,d)$ in the dual. In the next proposition, we show that these are the only minimum words of the dual.

Proposition 3.5. *Let* $C_2(B_n)^\perp$ *be the dual of the binary code from the row span of* B_n, *an incidence matrix of the triangular graph* $L^1(K_n)$ *where* $n \geq 3$. *Then the weight-*3 *vectors given in* Equation (3.7) *are the only minimum words of* $C_2(B_n)^\perp$.

Proof. Let w be a minimum word of $C_2(B_n)^\perp$. Let $[[a,b],[b,c]] \in \text{Supp}(w)$. We need to determine all possibilities for the remaining two elements X and

Y of Supp(w). Note that $[[a,b],[b,c]] \in \overline{[a,b]}, \overline{[b,c]}$. We must have $X \in \overline{[a,b]}$ and $Y \in \overline{[b,c]}$ or $X \in \overline{[b,c]}$ and $Y \in \overline{[a,b]}$. This assumption is reasonable because if X or Y is not in $\overline{[a,b]}$ or $\overline{[b,c]}$ then $(v^{\overline{[a,b]}}, w) = 1 = (v^{\overline{[b,c]}}, w)$, contradicting the assumption that w is in the dual.

Without loss of generality, suppose $X \in \overline{[a,b]}$ and $Y \in \overline{[b,c]}$. Let $X = [[a,b],[x,y]]$ and $Y = [[b,c],[x',y']]$. To satisfy the required conditions, we must also have $[x,y] = [x',y']$. Otherwise, one obtains $(v^{\overline{[x,y]}}, w) = 1 = (v^{\overline{[x',y']}}, w)$.

Consider the point $X = [[a,b],[x,y]]$. By definition, either $x = a$ or $x = b$. If $x = a$ then $y = c$. Hence

$$\text{Supp}(w) = \{[[a,b],[b,c]], [[a,b],[a,c]], [[b,c],[a,c]]\}.$$

Thus w is of the form $u(a,b,c)$ given in Equation (3.7). If $x = b$ then $y = d$. In this case

$$\text{Supp}(w) = \{[[a,b],[b,c]], [[a,b],[b,d]], [[b,c],[b,d]]\},$$

i.e., w is of the form $u(a,b,c,d)$ given in Equation (3.7). Hence $u(a,b,c)$ and $u(a,b,c,d)$ are the only minimum words of $C_2(B_n)^\perp$. □

Let x and y be elements of Ω such that $x < y$. Consider the following codewords in the dual.

$$\begin{aligned}
p(x,y,j) &= v^{[[x,y],[x,j]]} + v^{[[x,y],[x,(j+1)]]} + v^{[[x,j],[x,(j+1)]]} \text{ where } y < j < n,\\
q(x,y,n) &= v^{[[x,y],[x,n]]} + v^{[[x,y],[y,n]]} + v^{[[x,n],[y,n]]},\\
r(x,y,n) &= v^{[[x,n],[y,n]]} + v^{[[x,n],[(y+1),n]]} + v^{[[y,n],[(y+1),n]]},\\
s(x,y,j) &= v^{[[x,y],[y,j]]} + v^{[[x,y],[y,(j+1)]]} + v^{[[y,j],[y,(j+1)]]} \text{ where } x < j < n.
\end{aligned} \tag{3.8}$$

In $s(x,y,j)$, if $j+1 = y$ then take $j+1$ to be $y+1$. In the proof of Lemma 3.6 below, we refer to the vectors $v^{[[x,y],[x,j]]}$, $v^{[[x,y],[x,n]]}$, $v^{[[x,n],[y,n]]}$ and $v^{[[x,y],[y,j]]}$ as leading vectors and show that they are linearly independent. We count them to show that p, q, r and s form a basis of minimum weight vectors for the dual.

Lemma 3.6. *For* $n \geq 3$, $x < y$, *and* $[x,y] \neq [n-1,n]$, $C_2(B_n)^\perp$ *has a basis of minimum weight comprising the vectors* $p(x,y,j)$ *where* $y < j < n$, $q(x,y,n)$, $r(x,y,n)$ *and* $s(x,y,j)$ *where* $x < j < n$ *given in* Equation (3.8) *above.*

Proof. Each leading vector is used exactly once hence when re-ordered, the vectors p, q, r and s above yield a matrix in upper triangular form. The only unit vectors that are not used as leading vectors are the $\binom{n-1}{2}$ vectors of the form $v^{[[x,y],[y,n]]}$ and the $n-2$ vectors of the form $v^{[[x,n],[n,(n-1)]]}$. Since the design has $(n-2)\binom{n}{2}$ points, the total number of leading vectors is

$$\begin{aligned}
&(n-2)\binom{n}{2} - \binom{n-1}{2} - (n-2) \\
&= (n-2)\binom{n}{2} - \left(\binom{n}{2} - 1\right) \\
&= \dim(C_2(B_n)^{\perp}).
\end{aligned}$$

We therefore have a basis for $C_2(B_n)^{\perp}$. □

3.3.4 Automorphisms of codes from incidence matrices of triangular graphs

We now consider permutation automorphisms of the codes $C_p(B_n)$ for any prime p.

Proposition 3.7. *Let $\mathcal{D}_n$ be the incidence design of the triangular graph $L^1(K_n)$ with incidence matrix B_n where $n \geq 5$. Let $C_p(B_n)$ be the p-ary linear code from the row span of B_n where p is any prime. Then* $\mathrm{Aut}(C_p(B_n)) \cong \mathrm{Aut}(\mathcal{D}_n) = \mathrm{Aut}(L^1(K_n)) = S_n$.

Proof. By Proposition 2.11, $\mathrm{Aut}(L^1(K_n)) \cong S_n$. By Lemma 2.20, $\mathrm{Aut}(\mathcal{D}_n) = \mathrm{Aut}(L^1(K_n))$. Since every automorphism of the graph induces an automorphism of the code, we have $\mathrm{Aut}(L^1(K_n)) \subseteq \mathrm{Aut}(C_p(B_n))$. To show that $\mathrm{Aut}(C_p(B_n)) \cong S_n$ it is hence sufficient to show that $\mathrm{Aut}(C_p(B_n)) \subseteq \mathrm{Aut}(\mathcal{D}_n)$.

By Proposition 3.3, if $n \geq 5$ then minimum words of $C_p(B_n)$ are scalar multiples of incidence vectors of blocks of $\mathcal{D}_n$. Let $\sigma \in \mathrm{Aut}(C_p(B_n))$. Since σ preserves weight classes of the code, there exist incidence vectors $v^{\overline{[a,b]}}$ and $v^{\overline{[a',b']}}$ such that $\sigma(v^{\overline{[a,b]}}) = v^{\overline{[a',b']}}$. By definition, σ acts on coordinate positions of the code, the points of the design. Hence it maps points from the block $\overline{[a,b]}$ to points in a possibly different block $\overline{[a',b']}$, permuting the blocks. Hence $\sigma \in \mathrm{Aut}(\mathcal{D}_n)$. This completes the proof. □

If $n = 4$ then, by Whitney's theorem [64, Theorem 8], $\mathrm{Aut}(L^1(K_4)) \neq S_4$. In fact, $\mathrm{Aut}(L^1(K_4))$ is the wreath product $S_2 \wr S_3$. To see this, consider the complement of $L^1(K_4)$. It is not connected and its edges are $[12, 34]$, $[13, 24]$ and $[14, 23]$. That $\mathrm{Aut}(L^1(K_4)) = S_2 \wr S_3$ hence follows from the main result in Frucht [25]. Computations using Magma [7] for small values of p suggest that $\mathrm{Aut}(C_p(B_4)) \cong \mathrm{Aut}(L^1(K_4))$.

3.4 The binary codes $C_2(A_n)$ of the line graphs $L^2(K_n)$

In this section we consider binary codes spanned by the rows of A_n, an adjacency matrix of the line graph of the triangular graph. Parameters of the codes are obtained in Proposition 3.8. If $n \equiv 2, 3 \pmod 4$ then $C_2(A_n) = C_2(B_n)$, the binary code from an incidence matrix of the triangular graph considered in Section 3.3. Otherwise, $C_2(A_n)$ has co-dimension 1 in $C_2(B_n)$ and minimum weight equal to the degree of $L^2(K_n)$.

Proposition 3.8. *Let B_n be an incidence matrix of the triangular graph $L^1(K_n)$ and A_n an adjacency matrix of $L^2(K_n)$, the line graph of the triangular graph. Denote the respective binary codes by $C_2(B_n)$ and $C_2(A_n)$. If $n \equiv 0, 1 \pmod 4$ then $C_2(A_n) = \left[(n-2)\binom{n}{2}, \binom{n}{2} - 2, 4n - 10\right]_2$ and its minimum words are the rows of A_n. If $n \equiv 2, 3 \pmod 4$ then $C_2(B_n) = C_2(A_n)$.*

Proof. We first determine the dimension of $C_2(A_n)$. Since $B_n^T B_n = A_n$ over $\mathbb{F}_2$, $C_2(A_n)$ is a subcode of $C_2(B_n)$. By Corollary 2.26, $C_2(A_n) = E_2(B_n)$, the binary code obtained from the span of the differences of rows of B_n. By Corollary 2.29, $E_2(B_n)$ has co-dimension 1 in $C_2(B_n)$ if and only if $\jmath \in C_2(B_n^T)$ where $\jmath$ is the all-one vector of length $\binom{n}{2}$. Otherwise, $E_2(B_n) = C_2(B_n)$. We hence need to determine when $\jmath \in C_2(B_n^T)$.

By Theorem 2.16, triangular graphs are 0-covered if $\binom{n}{2}$ is even. This is satisfied if $n \equiv 0, 1 \pmod 4$. Hence for these values of n, the triangular graph has a perfect matching, say M. In the dual design with incidence matrix B_n^T, this implies that

$$\sum_{[[a,b],[b,c]] \in M} v^{\overline{[[a,b],[b,c]]}} = \jmath$$

where $v^{\overline{[[a,b],[b,c]]}}$ is the weight-2 incidence vector of the block $\overline{[[a,b],[b,c]]}$. Hence if $n \equiv 0,1 \pmod 4$ then $\jmath \in C_2(B_n^T)$. By Corollary 2.29, $\dim(C_2(A_n)) = \binom{n}{2} - 2$.

If $n \equiv 2,3 \pmod 4$ then $\binom{n}{2}$ is odd. Since $C_2(B_n^T)$ is an even weight code, $\jmath \notin C_2(B_n^T)$. By Proposition 2.28, we have $C_2(A_n) = E_2(B_n) = C_2(B_n)$ if $n \equiv 2,3 \pmod 4$.

Let us now consider the minimum weight of $C_2(A_n)$ if $n \equiv 0,1 \pmod 4$. Let $c \in C_2(A_n)$. Since $C_2(A_n) = E_2(B_n)$ by Lemma 2.26(a), we use Equation (3.3) to write

$$c = \sum_{[a,b]\in S} \left(v^{\overline{[a,b]}} + v^{\overline{[a_0,b_0]}} \right)$$

for some $S \subseteq V(L^1(K_n)) \setminus \{[a_0,b_0]\}$ and fixed vertex $[a_0,b_0]$. Simplifying, we obtain

$$c = \sum_{[a,b]\in S} v^{\overline{[a,b]}} + s v^{\overline{[a_0,b_0]}}$$

where $s = |S|$. Hence c is a sum of s or $s+1$ incidence vectors of $\mathcal{D}_n$ depending on whether s is even or odd. Without loss of generality, suppose s is odd. By Lemma 2.25(a),

$$\mathrm{Supp}(c) = \left(\cdots \left(\left(\overline{[a_0,b_0]} \triangle \overline{[a_1,b_1]} \right) \triangle \overline{[a_2,b_2]} \right) \cdots \triangle \overline{[a_s,b_s]} \right).$$

In the worst case, the pairwise intersection of the blocks is non-empty. Hence

$$\left| \bigcap_{i=0}^{s} \left\{ \overline{[a_i,b_i]} \right\} \right| \leq \binom{s+1}{2}.$$

Therefore

$$\begin{aligned} |\mathrm{Supp(c)}| &\geq 2(s+1)(n-2) - 2\binom{s+1}{2} \\ &\geq 4n - 10. \end{aligned}$$

Equality occurs if $s = 1$ and $|\{a,b\} \cap \{a_0,b_0\}| = 1$. Hence vectors of the form

$$v^{\overline{[a,b]}} + v^{\overline{[a,b_0]}} = v^{\overline{[[a,b],[a,b_0]]}},$$

the rows of A_n, are minimum words of the code. This completes the proof. $\square$

3.5 Non-binary codes from differences of rows of incidence matrices of triangular graphs

For any odd prime p and $n \geq 3$, we now determine parameters of non-binary codes $E_p(B_n)$ from the span of the differences of rows of B_n. It is easily checked that $E_p(B_3) = [3, 2, 2]_p$. The cases for $n \geq 4$ are considered in the proposition below.

Proposition 3.9. *Let $E_p(B_n)$ be the non-binary code spanned over $\mathbb{F}_p$ by differences of rows of B_n where p is an odd prime.*

(a) *If $n \geq 4$ then* $\dim(E_p(B_n)) = \binom{n}{2} - 1$.

(b) *$E_p(B_4)$ has minimum weight 4 and its minimum words include the scalar multiples of the vectors of the form $v^{[[a,b],[b,d]]} + v^{[[b,d],[c,d]]} - v^{[[a,d],[a,c]]} - v^{[[a,c],[b,c]]}$.*

(c) *If $n \geq 5$ then $E_p(B_n)$ has minimum weight $4n - 10$ and its minimum words are the scalar multiples of differences of pairs of rows of B_n indexed by adjacent vertices of $L^1(K_n)$.*

Proof. (a) Let $\jmath$ be the all-one vector of length $\binom{n}{2}$. From the proof of Proposition 3.8, if $n \equiv 0, 1 \pmod 4$ then $\jmath \in C_p(B_n^T)$. It remains to check if $\jmath \in C_p(B_n^T)$ when $n \equiv 2, 3 \pmod 4$.

Recall that the triangular graph $L^1(K_n)$ is vertex-transitive. Hence by Theorem 2.16, the graph is 1-covered if $|V(L^1(K_n))| = \binom{n}{2}$ is odd. In particular, the subgraph of $L^1(K_n)$ induced by $V(L^1(K_n)) \setminus \{[n-2, n]\}$ has a perfect matching. Further, the subgraph of $L^1(K_n)$ induced by $V(L^1(K_n)) \setminus T$, where

$$T = \{[n-2, n-1], [n-1, n], [n-2, n]\},$$

has a defect-3 matching M.

Let $v^{\overline{[[a,b],[b,c]]}}$ be an incidence vector of the block $\overline{[[a,b],[b,c]]}$ in the dual structure with incidence matrix B_n^T. $\overline{[[a,b],[b,c]]}$ contains the two vertices $[a, b]$ and $[b, c]$ incident with edge $[[a, b], [b, c]]$. Then the vector

$$\sum_{[[a_i,b_i],[b_i,c_i]] \in M} v^{\overline{[[a_i,b_i],[b_i,c_i]]}} = \jmath'$$

has entries 0 in the three coordinate positions indexed by elements of T. The remaining $\binom{n}{2} - 3$ entries are 1. Also, the vector

$$v^{\overline{[[n-1,n],[n-2,n]]}} + v^{\overline{[[n-1,n],[n-2,n-1]]}} + v^{\overline{[[n-2,n],[n-2,n-1]]}} = \overline{\jmath}$$

has coordinate entries 2 in the three coordinate positions indexed by elements of T and 0 in the $\binom{n}{2} - 3$ coordinate positions where entries of $\jmath'$ are 1. Since $\jmath'$ and $\overline{\jmath}$ are not commonly incident, we have

$$2\jmath' + \overline{\jmath} = 2\jmath.$$

Hence $\jmath \in C_p(B_n^T)$ for all n. By Corollary 2.29, $E_p(B_n)$ has co-dimension 1 in $C_p(B_n)$. This concludes our proof on the dimension of $E_p(B_n)$ if $n \geq 4$.

(b) Since $E_p(B_4)$ is a subcode of $C_p(B_4) = [12, 6, 4]_p$, its minimum weight does not exceed 4. In fact, $E_p(B_4)$ also has minimum weight 4 because, like its supercode $C_p(B_4)$, it contains the weight-4 codewords in Equation (3.6). Notice that Equation (3.5) can also be expressed as a sum of the differences of rows of B_4. By definition, these are codewords of $E_p(B_4)$.

(c) We now need to prove the assertion about the minimum weight and minimum words of $E_p(B_n)$ if $n \geq 5$. To do this, we use the fact that $E_p(B_n) \subseteq C_p(B_n)$ and show that $C_p(B_n)$ does not contain a codeword c such that $2n - 3 \leq \text{wt}(c) \leq 4n - 11$ but it has codewords of weight $4n - 10$ which are also in $E_p(B_n)$.

Let $c \in C_p(B_n)$ be a non-zero linear combination of $r \geq 2$ rows of B_n. Then

$$c = \sum_{[a,b] \in R} \alpha_{ab} v^{\overline{[a,b]}} \tag{3.9}$$

for some $R \subseteq V(L^1(K_n))$ and $\alpha_{ab} \in \mathbb{F}_p^*$. Let $c([[a, b], [b, d]])$ be the coordinate entry of c in the position indexed by edge $[[a, b], [b, d]]$. If $\alpha_{ab} v^{\overline{[a,b]}}$ and $\alpha_{bd} v^{\overline{[b,d]}}$ are both non-zero in Equation (3.9) then

$$c([[a, b], [b, d]]) = \alpha_{ab} + \alpha_{bd}.$$

If $\alpha_{ab} v^{\overline{[a,b]}}$ is non-zero and $\alpha_{bd} v^{\overline{[b,d]}} = \mathbf{0}$ then

$$c([[a, b], [b, d]]) = \alpha_{ab} \in \text{Supp}(c). \tag{3.10}$$

Now, $\mathrm{wt}(c) \geq 2r(n-2) - 2t$ where t, $0 \leq t \leq (n-2)\binom{n}{2}$, is the number of coordinate positions such that the r rows intersect. In these positions, it is possible to have $\alpha_{ab} + \alpha_{bd} = 0$. Let us first consider the possibilities for t.

If $r = \binom{n}{2}$ then $t = (n-2)\binom{n}{2}$. Hence $\mathrm{wt}(c) \geq 0$. We however know from Proposition 3.3 that $\mathrm{wt}(c) \geq 2(n-2)$. If $r = \binom{n}{2} - 1$ then there is an incidence vector $v^{\overline{[a,b]}}$ that is not in the linear combination in Equation (3.9). Hence $\overline{[a,b]} \subseteq \mathrm{Supp}(c)$ and $\mathrm{wt}(c) \geq |\overline{[a,b]}| = 2(n-2)$. If $r = \binom{n}{2} - 2$ then, similarly, $\mathrm{Supp}(c)$ has at least $4n - 10$ non-zero entries. Proceeding in this manner, notice that if $3 \leq r \leq \binom{n}{2} - 3$ then $\mathrm{Supp}(c)$ has more than $4n - 10$ elements. To show that $\mathrm{wt}(c) \geq 4n - 10$ if $r \geq 2$ then we need to show that $\mathrm{wt}(c) \not< 4n - 10$ if $r = \binom{n}{2} - 1$ or if $r = \binom{n}{2}$. We adapt a method used by Key, Moori and Rodrigues in [42].

Suppose $r = \binom{n}{2} - 1$, i.e., $R = \Omega^{\{2\}} \setminus \{[a,b]\}$ for some reference vertex $[a,b]$. Then

$$c([[a,b],[b,x]]) = \alpha_{bx} \neq 0.$$

Also,

$$c([[a,b],[a,x]]) = \alpha_{ax} \neq 0.$$

Hence

$$\{[[a,b],[b,x]],[[a,b],[a,x]] : x \neq a,b\} = \overline{[a,b]} \subseteq \mathrm{Supp}(c).$$

Since $\mathrm{wt}(c) > 2(n-2)$ by assumption, $\mathrm{Supp}(c) \neq \overline{[a,b]}$.

For any three distinct vertices $[a',y]$, $[b',y]$ and $[c',y]$ such that $y \neq a,b$, it is not possible to have

$$\alpha_{a'y} + \alpha_{b'y} = \alpha_{a'y} + \alpha_{c'y} = \alpha_{b'y} + \alpha_{c'y} = 0.$$

At least one of the points $[[a',y],[y,b']]$, $[[a',y],[y,c']]$ and $[[b',y],[y,c']]$ is therefore in $\mathrm{Supp}(c)$. We count the number of possibilities of choosing one of these points exactly once. For every choice of $y \in \Omega$ such that $y \neq a,b$, the three distinct elements a', b' and c' determine the coordinate positions $[[a',y],[y,b']]$, $[[a',y],[y,c']]$ and $[[b',y],[y,c']]$. There are $\binom{n-1}{3}$ possibilities for a', b' and c'. Any two of these elements, say a' and b', are together on the $n-3$ triples a', b', x where $x \neq a', b', y$. Hence there are at least $\frac{n-2}{n-3}\binom{n-1}{3}$

coordinate positions in Supp(c) chosen this way. And so

$$\mathrm{wt}(c) \geq 2(n-2) + \frac{n-2}{n-3}\binom{n-1}{3} \geq 4n-10 \text{ if } n \geq 4.$$

Similarly, if $r = \binom{n}{2}$ then

$$\mathrm{wt}(c) \geq \frac{n}{n-3}\binom{n-1}{3} = \frac{n(n-1)(n-2)}{6} \geq 4n-10 \text{ for } n \geq 5.$$

It is easily seen that scalar multiples of codewords of the form $v^{\overline{[a,b]}} - v^{\overline{[c,d]}}$ have minimum weight if $[a,b]$ and $[c,d]$ are adjacent, i.e., if the corresponding rows of B_n intersect. This completes the proof. □

3.6 Permutation decoding

In this section, we consider permutation decoding of the codes discussed above. An information set for the binary codes is given in Lemma 3.10 and PD-sets exhibited in Proposition 3.11. A similar treatment is given to the non-binary codes in Lemma 3.12 and Proposition 3.13, respectively.

3.6.1 PD-sets for the binary code $C_2(B_n)$

Lemma 3.10. *For $n \geq 5$, let $C_2(B_n)$ be the binary code from the row span of B_n, an incidence matrix of the triangular graph $L^1(K_n)$. Then*

$$\mathcal{I}_n = \{[[1,2],[1,x]], [[1,y],[y,z]] : 3 \leq x \leq n, 2 \leq y < z \leq n\} \tag{3.11}$$

is an information set for the code.

Proof. Consider the submatrix B_n^* formed by all rows of B_n excluding the one indexed by the vertex $[1,2]$. Re-order columns of B_n^* so that they start with those indexed by the points

$[[1,2],[1,3]], [[1,2],[2,3]], [[1,2],[1,4]], [[1,2],[2,4]], [[1,3],[3,4]], [[1,2],[1,5]],$
$[[1,2],[2,5]], [[1,3],[3,5]], [[1,4],[4,5]], \cdots, [[1,2],[1,n]], [[1,2],[2,n]],$
$[[1,3],[3,n]], \cdots, [[1,(n-1)],[(n-1),n]],$

in that order. These are followed by columns indexed by the remaining $(n-3)\binom{n}{2}+1$ check points in any order. Looked at as edges of $L^1(K_n)$, the endpoints $[b,c]$ in each coordinate position $[[a,b],[b,c]]$ are ordered as the rows $v^{\overline{[b,c]}}$ of B_n^*. Hence we get a square $\left(\binom{n}{2}-1\right)\times\left(\binom{n}{2}-1\right)$ upper triangular submatrix in the first $\binom{n}{2}-1$ columns of B_n^*. All entries on the main diagonal are equal to 1. Hence columns indexed by points in $\mathcal{I}_n$ are linearly independent and $\mathcal{I}_n$ is an information set. □

Notice that the only rows that have non-zero entries off the main diagonal in the first $\binom{n}{2}-1$ columns are those indexed by vertices of the form $\overline{[1,x]}$ where $3\leq x\leq n-1$. There are $n-x$ such entries in each row. Replacing every row of this form with the row

$$v^{\overline{[1,x]}}+\sum_{1\leq i\leq n}v^{\overline{[x,x+i]}},$$

one obtains a generator matrix in standard form.

Proposition 3.11. *For $n\geq 5$, let $C_2(B_n)$ be the binary code from the row span of B_n, an incidence matrix of the triangular graph. Let $\mathcal{I}_n$ be the information set of $C_2(B_n)$ obtained in* Lemma 3.10. *Then the set*

$$S=\{(1),(1,\check{z}),(1,\check{z},\check{x}):\check{x},\check{z}\neq 1,2\} \tag{3.12}$$

of $1+\binom{n-1}{2}$ elements of S_n is a PD-set for the binary code $C_2(B_n)$ with information set $\mathcal{I}_n$.

Proof. Let

$$\begin{aligned}\mathcal{C}_1&=\{[[1,\tilde{x}],[1,\tilde{y}]]:3\leq\tilde{x}<\tilde{y}\leq n\}\,,\\ \mathcal{C}_2&=\{[[1,\hat{y}],[\hat{y},\hat{z}]]:2\leq\hat{z}<\hat{y}\leq n\}\,,\\ \mathcal{C}_3&=\{[[\bar{x},\bar{y}],[\bar{y},\bar{z}]]:\bar{x},\bar{y},\bar{z}\neq 1\}\,.\end{aligned}$$

In view of Lemma 3.10, the check set for the code is the set $\mathcal{C}=\mathcal{C}_1\cup\mathcal{C}_2\cup\mathcal{C}_3$. Recall that the code corrects up to $n-3$ errors in a received word. Suppose a codeword c is sent and a vector $y=c+e$ is received such that wt(e) $\leq$ n -3, i.e., at most $n-3$ errors occur. Let $\mathcal{E}$ denote the set of error positions of y, i.e., the coordinate positions where coordinate entries of e are non-zero. We show that every possible error pattern in $\mathcal{E}$ is mapped by some element of S into $\mathcal{C}$. The possible cases are as follows.

1. If $\mathcal{E} \subset \mathcal{C}$ then the identity element (1) of S_n can be used to keep the errors in the check set $\mathcal{C}$.

2. Suppose $\mathcal{E} \subset \mathcal{I}_n$. We examine three possible cases.

   (a) $\mathcal{E} \subset \{[[1,2],[1,x]] : x \geq 3\}$. Any transposition of the form $(1,\check{z})$, where $\check{z} \neq 1,2$, will do.

   (b) $\mathcal{E} \subset \{[[1,y],[y,z]] : 2 \leq y < z \leq n\}$. Since we assume that $|\mathcal{E}| \leq n-3$ and there are $n-2$ possible values that z can take, there is at least one value $\check{z} \in \Omega \setminus \{1,2\}$ that z does not take. $(1,\check{z})$ will do.

   (c) $\mathcal{E} \subset \{[[1,2],[1,x]] : x \geq 3\} \cup \{[[1,y],[y,z]], 2 \leq y < z \leq n\}$. If there is at least one error in each of positions of the form $[[1,2],[1,x]]$ and $[[1,y],[y,z]]$, then

   $$|\{[[1,y],[y,z]] : 2 \leq y < z \leq n\}| \leq n-4.$$

   Hence there is an element $\check{z} \in \Omega \setminus \{1,2\}$ such that $z \neq \check{z}$. $(1,\check{z})$ will do.

3. $\mathcal{E} \subset \mathcal{I}_n \cup \mathcal{C}$. Transpositions of the form $(1,\check{z})$ (where $\check{z}$ is the element mentioned in 2(b) and 2(c)) map all errors from $\mathcal{I}_n$ into $\mathcal{C}$. Since some error positions are already in $\mathcal{C}$, there is a possibility that $(1,\check{z})$ maps these into $\mathcal{I}_n$. We show that in all such cases, automorphisms of the form $(1,\check{z},\check{x})$ can be used where $\check{x} \in \Omega \setminus \{1,2,\check{z}\}$. We have the following possibilities:

   (a) $\mathcal{E} \subset \mathcal{I}_n \cup \{[[1,\tilde{x}],[1,\tilde{y}]] : 3 \leq \tilde{x} < \tilde{y} \leq n\}$. It is possible to have error positions in $\mathcal{C}$ such that $\check{z} = \tilde{x}$. The transpositions $(1,\check{z})$ map such positions to positions of the form $[[1,\check{z}],[\check{z},\tilde{y}]] \in \mathcal{I}_n$ (since $\tilde{x} < \tilde{y}$ by assumption). Use automorphisms of the form $(1,\check{z},\check{x})$, where $\check{x} \neq 1,2,\check{z}$ to map $\mathcal{E}$ into $\mathcal{C}$ and fix in $\mathcal{C}$ errors already in $\mathcal{C}$. Error positions of the form $[[1,\tilde{x}],[1,\tilde{y}]]$ are then mapped to $[[\check{z},\check{x}],[\check{z},\tilde{y}]]$ an element of $\mathcal{C}$.

   (b) $\mathcal{E} \subset \mathcal{I}_n \cup \{[[1,\hat{y}],[\hat{y},\hat{z}]] : 2 \leq \hat{z} < \hat{y} \leq n\}$. The transposition $(1,\check{z})$ will do unless there is an error position in $\mathcal{C}$ such that $\hat{z} = 2$ and

$\check{z} = \hat{y}$. In this case, use $(1, \check{z}, \check{x})$, $\check{z}, \check{x} \in \Omega \setminus \{1, 2\}$. In particular, the point $[[1, \check{z}], [2, \check{z}]]$ is mapped to $[[\check{z}, \check{x}], [2, \check{x}]]$.

(c) $\mathcal{E} \subset \mathcal{I}_n \cup \{[[\bar{x}, \bar{y}], [\bar{y}, \bar{z}]] : \bar{x}, \bar{y}, \bar{z} \neq 1, \bar{x} < \bar{z}\}$. It is possible to have error positions in $\mathcal{C}$ such that:

(i) $\check{z} = \bar{x}$ and $\bar{y} < \bar{z}$.

(ii) $\check{z} = \bar{y}$ and $\bar{x} = 2$.

(iii) $\check{z} = \bar{z}$ and $\bar{y} < \bar{x}$.

The transpositions $(1, \check{z})$ map such errors into $\mathcal{I}_n$. Use automorphisms of the form $(1, \check{z}, \check{x})$ where $\check{z}, \check{x} \in \Omega \setminus \{1, 2\}$.

(d) $\mathcal{E} \subset \mathcal{I}_n \cup \{[[1, \tilde{x}], [1, \tilde{y}]], [[1, \hat{y}], [\hat{y}, \hat{z}]] : 3 \leq \tilde{x} < \tilde{y} \leq n, 2 \leq \hat{z} < \hat{y} \leq n\}$. Use transpositions of the form $(1, \check{z})$ except if we have the cases listed in 3(a) and 3(b) occurring or if $\check{z} = \tilde{x} = \hat{y}$ and $\hat{z} = 2$. $(1, \check{z}, \check{x})$, $\check{z}, \check{x} \in \Omega \setminus \{1, 2\}$ will do where $\check{z}, \check{x} \in \Omega \setminus \{1, 2\}$.

(e) $\mathcal{E} \subset \mathcal{I}_n \cup \{[[\bar{x}, \bar{y}], [\bar{y}, \bar{z}]], [[1, \tilde{x}], [1, \tilde{y}]] : \bar{x}, \bar{y}, \bar{z} \neq 1, \bar{x} < \bar{z}, 3 \leq \tilde{x} < \tilde{y} \leq n\}$. In addition to cases listed in 3(a) and 3(c) above, the transpositions $(1, \check{z})$ map errors in $\mathcal{C}$ into $\mathcal{I}_n$ if

(i) $\check{z} = \bar{x} = \tilde{x}$, $\bar{y} < \bar{z}$.

(ii) $\check{z} = \bar{y} = \tilde{x}$, $\bar{x} = 2$.

(iii) $\check{z} = \bar{z} = \tilde{x}$, $\bar{y} < \bar{x}$.

Use automorphisms of the form $(1, \check{z}, \check{x})$, $\check{z}, \check{x} \in \Omega \setminus \{1, 2\}$.

(f) $\mathcal{E} \subset \mathcal{I}_n \cup \{[[\bar{x}, \bar{y}], [\bar{y}, \bar{z}]], [[1, \hat{y}], [\hat{y}, \hat{z}]] : \bar{x}, \bar{y}, \bar{z} \neq 1, \bar{x} < \bar{z}, 2 \leq \hat{z} < \hat{y} \leq n\}$. In addition to cases listed in 3(a) and 3(b), $(1, \check{z})$ maps errors from $\mathcal{C}$ into $\mathcal{I}_n$ if one of the cases below occur.

(i) $\check{z} = \bar{y} = \hat{y}$, $\hat{z} = \bar{x} = 2$.

(ii) $\check{z} = \bar{x} = \hat{y}$, $\bar{y} < \bar{z}$, $\hat{z} = 2$.

(iii) $\check{z} = \bar{z} = \hat{y}$, $\bar{y} < \bar{x}$, $\hat{z} = 2$.

Use automorphisms of the form $(1, \check{z}, \check{x})$, $\check{z}, \check{x} \in \Omega \setminus \{1, 2\}$.

(g) $\mathcal{E} \subset \mathcal{I}_n \cup \{[[1, \tilde{x}], [1, \tilde{y}]], [[1, \hat{y}], [\hat{y}, \hat{z}]], [[\bar{x}, \bar{y}], [\bar{y}, \bar{z}]] : 3 \leq \tilde{x} < \tilde{y} \leq n, 2 \leq \hat{z} < \hat{y} \leq n, \bar{x}, \bar{y}, \bar{z} \neq 1\}$. In addition to the cases mentioned above, transpositions of the form $(1, \check{z})$ map errors from $\mathcal{C}$ into $\mathcal{I}_n$ if one of the following cases occur:

(i) $\check{z} = \tilde{x} = \hat{y} = \bar{x}$, $\bar{y} < \bar{z}$ and $\hat{z} = 2$.

(ii) $\check{z} = \tilde{x} = \hat{y} = \bar{y}$ and $\bar{x} = \hat{z} = 2$.

(iii) $\check{z} = \tilde{x} = \hat{y} = \bar{z}$, $\hat{z} = 2$ and $\bar{y} < \bar{x}$.

Automorphisms of the form $(1, \check{z}, \breve{x})$ will do where $\check{z}, \breve{x} \in \Omega \backslash \{1, 2\}$.

□

3.6.2 PD-sets for the non-binary code $C_p(B_n)$

In this section we consider PD-sets for the non-binary code $C_p(B_n)$ from the row span of B_n where p is any odd prime and $n \geq 5$. The PD-set given here has four elements less than that of the binary codes. As was done for the binary codes, we first give an information set for the codes.

Lemma 3.12. *Let $\mathcal{I}_n$ be as in* Equation (3.11). *Then $\mathcal{I}_n \cup \{[[1,3],[1,4]]\}$ is an information set for the non-binary codes $C_p(B_n)$ from the row span of B_n, an incidence matrix of the triangular graph, where p is any odd prime and $n \geq 5$.*

Proof. We need to show that columns of B_n indexed by points in $\mathcal{I}_n \cup \{[[1,3],[1,4]]\}$ are linearly independent over $\mathbb{F}_p$. First, order these columns so that they begin with those indexed by the points below in the given order.

$$
\begin{aligned}
&[[1,2],[1,3]], [[1,2],[2,3]], [[1,2],[1,4]], [[1,2],[2,4]], [[1,3],[3,4]], [[1,2],[1,5]],\\
&[[1,2],[2,5]], [[1,3],[3,5]], [[1,4],[4,5]], \cdots, [[1,2],[1,n]], [[1,2],[2,n]],\\
&[[1,3],[3,n]], \cdots, [[1,(n-1)],[(n-1),n]], [[1,3],[1,4]].
\end{aligned} \tag{3.13}
$$

Order the rows of B_n from $v^{\overline{[1,3]}}$ to $v^{\overline{[n-1,n]}}$ as before and make $v^{\overline{[1,2]}}$ the last row. Since the ordering of rows from $v^{\overline{[1,3]}}$ to $v^{\overline{[n-1,n]}}$ corresponds to the ordering of the vertices $[b,c]$ in the points $[[a,b],[b,c]]$ in (3.13) above, the submatrix of B_n in the first $\binom{n}{2} - 1$ rows and columns is right triangular. $v^{\overline{[1,2]}}$ has non-zero entries at positions of the form $[[1,2],[1,x]]$ and $[[1,2],[2,x]]$ where $3 \leq x \leq n$. Let

$$u = \sum_{3 \leq x \leq n} \left(v^{\overline{[1,x]}} + v^{\overline{[2,x]}} \right)$$

and let

$$w = v^{\overline{[1,2]}} + \sum_{\substack{2 \leq x \leq n-1 \\ 1 \leq i \leq n-x}} v^{\overline{[x,x+i]}}.$$

In the first $\binom{n}{2}$ coordinate positions,

$$u = (1, 1, \cdots, 1, 2)$$

and

$$w = (1, 1, \cdots 1, 0).$$

Hence $u - w = (0, \cdots, 0, 2)$ in these positions. We can therefore replace $v^{\overline{[1,2]}}$ with $u - w$ to obtain a right triangular matrix in the first $\binom{n}{2}$ columns. □

For the PD-sets of $C_p(B_n)$, in addition to cases studied in Proposition 3.11, we choose automorphisms such that errors are not mapped to the point $[[1,3],[1,4]]$.

Proposition 3.13. *Let $C_p(B_n)$ be an the non-binary code from the row span of incidence matrices B_n of triangular graphs where p is an odd prime and $n \geq 5$. Let S be as in* Equation (3.12)*. The set*

$$S \setminus \{(1,3), (1,4), (1,3,4), (1,4,3)\}$$

of elements of S_n is a PD-set for $C_p(B_n)$ where p is an odd prime.

Proof. We use the following notation: $\mathcal{E}$ refers to a set of at most $n-3$ error positions, $\overline{\mathcal{I}}_n$ is the information set $\mathcal{I}_n \cup \{[[1,3],[1,4]]\}$ and $\overline{\mathcal{C}}$ is the check set $\mathcal{C} \setminus \{[[1,3],[1,4]]\}$. The possible cases are as follows:

1. $\mathcal{E} \subset \overline{\mathcal{I}}_n$.

   (a) $\mathcal{E} \subset \{[[1,2],[1,x]], [[1,3],[1,4]] : x \geq 3\}$. Any transposition of the form $(1, \check{z})$ where $\check{z} \in \Omega \setminus \{1,2,3\}$, will do.

   (b) $\mathcal{E} \subset \{[[1,y],[y,z]], [[1,3],[1,4]] : 2 \leq y < z \leq n\}$. If $[[1,3],[1,4]] \in \mathcal{E}$ then z can take up to $n-4$ values. Hence there are at least two elements $\check{z}_1, \check{z}_2 \in \Omega \setminus \{1,2\}$ such that $z \neq \check{z}_i$. Since both are not 3, any transposition of the form $(1,x)$, where x is one of these values and $x \neq 3$, will do. If $[[1,3],[1,4]] \notin \mathcal{E}$ then, from the proof of Proposition 3.11, there is an element $\check{z} \in \Omega \setminus \{1,2\}$ such that $z \neq \check{z}$. Since it is possible to have $[[1,3],[3,4]]$ in $\mathcal{E}$, the transpositions $(1,\check{z})$ cannot be used if $\check{z} = 3$ or if $\check{z} = 4$. Use automorphisms of the form $(1,\check{z},\check{x})$ where $\check{x} \neq 3$ if $\check{z} = 4$.

(c) $\mathcal{E} \subset \{[[1,2],[1,x]], [[1,y],[y,z]], [[1,3],[1,4]] : x \geq 3, 2 \leq y < z \leq n\}$. If there is an error in at least each of the positions of the form $[[1,2],[1,x]]$, $[[1,y],[y,z]]$ and $[[1,3],[1,4]]$, then

$$|\{[[1,y],[y,z]] : 2 \leq y < z \leq n\}| \leq n-5.$$

Hence there are at least three values $\check{z}_1$, $\check{z}_2$ and $\check{z}_3$ in $\Omega \setminus \{1,2\}$ such that $z \neq \check{z}_i$. Use a transposition of the form $(1,x)$ where $x = \check{z}_i$ and $x \neq 3$.

2. $\mathcal{E} \subset \overline{\mathcal{I}}_n \cup \overline{\mathcal{C}}$. Since elements of S_n are bijections and we are interested in identifying cases where errors are mapped to $[[1,3],[1,4]]$, it is sufficient to consider the cases $\mathcal{E} \subset \overline{\mathcal{I}}_n \cup \{[[1,\tilde{x}],[1,\tilde{y}]] : 3 \leq \tilde{x} < \tilde{y} \leq n, \tilde{y} \neq 4\}$, $\mathcal{E} \subset \overline{\mathcal{I}}_n \cup \{[[1,\hat{y}],[\hat{y},\hat{z}]] : 2 \leq \hat{z} < \hat{y} \leq n\}$ and $\mathcal{E} \subset \overline{\mathcal{I}}_n \cup \{[[\bar{x},\bar{y}],[\bar{y},\bar{z}]] : \bar{x},\bar{y},\bar{z} \neq 1\}$.

(a) $\mathcal{E} \subset \overline{\mathcal{I}}_n \cup \{[[1,\tilde{x}],[1,\tilde{y}]] : 3 \leq \tilde{x} < \tilde{y} \leq n, \tilde{y} \neq 4\}$. There is no transposition of the form $(1,\check{z})$ that maps a point of the form $[[1,\tilde{x}],[1,\tilde{y}]]$, $\tilde{y} \neq 4$ to $[[1,3],[1,4]]$. Hence this case can hence be handled as the cases in 1. above.

(b) $\mathcal{E} \subset \overline{\mathcal{I}}_n \cup \{[[1,\hat{y}],[\hat{y},\hat{z}]] : 2 \leq \hat{z} < \hat{y} \leq n\}$. It is possible in this case to have $[[1,4],[4,3]] \in \mathcal{E}$ and $\check{z} = 4$. Use an automorphism of the form $(1,\check{z},\check{x})$ where $\check{x} \neq 3$ if $\check{z} = 4$ and $\check{x} \neq 4$ if $\check{z} = 3$.

(c) $\mathcal{E} \subset \overline{\mathcal{I}}_n \cup \{[[\bar{x},\bar{y}],[\bar{y},\bar{z}]] : \bar{x},\bar{y},\bar{z} \neq 1, \bar{x} < \bar{z}\}$. It is possible to have a point of the form $[[3,\bar{y}],[\bar{y},4]] \in \mathcal{E}$ and $\check{z} = \bar{y}$. Use an automorphism of the form $(1,\check{z},\check{x})$.

□

Note. Using Magma [7], the Gordon bound on the size of a PD-set S for the codes $C_p(B_n)$, p any prime, appears to be $|S| \geq n-2$ for any prime p. In our case, $|S| = \binom{n-1}{2} + 1$ if $p = 2$ and $|S| = \binom{n-1}{2} - 3$ if p is any odd prime.

Chapter 4

Embeddings of strong products of triangular graphs and K_2 and their codes

4.1 Introduction

In this chapter we introduce a class of vertex-transitive graphs Γ_n that are embeddable into the strong product $L^1(K_n)\boxtimes K_2$ of triangular graphs $L^1(K_n)$ and K_2. Pertinent properties of the graphs are determined. In addition to neighbourhood and incidence designs that naturally come with regular graphs, we show that Γ_n has 6-*cycle designs*; these are 1-designs in which points are vertices of the graph and every block contains vertices of a 6-cycle in the graph.

For any prime p, we consider p-ary linear codes obtained from the row span of incidence matrices of Γ_n. We determine main parameters of the codes and their permutation automorphism groups. Unlike most binary codes obtained from incidence and neighbourhood designs of regular graphs in this thesis and in the literature in general, we show that binary codes from incidence matrices of Γ_n have other minimum words apart from rows of the matrices. Using specific information sets, we have exhibited PD-sets for full permutation decoding of the codes.

Further, we consider complete porcupines (see Definition 4.11). These graphs are induced subgraphs of Γ_n. Codes from incidence matrices of complete porcupines are therefore considered first.

Part of the work in this chapter is the content of [24]. The graph Γ_n that has been alluded to is defined as follows.

Definition 4.1. For $n \geq 3$, let $\Omega = \{1, \cdots, n\}$. Let $\Omega^{\{k\}}$ be the set of subsets of Ω of size k. Consider the cartesian product $X = \Omega^{\{2\}} \times \Omega^{\{1\}}$. Define a graph Γ_n by

$$V(\Gamma_n) = \{(A, B) \in X : A \supset B\};$$
$$[(A, B), (A', B')] \in E(\Gamma_n) \Longleftrightarrow A = A' \text{ or } B = B'.$$

Our main results are summarised in Theorem 4.2.

Theorem 4.2. *For any prime p and $n \geq 4$, let $C_p(G_n)$ be the p-ary code obtained from the row span over $\mathbb{F}_p$ of G_n, an incidence matrix of Γ_n, the graph of* Definition 4.1*. Let $A_1 = \{[(\{a, n\}, \{a\}), (\{a, x\}, \{a\})] | x \neq a, n\}$, $A_2 = \{[(\{b, n\}, \{n\}), (\{b, n\}, \{b\})] | b \neq n\}$ and $A_3 = \{[(\{n-1, n\}, \{n\}), (\{c, n\}, \{n\})] | c \neq n-1, n\}$.*

(a) *If p is odd then $C_p(G_n) = \big[(n-1)\binom{n}{2}, 2\binom{n}{2}, n-1\big]_p$ and its minimum words are the scalar multiples of the rows of G_n.*

(b) *$C_2(G_n) = \big[(n-1)\binom{n}{2}, 2\binom{n}{2} - 1, n-1\big]_2$ and its minimum words are the rows of G_n and the n vectors $\sum_x v^{\overline{(\{a,x\},\{a\})}}$ where $x \neq a$.*

(c) $\mathrm{Aut}(C_p(G_n)) \cong \mathrm{Aut}(\Gamma_n) \cong S_n$.

(d) *$\mathcal{I}_n = \bigcup_{i=1}^{3} A_i$ is an information set for the binary code $C_2(G_n)$. If p is odd then*

$$\mathcal{I}_n \cup \{[(\{n-3, n\}, \{n\}), (\{n-2, n\}, \{n\})]\}$$

is an information set for $C_p(G_n)$.

(e) *If $p = 2$ then*

$$S = \{(1), (n-1, y)(x, n) | 1 \leq x, y \leq n-1, x \neq y\}$$

consisting of $n + (n-2)^2$ elements of S_n is a PD-set for $C_2(G_n)$ with $\mathcal{I}_n$ as information set. If p is odd then

$$S \cup \{(n-2, y)(n, x) : x, y \in \Omega \setminus \{n\}, y \leq n-4\}$$

is a PD-set with

$$\mathcal{I}_n \cup \{[(\{n-3, n\}, \{n\}), (\{n-2, n\}, \{n\})]\}$$

as information set.

The proof of Theorem 4.2 follows from a series of lemmas and propositions presented in the various section below.

The rest of the chapter is organized as follows. In Section 4.2, we show that Γ_n is an embedding of the strong product $L^1(K_n) \boxtimes K_2$ of triangular graphs and K_2. We also consider properties of the graphs including automorphism groups. 6-cycle designs of the graphs are considered in Section 4.2.2. In Section 4.2.3, we describe how incidence matrices of Γ_n will be written. Codes from incidence matrices of complete porcupines are discussed in Section 4.3. Codes from incidence matrices of Γ_n are examined in Section 4.4. Permutation automorphism groups of these codes are determined in Section 4.5. We also determine PD-sets for full permutation decoding of the codes.

4.2 The embeddings Γ_n of $L^1(K_n) \boxtimes K_2$

For $n \geq 3$, let Γ_n be as in Definition 4.1. The graph has $2\binom{n}{2}$ vertices. The neighbourhood of each vertex $(\{a, b\}, \{a\})$ is the set

$$N((\{a, b\}, \{a\})) = \{(\{a, b\}, \{b\})\} \cup \{(\{a, x\}, \{a\}) : x \neq a\}.$$

Hence Γ_n is $(n-1)$-regular and it has $(n-1)\binom{n}{2}$ edges. Γ_3 is the 6-cycle. We have illustrated Γ_4 in Figure 4.1.

Identifying the vertex-set of the triangular graph with $\Omega^{\{2\}}$ and that of K_2 with $\{0, 1\}$, we give the following characterisation of Γ_n.

Proposition 4.3. *Γ_n is an embedding of the strong product $L^1(K_n) \boxtimes K_2$ of triangular graphs and K_2.*

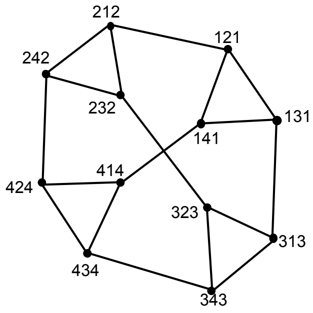

Figure 4.1: Γ_4 (iji denotes the vertex $(\{i,j\},\{i\})$)

Proof. Define a map $\phi : V(\Gamma_n) \to V\left(L^1(K_n) \boxtimes K_2\right)$ by

$$\phi\left((\{a,b\},\{a\})\right) = \begin{cases} ([a,b],0), & \text{if } a<b \\ ([a,b],1), & \text{otherwise} \end{cases}.$$

We first show that ϕ is a homomorphism. Let $u = (\{a,b\},\{a\})$ be an arbitrary vertex of Γ_n. Then u is adjacent to $v = (\{a,b\},\{b\})$ and to $n-2$ vertices of the form $w = (\{a,x\},\{a\})$ where $x \neq a,b$.

Suppose $a < b$. Then $[\phi(u),\phi(v)] = [([a,b],0),([a,b],1)]$, an edge in the graph product $L^1(K_n) \boxtimes K_2$.

Let us now consider the edges $[\phi(u),\phi(w)]$. There are two possibilities. If $a < x$ then $[\phi(u),\phi(w)] = [([a,b],0),([a,x],0)]$. If $a > x$ then $[\phi(u),\phi(w)] = [([a,b],0),([a,x],1)]$. In either case, we have $[\phi(u),\phi(w)] \in E(L^1(K_n) \boxtimes K_2)$. A similar result is obtained if $a > b$. Hence ϕ is a homomorphism.

That ϕ is injective follows from the definition of the map. Hence ϕ is an embedding of $L^1(K_n) \boxtimes K_2$. □

4.2.1 Automorphisms of Γ_n

We now consider automorphisms of Γ_n. Let $\alpha \in S_n$. Define a map $\sigma_\alpha : V(\Gamma_n) \to V(\Gamma_n)$ by

$$\sigma_\alpha((\{a,b\},\{a\})) = (\{\alpha(a),\alpha(b)\},\{\alpha(a)\}).$$

Claim 4.4. $\sigma_\alpha \in \mathrm{Aut}(\Gamma_n)$.

Proof. Since σ_α is clearly one-to-one and hence onto, it remains to show that it preserves adjacency in the graph. There are two cases to consider. Any vertex $u = (\{a, b\}, \{a\})$ is adjacent to $v = (\{a, b\}, \{b\})$ and to $n - 2$ vertices of the form $w = (\{a, x\}, \{a\})$ where $x \neq a, b$. We see that $\sigma_\alpha(u)$ is adjacent to $\sigma_\alpha(v)$ and to $\sigma_\alpha(w)$. Hence $\sigma_\alpha \in \mathrm{Aut}(\Gamma_n)$. □

Remark 4.5. The graphs Γ_n are vertex-transitive. To see this, consider any two distinct vertices $(\{a, b\}, \{a\})$ and $(\{a', b'\}, \{a'\})$ of Γ_n. There exists a permutation $\alpha \in S_n$ such that $\alpha(a) = a'$ and $\alpha(b) = b'$. Hence α induces an automorphism $\sigma_\alpha \in \mathrm{Aut}(\Gamma_n)$ such that $\sigma_\alpha((\{a, b\}, \{a\})) = (\{a', b'\}, \{a'\})$.

Let
$$X_a = \{(\{a, x\}, \{a\}) : x \neq a\}.$$
There are n sets of this form and they partition $V(\Gamma_n)$. Let
$$P = \{X_a : a \in \Omega\}.$$
The quotient graph Γ_n/P has vertex set P and two vertices X_a and X_b are adjacent if there exists $u \in X_a$ and $v \in X_b$ such that $[u, v]$ is an edge of Γ_n. It is readily seen that Γ_n/P is isomorphic to the complete graph K_n.

Lemma 4.6. *X_a is a maximum clique.*

Proof. That X_a is a clique follows from the definition of adjacency in Γ_n. We need to show that the clique is maximum.

Consider the closed neighbourhood of a vertex $v = (\{a, b\}, \{a\}) \in X_a$, i.e.,
$$N[v] = \{(\{a, b\}, \{b\})\} \cup \{(\{a, x\}, \{a\}) : x \neq a\}.$$
Since Γ_n is regular and vertex-transitive, to show that X_a is maximum it is sufficient to show that X_a is the largest clique containing v in $N[v]$. This is easily seen to hold because in $N[v]$, the vertex $(\{a, b\}, \{b\})$ is adjacent only to v. The remaining vertices in
$$N[v] \setminus \{(\{a, b\}, \{b\})\} = X_a$$
are pairwise adjacent. Hence X_a is the largest clique in $N[v]$. □

Corollary 4.7. *Γ_n has clique number $n - 1$ and it has n maximum cliques.*

We now consider automorphisms of Γ_n for $n \geq 4$. Recall that Γ_3 is the 6-cycle and hence has automorphism group D_6, the dihedral group.

Proposition 4.8. *If* $n \geq 4$ *then* $\mathrm{Aut}(\Gamma_n) \cong S_n$.

Proof. Let $\alpha \in S_n$. Since α induces a permutation σ_α of $V(\Gamma_n)$, define a map $f : S_n \to \mathrm{Aut}(\Gamma_n)$ by $f(\alpha) = \sigma_\alpha$. Then f is a homomorphism. It remains to show that f is also bijective.

Let α and β be distinct permutations in S_n. Then there exists an element a in Ω such that $\alpha(a) \neq \beta(a)$. Let $u = (\{a,b\},\{a\}) \in V(\Gamma_n)$. Then $\sigma_\alpha(u) = (\{\alpha(a),\alpha(b)\},\{\alpha(a)\})$ and $\sigma_\beta(u) = (\{\beta(a),\beta(b)\},\{\beta(a)\})$. Since $\sigma_\alpha(u) \neq \sigma_\beta(u)$, f is injective.

Let $\phi \in \mathrm{Aut}(\Gamma_n)$. By definition, ϕ preserves maximum cliques of Γ_n, i.e., $\phi : X_a \to X_b$ for some $a, b \in \Omega$. Since every maximum clique corresponds to an element of Ω, ϕ induces a permutation $\alpha \in S_n$ defined by $\phi(X_a) = X_{\alpha(a)}$. Hence f is onto. □

4.2.2 Designs from embeddings of $L^1(K_n) \boxtimes K_2$

In this section we consider designs obtained from Γ_n. We show that, in addition to the incidence design whose codes are our primary interest in Section 4.4, the graphs have what we have termed as 6-cycle designs.

In the incidence design of Γ_n, the block containing edges incident on a vertex $v = (\{a,b\},\{b\})$ is the set

$$\overline{(\{a,b\},\{b\})} = \{[(\{a,b\},\{b\}),(\{a,b\},\{a\})]\} \cup \{[(\{a,b\},\{b\}),(\{b,x\},\{b\})] : x \neq a,b\}.$$

It has incidence vector

$$v^{\overline{(\{a,b\},\{b\})}} = v^{[(\{a,b\},\{b\}),(\{a,b\},\{a\})]} + \sum_{x \neq a,b} v^{[(\{a,b\},\{b\}),(\{b,x\},\{b\})]}.$$

The 6-*cycle design* of Γ_n has parameters $1-\left(2\binom{n}{2}, 6, n-2\right)$. Its points are vertices of the graph. Each block contains vertices of a 6-cycle in the graph. Hence for any distinct elements a, b and c of Ω, the points

$$(\{a,b\},\{a\}),(\{a,c\},\{a\}),(\{a,c\},\{c\}),(\{b,c\},\{c\}),(\{b,c\},\{b\}),(\{a,b\},\{b\})$$

make up one block of the design. Notice that the 6-cycle formed by these vertices contains a pair of points from each of the maximum cliques X_a, X_b and X_c. Hence any pair of points from a given maximum clique determines a 6-cycle in the graph. Since every vertex in a maximum clique is adjacent to the remaining $n-2$ vertices, it lies on $(n-2)$ 6-cycles determined this way. By [2, Equation (1.2), p. 7], the design has $\binom{n-2}{3}\binom{n}{2}$ blocks.

Properties of the design are summarized in the following definition.

Definition 4.9. *Let* C_6 *be the* 6*-cycle* ($(\{a,b\},\{a\})$, $(\{a,c\},\{a\})$, $(\{a,c\},\{c\})$, $(\{b,c\},\{c\})$, $(\{b,c\},\{b\})$, $(\{a,b\},\{b\})$) *in* Γ_n *where* a, b *and* c *are distinct elements of* $\Omega = \{1,\cdots,n\}$. *Then the* 6***-cycle design*** *of* Γ_n *is a* $1-\left(2\binom{n}{2}, 6, n-2\right)$ *design with points the vertices of* Γ_n *and blocks the* $\binom{n-2}{3}\binom{n}{2}$ 6*-cycles of the form* C_6.

4.2.3 Incidence matrices of the graphs

Let Γ_n be an embedding of the strong product $L^1(K_n) \boxtimes K_2$ as presented in Definition 4.1. In this section we describe how incidence matrices G_n of the graphs will be written.

Let

$$V_1 = \{(\{a,b\},\{a\}),(\{a,b\},\{b\}) : a,b \in \{1,2,3\}, a<b\}\,.$$

For $4 \le i \le n$, let

$$V_{i-2} = \{(\{a,i\},\{a\}),(\{a,i\},\{i\}) : 4 \le i \le n, a<i\}\,.$$

Write G_n as follows. Order rows of G_n so that for given values of a and i, a row corresponding to a vertex $(\{a,i\},\{a\})$ is followed by a row corresponding to $(\{a,i\},\{i\})$. The first $(n-2)\binom{n-1}{2}$ columns of G_n correspond to edges between vertices in $\bigcup_{i=1}^{n-3} V_i$. These are followed by columns corresponding to edges between vertices in $\bigcup_{i=1}^{n-3} V_i$ and vertices in V_{n-2}, i.e., $\left(\bigcup_{i=1}^{n-3} V_i, V_{n-2}\right)$ is a bipartition. Lastly, write columns corresponding to edges between vertices in V_{n-2}. The resulting matrix is $2\binom{n}{2} \times (n-1)\binom{n}{2}$ of the form

$$G_n = \left[\begin{array}{c|c|c} G_{n-1} & I & \mathbf{0} \\ \hline \mathbf{0} & J & M_{n-1} \end{array}\right] \tag{4.1}$$

where:

(a) G_{n-1} is an incidence matrix of Γ_{n-1};

(b) I is the identity matrix of rank $(n-1)(n-2)$;

(c) J is a $2(n-1) \times (n-1)(n-2)$ matrix where every column is a unit vector. For $a < n$, each row corresponding to a vertex of the form $(\{a, n\}, \{a\})$ has weight $n-2$. The remaining $n-1$ rows corresponding to vertices of the form $(\{a, n\}, \{n\})$ are zero vectors;

(d) M_{n-1} is an incidence matrix of the complete porcupine H_{n-1} (see Definition 4.11).

Example 4.10. The twelve vertices of Γ_4 are ordered as follows: $(\{1,2\},\{1\})$, $(\{1,2\},\{2\})$, $(\{1,3\},\{1\})$, $(\{1,3\},\{3\})$, $(\{2,3\},\{2\})$, $(\{2,3\},\{3\})$, $(\{1,4\},\{1\})$, $(\{1,4\},\{4\})$, $(\{2,4\},\{2\})$, $(\{2,4\},\{4\})$, $(\{3,4\},\{3\})$, $(\{3,4\},\{4\})$. Its incidence matrix is

$$G_4 = \left[\begin{array}{c|c|c}
110000 & 100000 & 000000 \\
101000 & 010000 & 000000 \\
010100 & 001000 & 000000 \\
000110 & 000100 & 000000 \\
001001 & 000010 & 000000 \\
000011 & 000001 & 000000 \\
\hline
000000 & 101000 & 100000 \\
000000 & 000000 & 111000 \\
000000 & 010010 & 000100 \\
000000 & 000000 & 010110 \\
000000 & 000101 & 000001 \\
000000 & 000000 & 001011
\end{array}\right]. \tag{4.2}$$

4.3 Complete porcupines and their codes

We now consider complete porcupines (also simply called porcupines in [26]) and codes from their incidence matrices. We begin by defining the graphs. Codes from these graphs are examined in Proposition 4.12 and Corollary 4.13.

Definition 4.11. Let $\Omega = \{1, \cdots, n\}$ where $n \geq 3$. Let $A = \{(a, 0) : a \in \Omega\}$ and $B = \{(b, 1) : b \in \Omega\}$. Let K_A be the complete graph on A. The *complete porcupine* H_n is defined by $V(H_n) = A \cup B$ and $E(H_n) = E(K_A) \cup E_Q$ where $E_Q = \{[(a, 0), (a, 1)] | a \in \Omega\}$ is the set of *quills*.

Let M_n be an incidence matrix of the complete porcupine H_n. Write M_n as follows. Order its rows by first listing vertices in A followed by vertices in B. Order columns of the matrix by first obtaining edges between vertices in A followed by edges corresponding to quills of the complete porcupine. Then M_n takes the form

$$\left[\begin{array}{c|c} L_n & I \\ \hline \mathbf{0} & I \end{array}\right] \tag{4.3}$$

where L_n is an incidence matrix of K_A.

Proposition 4.12. *For $n \geq 3$ and any prime p, let $C_p(M_n)$ be the p-ary code from the row span of M_n, an incidence matrix of the complete porcupine H_n. Then $C_2(M_n) = \left[\binom{n+1}{2}, 2n-1, 1\right]_2$. If p is odd then $C_p(M_n) = \left[\binom{n+1}{2}, 2n, 1\right]_p$. In both cases, minimum words are the n unit vectors corresponding to quills of the porcupine.*

Proof. The length of the code is the order of $E(H_n) = E(K_A) \cup E_Q$ where, as in Definition 4.11, K_A is the complete graph on $A = \{(a, 0) : a \in \Omega\}$ and E_Q is the set of quills. Since the minimum weight and minimum words are easy to see, we only check the dimension of the codes.

The complete porcupine is connected and hence by Lemma 2.22, M_n has dimension $2n - 1$ over $\mathbb{F}_2$. Since the graph is not bipartite (as it has odd cycles in K_A), by Lemma 2.23, M_n has full rank over $\mathbb{F}_p$ if p is odd . □

Notice that the codes $C_p(M_n)$ are not full spaces despite having codewords of weight one. The following corollary is useful.

Corollary 4.13. *Let M_n be an incidence matrix of the complete porcupine as presented in* Equation (4.3). *For any prime p, let $C_p(M_n)$ be the p-ary code from the row span of M_n. Let $C_p(N_n)$ be the subcode of $C_p(M_n)$ from the row span over $\mathbb{F}_p$ of the submatrix $N_n = [L_n|I]$ of M_n. Then $C_p(N_n) = \left[\binom{n+1}{2}, n, n\right]_p$. Minimum words are scalar multiples of the rows of N_n.*

Proof. The length and dimension are clear. For the minimum weight, let $c \in C_p(N_n)$. Then c is a concatenation of two vectors c_1 and c_2 from the two column blocks in N_n. By Theorem 2.35, we have $\text{wt}(c_1) \geq n-1$. Since $\text{wt}(c_2) \geq 1$, the result follows. □

4.4 Codes from embeddings of the strong products $L^1(K_n) \boxtimes K_2$

We now turn to the main issue at hand; namely, the description and permutation decoding of codes from embeddings Γ_n of the strong products $L^1(K_n) \boxtimes K_2$ of triangular graphs and K_2. The case of $n = 3$ is less interesting; Γ_3 being a 6-cycle. It is stated in the following lemma.

Lemma 4.14. *Let G_3 be an incidence matrix of the* 6*-cycle* Γ_3 *and let $C_p(G_3)$ be the p-ary code from the row span of G_3 where p is any prime. Then $C_p(G_3) = [6, 5, 2]_p$.*

Proof. Dimensions of the binary and non-binary codes follow from Lemmas 2.22 and 2.23, respectively, since the 6-cycle is connected and bipartite.

Since $C_p(G_3)$ is spanned by weight-2 vectors, the binary code is even hence it does not have unit codewords. We need to check the minimum weight of $C_p(G_3)$ if p is an odd prime.

Write G_3 as the left uppermost submatrix of G_4 in Equation (4.2). Partition rows of the matrix as follows. Let R_1 be the block of the first three rows of G_3 and R_2 the remaining three rows of the matrix. Partition the columns into two blocks, the first comprising the first three columns.

Let $c \in C_p(G_3)$. Then c is a concatenation of two vectors, $c_1, c_2 \in \mathbb{F}_p^3$, from the two column blocks of G_3. Observe that each of the four submatrices of G_3 obtained from the partition described above has a unit vector. Thus if all possible linear combinations of rows of G_3 are considered, one obtains $\text{wt}(c_1) \geq 1$ and $\text{wt}(c_2) \geq 1$. Hence $\text{wt}(c) \geq 2$. This completes the proof of the lemma. □

Other minimum words of $C_p(G_3)$ are scalar multiples of codewords of the form $v^{\overline{u}} - v^{\overline{w}}$ where u and w are any adjacent vertices of Γ_3. The following codewords also have minimum weight:

$$v^{\overline{(\{a,b\},\{b\})}} - \sum_{(\{a',b'\},\{b'\}) \in N((\{a,b\},\{b\}))} v^{\overline{(\{a',b'\},\{b'\})}}.$$

We now determine parameters of the codes $C_p(G_n)$ where $n \geq 4$.

Proposition 4.15. *For $n \geq 4$ let G_n be an incidence matrix of Γ_n. Let $C_p(G_n)$ be the p-ary code from the row span of G_n where p is any prime.*

(a) *If p is odd then $C_p(G_n) = \left[(n-1)\binom{n}{2}, 2\binom{n}{2}, n-1\right]_p$ and its minimum words are scalar multiples of the rows of G_n.*

(b) *$C_2(G_n) = \left[(n-1)\binom{n}{2}, 2\binom{n}{2} - 1, n-1\right]_2$ and its minimum words are rows of G_n and the n vectors of the form $\sum_x v^{\overline{(\{a,x\},\{a\})}}$ where $x \neq a$.*

Proof. Recall that the complete porcupine H_{n-1} is an induced subgraph of Γ_n. H_{n-1} has odd cycles because it contains the complete graph. Hence by Proposition 2.3, Γ_n is non-bipartite. Since the graph is also connected, the non-binary codes have dimension $2\binom{n}{2}$ by Lemma 2.23. On the other hand, the binary codes have dimension $2\binom{n}{2} - 1$ by Lemma 2.22.

We now use induction to prove the assertion about the minimum weight of $C_p(G_n)$ noting that it holds for $C_p(G_3)$ in Lemma 4.14. Suppose the result holds for $n-1$. Write G_n as in Equation (4.1). Label the first $(n-1)(n-2)$ rows of G_n by R_1 and the remaining $2(n-1)$ rows by R_2, i.e., $R_1 = [G_{n-1}|I|\mathbf{0}]$ and $R_2 = [\mathbf{0}|J|M_{n-1}]$.

Let $c \in C_p(G_n)$. Then c is a concatenation of three vectors, c_1, c_2 and c_3, from the three column blocks of G_n where $c_i \in \mathbb{F}_p^{k_i}$, $k_1 = (n-2)\binom{n-1}{2}$, $k_2 = (n-1)(n-2)$ and $k_3 = \binom{n}{2}$.

(a) Suppose c is a linear combination of r_1 rows of R_1. Then $c_1 = \sum \alpha_i g_i$ and $c_2 = \sum \alpha_i I$ where $\alpha_i \in \mathbb{F}_p^*$ and g_i is the ith row of G_{n-1}. By assumption, $\text{wt}(c_1) \geq n-2$. Since $\text{wt}(c_2) = r_1$, we have $\text{wt}(c) \geq n-2+r_1 \geq n-1$. From the form of G_n, it is clear that $\text{wt}(c) = n-1$ if c is a scalar multiple of a row of R_1.

Suppose c is a linear combination of r_2 rows of R_2. Then $c_2 = \sum \alpha_i j_i$ and $c_3 = \sum \alpha_i m_i$ where $\alpha_i \in \mathbb{F}_p^*$ and j_i and m_i are ith rows of J and M_{n-1}, respectively. If $j_i \neq \mathbf{0}$ for any i then $\text{wt}(c_2) \geq n-2$ since no pair of rows of

J is commonly incident. Equality occurs if c is a non-zero row of J in which case $\mathrm{wt}(c_3) = 1$. Hence $\mathrm{wt}(c) \geq n-1$ with equality if c is a scalar multiple of a row of R_2. If c is a linear combination of rows corresponding to vertices of the form $(\{a, n\}, \{n\})$ then $c_2 = \mathbf{0}$. By Corollary 4.13, $\mathrm{wt}(c) = \mathrm{wt}(c_3) \geq n-1$ with equality if c is a multiple of an $(\{a, n\}, \{n\})$-indexed row of G_n.

Finally, suppose c is a linear combination of r_1 rows of R_1 and r_2 rows of R_2. By assumption, $\mathrm{wt}(c_1) \geq n-2$. By Proposition 4.12, $\mathrm{wt}(c_3) \geq 1$. If $\mathrm{wt}(c_3) = 1$ then it is clear that $c_2 \neq \mathbf{0}$. Hence $\mathrm{wt}(c) \geq (n-1) + \mathrm{wt}(c_2) > n-1$.

(b) Let us now consider the minimum weight of the binary codes. Since the result of adding all rows of an incidence matrix is the zero vector, in addition to cases considered in (a) above, we only need to examine situations where all rows of G_{n-1} or M_{n-1} are added.

Let $c \in C_2(G_n)$. Suppose c is a sum of all rows of R_1. Then $c_2 = \sum_i e_i$ where e_i is the ith row of the identity matrix I. Since I has rank $(n-1)(n-2)$, we have $\mathrm{wt}(c) = \mathrm{wt}(c_2) = (n-1)(n-2) > n-1$.

Suppose c is a sum of all rows of R_2. Then $c_2 = \sum_i j_i$ where j_i is the ith row of J. Since no pair of rows of J is commonly incident and the $n-1$ non-zero rows have weight $n-2$, we have $\mathrm{wt}(c) = \mathrm{wt}(c_2) = (n-1)(n-2) > n-1$.

Suppose c is a sum of r_1 rows of R_1 and r_2 rows of R_2. There are two possible cases to consider in addition to those examined in (a).

Case (i)**.** $r_1 = (n-1)(n-2)$ and $r_2 < 2(n-1)$.

If r_2' of the r_2 rows of J are non-zero then $\mathrm{wt}(c_2) = (n-1)(n-2) - r_2'(n-2)$ and $\mathrm{wt}(c_3) \geq 1$. If $r_2' = n-1$ then all non-zero rows of J are added. Hence $\mathrm{wt}(c_2) = 0$ and c_3 is a sum of $n-1$ unit vectors. We have $\mathrm{wt}(c) = \mathrm{wt}(c_3) = n-1$. In this case, c has support

$$\{[(\{a, n\}, \{a\}), (\{a, n\}, \{n\})] : a < n\} = \mathrm{Supp}\left(\sum_{a<n} v^{\overline{(\{a,n\},\{n\})}}\right).$$

Hence $c = \sum\limits_{a<n} v^{\overline{(\{a,n\},\{n\})}}$.

If $r_2' < n-1$ then at least one $(\{a, n\}, \{a\})$-indexed row of J is not used in the sum. Hence $\mathrm{wt}(c_2) \geq n-2$, $\mathrm{wt}(c_3) \geq 1$ and $\mathrm{wt}(c) \geq n-1$. Equality occurs if $r_2' = r_2 = n-2$ and c is the $(\{a,n\},\{a\})$-indexed row of J that is not in the sum.

Case (ii)**.** $r_1 < (n-1)(n-2)$ and $r_2 = 2(n-1)$.

This case gives $\mathrm{wt}(c_1) \geq n-2$, $\mathrm{wt}(c_2) \geq 1$ and $c_3 = \mathbf{0}$. $\mathrm{wt}(c_2) = 1$ if $r_1 = (n-1)(n-2) - 1$ in which case c_2 is a row of I. Hence $\mathrm{wt}(c) = n-1$ if c is the row of G_n that is not added.

As seen from observations above, $C_2(G_n)$ has other minimum words in addition to rows of G_n. Since the $n-1$ vertices in X_a form a complete graph for each $a \in \Omega$, the $n-1$ incidence vectors $v^{\overline{(\{a,x\},\{a\})}}$, where $(\{a,x\},\{a\}) \in X_a$, are pairwise commonly incident at exactly $\binom{n-1}{2}$ coordinate positions. Therefore the codeword $\sum_x v^{\overline{(\{a,x\},\{a\})}}$ has weight $(n-1)^2 - 2\binom{n-1}{2} = n-1$. This way, we determine n more minimum words. □

4.5 Permutation decoding

In this section we determine permutation automorphisms of the p-ary codes $C_p(G_n)$, p any prime, obtained from the row span of incidence matrices G_n of the graphs Γ_n of Definition 4.1. An information set for the codes is given in Proposition 4.17 where PD-sets for full permutation decoding are also exhibited.

Proposition 4.16. *For any prime p and $n \geq 4$, let $C_p(G_n)$ be the p-ary code from the row span of G_n, an incidence matrix of Γ_n. Let $\mathcal{D}$ be the incidence design of Γ_n. Then $\mathrm{Aut}(C_p(G_n)) \cong \mathrm{Aut}(\mathcal{D}) = S_n$.*

Proof. As in Proposition 3.7, we only need to show that $\mathrm{Aut}(C_p(G_n)) \subseteq \mathrm{Aut}(\mathcal{D})$. Cases of p odd and $p = 2$ are treated separately.

Case (i)**.** p odd.

By Proposition 4.15, if p is odd then minimum words of $C_p(G_n)$ are scalar multiples of incidence vectors of blocks of $\mathcal{D}$. Let $\rho \in \mathrm{Aut}(C_p(G_n))$. Since ρ

preserves weight classes of the code, it permutes the minimum words. For each incidence vector $v^{\overline{(\{a,b\},\{a\})}}$ there exists an incidence vector $v^{\overline{(\{a',b'\},\{a'\})}}$ such that $\rho(v^{\overline{(\{a,b\},\{a\})}}) = v^{\overline{(\{a',b'\},\{a'\})}}$. Hence ρ induces a permutation of blocks of $\mathcal{D}$ that preserves incidence of points with blocks. Therefore ρ corresponds to an automorphism of the design.

Case (ii)**.** $p = 2$.

By Proposition 4.15, minimum words of the binary codes are rows of G_n and codewords of the form $\sum_{x\neq a} v^{\overline{(\{a,x\},\{a\})}}$ where a is constant.

We show that it is not possible for an automorphism of $C_2(G_n)$ to map a row of G_n to a codeword of the form $\sum_{x\neq a} v^{\overline{(\{a,x\},\{a\})}}$. Let

$$S_a = \{[(\{a,x\},\{a\}),(\{a,x\},\{x\})] : x \neq a\} = \text{Supp}\left(\sum_{x\neq a} v^{\overline{(\{a,x\},\{a\})}}\right).$$

A fixed element $[(\{a,b\},\{a\}),(\{a,b\},\{b\})]$ of S_a is also in the support S_b of $\sum_{x\neq b} v^{\overline{(\{b,x\},\{b\})}}$. This holds for every element of S_a. Therefore minimum words of the form $\sum_{x\neq a} v^{\overline{(\{a,x\},\{a\})}}$ are pairwise commonly incident. This property is not satisfied by rows of G_n. An automorphism of $C_2(G_n)$ must preserve this property. It hence maps rows to rows and codewords of the form $\sum_{x\neq a} v^{\overline{(\{a,x\},\{a\})}}$ to similar codewords. By permuting the incidence vectors (as observed in the odd p case above), every automorphism of $C_2(G_n)$ induces an automorphism of the design. Hence $\text{Aut}(C_2(G_n)) \subseteq \text{Aut}(\mathcal{D})$. This completes the proof. □

We now give information sets for $C_p(G_n)$ and exhibit PD-sets for full permutation decoding.

Proposition 4.17. *For any prime p and $n \geq 5$, let $C_p(G_n)$ be the p-ary code from the row span of G_n, an incidence matrix of Γ_n. Let $A_1 = \{[(\{a,n\},\{a\}),(\{a,k\},\{a\})] | k \neq a, n\}$, $A_2 = \{[(\{b,n\},\{n\}),(\{b,n\},\{b\})] | b \neq n\}$, $A_3 = \{[(\{n-1,n\},\{n\}),(\{c,n\},\{n\})] | c \neq n-1, n\}$. Then*

(a) *$\mathcal{I}_n = \bigcup_{i=1}^{3} A_i$ is an information set for $C_2(G_n)$. If p is odd then*

$$\mathcal{I}_n \cup \{[(\{n-3,n\},\{n\}),(\{n-2,n\},\{n\})]\}$$

is an information set for $C_p(G_n)$;

(b) *If $p = 2$ then the set*

$$S = \{(1), (n-1, y)(n, x) | 1 \leq x, y \leq n-1, x \neq y\}$$

of $n + (n-2)^2$ elements of S_n is a PD-set for $C_2(G_n)$ with $\mathcal{I}_n$ as information set.

If p is odd then

$$S \cup \{(n-2, y)(n, x) : x, y \in \Omega \setminus \{n\}, y \leq n-4\}$$

is a PD-set with

$$\mathcal{I}_n \cup \{[(\{n-3, n\}, \{n\}), (\{n-2, n\}, \{n\})]\}$$

as information set.

Proof. (a) We first show that columns of G_n indexed by points in $\mathcal{I}_n$ are linearly independent over $\mathbb{F}_2$ and hence $\mathcal{I}_n$ is an information set for $C_2(G_n)$.

Write G_n as in Equation (4.1). Points in A_1 are indices of the $2\binom{n-1}{2}$ columns of the identity matrix.

Re-order rows and columns of M_{n-1} as follows. List rows corresponding to vertices in

$$B_1 = \{(\{b, n\}, \{b\}) | b \neq n\}$$

followed by rows corresponding to vertices in

$$B_2 = \{(\{b, n\}, \{n\}) | b \neq n\}$$

in lexicographic order. Write columns corresponding to edges between vertices in B_1 and vertices in B_2 followed by columns corresponding to edges between vertices in B_2. In this way, M_{n-1} takes the form

$$\left[\begin{array}{c|c} I & \mathbf{0} \\ \hline I & L_{n-1} \end{array}\right] \tag{4.4}$$

where I is the $(n-1) \times (n-1)$ identity matrix and L_{n-1} is an incidence matrix of K_{n-1}. Columns of I are indexed by points in A_2.

Re-arrange columns of L_{n-1} so that they begin with those indexed by the following points in the given order.

$$[(\{1,n\},\{n\}),(\{n-1,n\},\{n\})],\cdots,[(\{n-2,n\},\{n\}),(\{n-1,n\},\{n\})],$$
$$[(\{n-3,n\},\{n\}),(\{n-2,n\},\{n\})].$$

Then L_{n-1} takes the form

$$\left[\begin{array}{c|c} I & L_{n-2} \\ \hline 11\cdots1 & 00\cdots0 \end{array}\right]$$

where I is the $(n-2)\times(n-2)$ identity matrix with columns indexed by points in A_3. L_{n-2} is an incidence matrix of K_{n-2}.

With these permutations of rows and columns, G_n takes the form

$$\left[\begin{array}{c|c|c|cc} G_{n-1} & I & \multicolumn{3}{c}{\mathbf{0}} \\ \hline & & I & \multicolumn{2}{c}{\mathbf{0}} \\ \cline{3-5} \mathbf{0} & \bar{J} & & I & \multicolumn{1}{|c}{L_{n-2}} \\ \cline{4-5} & & I & 1\cdots1 & \multicolumn{1}{|c}{0\cdots0} \end{array}\right].$$

Excluding the last row from consideration, columns with the identity matrices are easily seen to be linearly independent over $\mathbb{F}_2$. They are indexed by elements of $\mathcal{I}_n$. Hence $\mathcal{I}_n$ is an information set for $C_2(G_n)$.

If p is odd, adding to $\mathcal{I}_n$ the point

$$[(\{n-3,n\},\{n\}),(\{n-2,n\},\{n\})]$$

gives a linearly independent set of columns. Hence

$$\mathcal{I}_n\cup\{[(\{n-3,n\},\{n\}),(\{n-2,n\},\{n\})]\}$$

is an information set for $C_p(G_n)$.

(b) Let

$$A_4=\{[(\{d,n\},\{n\}),(\{e,n\},\{n\})]|d,e\neq n-1,n\},$$
$$A_5=\{[(\{f,g\},\{g\}),(\{f,g\},\{f\})]|f,g\neq n\},$$
$$A_6=\{[(\{h,l\},\{l\}),(\{j,l\},\{l\})]|j,h,l\neq n\}.$$

Then $\mathcal{C} = A_4 \cup A_5 \cup A_6$ is a check set for $C_2(G_n)$. The non-binary codes have check set

$$\mathcal{C} \setminus \{[(\{n-3, n\}, \{n\}), (\{n-2, n\}, \{n\})]\}\,.$$

Notice that $A_5 \cup A_6 = E(\Gamma_{n-1})$.

We first determine PD-sets for the binary codes. Since the minimum distance is $n-1$, the codes correct up to $\lfloor (n-2)/2 \rfloor$ errors. Suppose a codeword is sent and a vector y is received such that $t \le \lfloor (n-2)/2 \rfloor$ errors occur. Let $\mathcal{E}$ be the set of error coordinates of y. There are three possible cases.

Case (i)**.** $\mathcal{E} \subset \mathcal{C}$.

Use the identity permutation (1) of S_n to fix errors in the check set $\mathcal{C}$.

Case (ii)**.** $\mathcal{E} \subset \mathcal{I}_n \cup \mathcal{C} \setminus A_6$.

Suppose there are at most n_i errors in A_i where $1 \le i \le 5$. Then $2\sum n_i \le n-2$. Let $\mathcal{T}_1 = \{a_1, \cdots, a_{n_1}, k_1, \cdots, k_{n_1}\}$, $\mathcal{T}_2 = \{b_1, \cdots, b_{n_2}\}$, $\mathcal{T}_3 = \{c_1, \cdots, c_{n_3}, n-1\}$, $\mathcal{T}_4 = \{d_1, \cdots, d_{n_4}, e_1, \cdots, e_{n_4}\}$, $\mathcal{T}_5 = \{f_1, \cdots, f_{n_5}, g_1, \cdots, g_{n_5}\}$. Let $\mathcal{T} = \bigcup_{i=1}^{5} \mathcal{T}_i$. Then

$$|\mathcal{T}| \le 2n_1 + n_2 + n_3 + 1 + 2n_4 + 2n_5 < n.$$

Since $2\sum n_i \le n-2$, we have $|\mathcal{T}| \le n-2$. Hence there exists $x \in \Omega \setminus \{n\}$ such that $x \notin \mathcal{T}$. Use a transposition of the form (n, x) to map $\mathcal{E}$ into $\mathcal{C}$ and fix errors already in $\mathcal{C}$.

Case (iii)**.** $\mathcal{E} \subset \mathcal{I}_n \cup \mathcal{C}$.

Suppose at most n_6 errors occur in A_6. Let

$$\mathcal{T}_6 = \{j_1, \cdots, j_{n_6}, l_1, \cdots, l_{n_6}\}.$$

Then

$$|\mathcal{T} \cup \mathcal{T}_6| \le 2n_1 + n_2 + n_3 + 2n_4 + 2n_5 + 2n_6 < n.$$

Since $2\sum n_i \leq n-2$, there exists $x \in \Omega \setminus \{n\}$ such that $x \notin \mathcal{T} \cup \mathcal{T}_6$. Use a transposition of the form (n, x).

Suppose $x = l$ and there is an error coordinate $[((n-1)l, l), (jl, l)]$ in A_6 where $j \leq n-2$. Then (n, x) maps this point to an information position in A_3. Use an automorphism of the form $(y, n-1)(n, x)$ where $y \leq n-2$ and $y \neq j, x$.

In addition to cases considered above, if p is odd there is a problem if $h = n-2$, $j = n-3$ and $x = l$ for points in A_6 because a transposition of the form (n, l) maps $[(\{n-2, l\}, \{l\}), (\{n-3, l\}, \{l\})]$ to $[(\{n-2, n\}, \{n\}), (\{n-3, n\}, \{n\})]$, an information position. Use an automorphism of the form $(n-2, y)(n, x)$ where $1 \leq y \leq n-4$. □

Remark 4.18. Computations using Magma [7] for small values of n suggest that the Gordon bound is $\frac{n}{2}+1$ if n is even and $\frac{n-1}{2}$ if n is odd.

Chapter 5

Codes from graphs related to the categorical product of triangular graphs and K_n

5.1 Introduction

In the previous chapter, we considered two classes of graphs, H_n and Γ_n, where $n \geq 3$, H_n is the complete porcupine and Γ_n is an embedding of $L^1(K_n) \boxtimes K_2$, the strong product of triangular graphs and K_2. Also recall that if $n \geq 4$ then H_{n-1} is an induced subgraph of Γ_n. We also examined codes from incidence matrices of the graphs and exhibited PD-sets for full permutation decoding of codes from Γ_n.

In this chapter, we consider complements of H_n and Γ_n and codes from their incidence matrices. The graphs are denoted $\overline{H}_n$ and $\overline{\Gamma}_n$, respectively. Since most properties of the graphs that are of interest to us are concluded from those of H_n and Γ_n, we only establish automorphisms of the complete porcupines as this was not done in Chapter 4. We also show that $\overline{\Gamma}_n$ is contained in the union of $L^1(K_n) \times K_n$ and $\overline{L^1(K_n)} \times K_n$, where $\times$ is the categorical product of graphs and $\overline{L^1(K_n)}$ is the complement of the triangular graph $L^1(K_n)$. In both cases, permutation decoding is used for codes from incidence matrices of the graphs. Even though the graphs $\overline{H}_n$ are not edge-transitive, we have achieved full permutation decoding for codes from their incidence matrices. In the case of codes from $\overline{\Gamma}_n$, we only exhibit PD-sets for partial permutation decoding.

What is presented in this chapter is the content of [48]. Our main results are summarised in the two theorems below. Theorem 5.1 is on codes from incidence matrices of $\overline{H}_n$ and Theorem 5.2 is on codes from incidence matrices of $\overline{\Gamma}_n$.

Theorem 5.1. *For $n \geq 3$, let $\overline{H}_n$ be the complement of the complete porcupine, the graph of* Definition 4.11. *Let G_n be an incidence matrix of $\overline{H}_n$. For any prime p, let $C_p(G_n)$ be the p-ary linear code from the row span of G_n. Let $A_1 = \{[(1,1),(a,1)] : a \neq 1\}$, $A_2 = \{[(1,1),(b,0)] : b \neq 1\}$ and $A_3 = \{[(2,1),(1,0)]\}$. Then*

(a) $\mathrm{Aut}(\overline{H}_n) \cong S_n \cong \mathrm{Aut}(C_p(G_n))$;

(c) $C_2(G_n) = \left[3\binom{n}{2}, 2n-1, n-1\right]_2$. *If p is odd then* $C_p(G_n) = \left[3\binom{n}{2}, 2n, n-1\right]_p$. *In both cases minimum words are scalar multiples of the rows indexed by vertices of degree $n-1$;*

(d) $\mathcal{I}_n = \bigcup_{i=1}^{3} A_i$ *is an information set for $C_2(G_n)$. If p is odd then $\mathcal{I}_n \cup \{[(2,1),(n,0)]\}$ is an information set for $C_p(G_n)$.*

The set $\{(1),(1,x) : x \in \Omega \setminus \{1\}\}$ of n elements of S_n is a PD-set for $C_p(G_n)$ for any prime p.

Theorem 5.2. *For $n \geq 4$, let $\overline{\Gamma}_n$ be the complement of an embedding Γ_n of the strong product $L^1(K_n) \boxtimes K_2$ presented in* Definition 4.1. *Let M_n be an incidence matrix of $\overline{\Gamma}_n$. For any prime p, let $C_p(M_n)$ be the p-ary code from the row span of M_n. Let $\mathcal{D}$ be the incidence design of $\overline{\Gamma}_n$. Let*
$A_1 = \{[(\{1,2\},\{1\}),u] : u \in N((\{1,2\},\{1\}))\}$ *and*
$A_2 = \{[(\{1,2\},\{2\}),(\{1,x\},\{1\})] : 3 \leq x \leq n\}$.

(a) $C_2(M_n) = \left[(n^2-2n)\binom{n}{2}, 2\binom{n}{2}-1, n(n-2)\right]_2$ *and its minimum words are rows of M_n;*

(b) *If p is odd then $C_p(M_n) = \left[(n^2-2n)\binom{n}{2}, 2\binom{n}{2}, n(n-2)\right]_p$ and its minimum words are scalar multiples of the rows of M_n;*

(c) $\mathrm{Aut}(C_p(M_n)) \cong \mathrm{Aut}(\mathcal{D}) \cong S_n$;

(d) *$\mathcal{I}_n = A_1 \cup A_2 \cup \{[(12,2),(13,3)]\}$ is an information set for $C_2(M_n)$. The set*

$$S = \{(1),(1,x)(2,y) : x,y \neq 1,2\}$$

of $\binom{n-2}{2}+1$ elements of S_n is an $\left\lfloor \frac{n^2-5n+6}{4} \right\rfloor$-PD-set for $C_2(M_n)$ with $\mathcal{I}_n$ as information set.

As has been done in previous chapters, the two theorems are proved using a series of lemmas and propositions in Sections 5.2 and 5.3, respectively. In Section 5.2 properties of $\overline{H}_n$ are given and automorphism groups of the graphs determined. The main focus of this section is the description and permutation decoding of binary and non-binary codes from incidence matrices of $\overline{H}_n$. An information set and PD-sets for full permutation decoding of the codes are exhibited in Proposition 5.9. The size of the PD-sets is only twice the Gordon bound. In Section 5.3, the main focus is on codes from incidence matrices of $\overline{\Gamma}_n$. Again, the main results of this section are the determination of parameters of the codes and PD-sets for partial permutation decoding of the binary codes.

5.2 The graphs $\overline{H}_n$ and their codes

The definition of $\overline{H}_n$ follows from Definition 4.11. We however state it formally below as done in [48]. This way some properties of the graphs are easier to see.

Definition 5.3. Let $\Omega = \{1,\cdots,n\}$ where $n \geq 3$. Let $A = \{(a,0) : a \in \Omega\}$ and $B = \{(a,1) : a \in \Omega\}$. Then the complement of the complete porcupine $\overline{H}_n$ is defined by

$$\begin{aligned} V(\overline{H}_n) &= A \cup B \\ E(\overline{H}_n) &= E(K_B) \cup \{[(a,0),(b,1)] : a,b \in \Omega, a \neq b\}. \end{aligned}$$

We make the following observations. Each vertex of the form $(i,0)$ has degree $n-1$ since it is adjacent to vertices of the form $(j,1)$ where $j \in \Omega$ and $j \neq i$. Each vertex of the form $(i,1)$ has degree $2(n-1)$ since it is adjacent to vertices of the form $(j,0)$ and $(j,1)$ where $j \in \Omega$ and $j \neq i$. Hence $\overline{H}_n$ is not regular. It has $3\binom{n}{2}$ edges. $\overline{H}_4$ is illustrated in Figure 5.1.

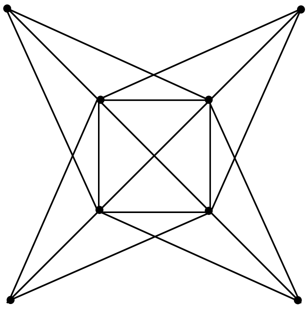

Figure 5.1: The graph $\overline{H}_4$

5.2.1 Automorphisms of complete porcupines

In this section we determine automorphisms of complete porcupines H_n.

Lemma 5.4. *For $n \geq 3$, let $\overline{H}_n$ be the complement of the complete porcupine as given in* Definition 5.3. *Let $\alpha \in S_n$. Then α induces an automorphism of $\overline{H}_n$.*

Proof. Define a map $\sigma_\alpha : V(\overline{H}_n) \rightarrow V(\overline{H}_n)$ by $\sigma_\alpha((a,x)) = (\alpha(a), x)$ where $x = 0, 1$. We need to show that $\sigma_\alpha \in \mathrm{Aut}(\overline{H}_n)$.

It is clear that σ_α is bijective. Also, σ_α preserves adjacency in the graph. To see this, let u and v be any two adjacent vertices in $\overline{H}_n$. By the adjacency conditions in Definition 5.3, either $u = (a,1)$ and $v = (b,1)$ or $u = (a,1)$ and $v = (b,0)$ for distinct $a, b \in \Omega$. In both cases, $[\sigma_\alpha(u), \sigma_\alpha(v)] \in E(\overline{H}_n)$. Hence $\sigma_\alpha \in \mathrm{Aut}(\overline{\mathrm{H}}_\mathrm{n})$. □

We now show that $\mathrm{Aut}(\overline{H}_n)$ is isomorphic to S_n, the symmetric group on Ω.

Proposition 5.5. *For $n \geq 3$, let $\overline{H}_n$ be the complement of the complete porcupine as presented in* Definition 5.3. *Then* $\mathrm{Aut}(\overline{H}_n) \cong S_n$.

Proof. Let $\alpha \in S_n$. By Lemma 5.4, α induces an automorphism σ_α of $\overline{H}_n$. Define a map $f : S_n \rightarrow \mathrm{Aut}(\overline{H}_n)$ by $f(\alpha) = \sigma_\alpha$. Then f is a homomorphism. We need to show that f is also bijective.

Let α and β be distinct elements of S_n. Then there exists $a \in \Omega$ such that $\alpha(a) \neq \beta(a)$. Consider the vertex (a, x) where $x = 0$ or $x = 1$. Since $\sigma_\alpha((a,x)) \neq \sigma_\beta((a,x))$, f is injective. It remains to show that f is onto.

Let B be as in Definition 5.3. Consider K_B, the maximum clique in $\overline{H}_n$. Let $\phi \in \operatorname{Aut}(\overline{H}_n)$. By definition, ϕ preserves maximum cliques. Hence $\phi((a,1)) = (b,1)$ for some vertices $(a,1)$ and $(b,1)$ in B. Thus ϕ induces a permutation $\bar{\alpha} \in S_n$ such that $\bar{\alpha}(a) = b$. This completes the proof. □

Notice that the complement of the complete porcupine is neither vertex-transitive nor edge-transitive.

5.2.2 Incidence matrices of the graphs

We now describe how incidence matrices of $\overline{H}_n$ will be written. Recall that $V(\overline{H}_n) = A \cup B$ where $A = \{(a,0) : a \in \Omega\}$ and $B = \{(a,1) : a \in \Omega\}$.

Let G_n be an incidence matrix of $\overline{H}_n$. Write G_n as follows. Rows are ordered by first writing rows corresponding to vertices in B followed by those corresponding to vertices in A. List columns corresponding to edges between vertices in B. These are followed by columns corresponding to edges between vertices in B and those in A. Then G_n is a $2n \times 3\binom{n}{2}$ matrix of the form

$$\left[\begin{array}{c|c} L_n & M \\ \hline \mathbf{0} & N \end{array}\right], \tag{5.1}$$

where

(a) L_n is an $n \times \binom{n}{2}$ incidence matrix of K_n;

(b) M is an $n \times 2\binom{n}{2}$ matrix such that each row has $n-1$ consecutive entries 1 and no pair of row vectors is commonly incident;

(c) N is a column permutation of M.

Example 5.6. *If $n = 4$ then*

$$G_4 = \left[\begin{array}{c|c} 111000 & 111000000000 \\ 100110 & 000111000000 \\ 010101 & 000000111000 \\ 001011 & 000000000111 \\ \hline 000000 & 000100100100 \\ 000000 & 100000010010 \\ 000000 & 010010000001 \\ 000000 & 001001001000 \end{array}\right].$$

5.2.3 Codes from complements of complete porcupines

In the proposition below, we determine parameters of the codes $C_p(G_n)$ spanned over $\mathbb{F}_p$ by rows of G_n where p is any prime.

Proposition 5.7. *For $n \geq 3$ and any prime p, let $C_p(G_n)$ be the p-ary code from the row span of G_n, an incidence matrix of the complement of the complete porcupine* (*see* Definition 5.3). *If $p = 2$ then $C_2(G_n) = [3\binom{n}{2}, 2n-1, n-1]_2$ while if p is odd then $C_p(G_n) = [3\binom{n}{2}, 2n, n-1]_p$. For any p, minimum words of $C_p(G_n)$ are scalar multiples of the rows of G_n of weight $n-1$.*

Proof. Dimensions of the binary and non-binary codes are obtained using Lemmas 2.22 and 2.23, respectively, since the graphs are connected and, having 3-cycles in K_B, non-bipartite. We hence only prove the assertion about the minimum weights.

Write G_n as in Equation (5.1). Let R_1 and R_2 be the submatrices $[L_n|M]$ and $[\mathbf{0}|N]$, respectively. Let $c \in C_p(G_n)$. Then c is a concatenation of two vectors, c_1 and c_2, from the two column blocks of G_n where $c_1 \in \mathbb{F}_p^{\binom{n}{2}}$ and $c_2 \in \mathbb{F}_p^{2\binom{n}{2}}$.

Suppose c is a linear combination of r_1 rows of R_1. By Theorem 2.35, $\mathrm{wt}(c_1) \geq n-1$ (the minimum weight of non-binary codes in Theorem 2.35 also holds for the binary codes as remarked in Section 2.6.2). Since $\mathrm{wt}(c_2) = (n-1)r_1$, we have $\mathrm{wt}(c) \geq (n-1)(1+r_1) > n-1$. If $r_1 = 1$ then $\mathrm{wt}(c) = 2(n-1)$ and c is a row of R_1. Over $\mathbb{F}_2$, if all rows of R_1 are added then $c_1 = \mathbf{0}$ and $\mathrm{wt}(c_2) = 2\binom{n}{2} > n-1$.

Suppose c is a linear combination of r_2 rows of R_2. Since no pair of rows of R_2 commonly incident, $\mathrm{wt}(c_2) = (n-1)r_2 \geq n-1$. If $r_2 = 1$ then $\mathrm{wt}(c) = \mathrm{wt}(c_2) = n-1$, i.e., c is a row of R_2.

Suppose c is a linear combination of r_1 rows of R_1 and r_2 rows of R_2. We first consider the binary case.

Over $\mathbb{F}_2$, if $r_1 \neq n$ and $r_2 \neq n$ then $\mathrm{wt}(c_1) \geq n-1$ by Theorem 2.35. Also, $\mathrm{wt}(c_2) \neq 0$. Hence $\mathrm{wt}(c) > n-1$. If $r_1 = n$ and $r_2 \neq n$ then $c_1 = \mathbf{0}$. Since the sum of all rows of M is the all-one vector, $\mathrm{wt}(c_2) \geq n-1$ with equality if c_2 is a row of N. If $r_1 \neq n$ and $r_2 = n$ then $\mathrm{wt}(c_1) \geq n-1$ and $\mathrm{wt}(c_2) \neq 0$.

Hence $\mathrm{wt}(c) > n-1$.

Over $\mathbb{F}_p$, p odd, we have $\mathrm{wt}(c_1) \geq n-1$ by Theorem 2.35. If $\mathrm{wt}(c_2) \neq 0$ then we are done. If $\mathrm{wt}(c_2) = 0$ then a scalar multiple of the sum of all rows of R_1 is subtracted from that of all rows of R_2. Since $\mathrm{wt}(c_1) = n-1$ only if c is a scalar multiple of a row of L_n by Theorem 2.35, we have $\mathrm{wt}(c_1) > n-1$, completing the proof. □

5.2.4 Permutation decoding

We now consider permutation decoding of the codes obtained in Proposition 5.7. We first determine the permutation automorphism group of the code. A subset of this group is used in Proposition 5.9 for permutation decoding of both the binary and non-binary codes.

Proposition 5.8. *Let $C_p(G_n)$ be the p-ary code from the row span of G_n, an incidence matrix of the complement of the complete porcupine $\overline{H}_n$ where $n \geq 3$ and p is any prime. Then* $\mathrm{Aut}(C_p(G_n)) \cong \mathrm{Aut}(\overline{H}_n) \cong S_n$.

Proof. As done in Propositions 3.7 and 5.3, we only need to show that $\mathrm{Aut}(C_p(G_n) \subseteq \mathrm{Aut}(\overline{H}_n)$.

Let $\sigma \in \mathrm{Aut}(C_p(G_n))$. Then σ preserves minimum words of the code. By Proposition 5.7, minimum words of $C_p(G_n)$ are scalar multiples of the rows of the form $v^{\overline{(a,0)}}$. Hence there exist incidence vectors $v^{\overline{(a,0)}}$ and $v^{\overline{(b,0)}}$ such that $\sigma(v^{\overline{(a,0)}}) = v^{\overline{(b,0)}}$. Let $[(a,0),(c,1)] \in \mathrm{Supp}(v^{\overline{(a,0)}})$, the support of $v^{\overline{(a,0)}}$. Since σ permutes coordinate positions of $C_p(G_n)$, there exists a point $[(b,0),(d,1)] \in \mathrm{Supp}(v^{\overline{(b,0)}})$ such that $\sigma([(a,0),(c,1)]) = [(b,0),(d,1)]$. Therefore σ corresponds to a permutation $\bar{\sigma} \in S_n$ such that $\bar{\sigma}(a) = b$ and $\bar{\sigma}(c) = d$ where $a,b,c,d \in \Omega$. Thus $\mathrm{Aut}(C_p(G_n) \subseteq \mathrm{Aut}(\overline{H}_n) = S_n$. This completes the proof. □

We now exhibit a subset of S_n for full permutation decoding of both the binary and non-binary codes.

Proposition 5.9. *For any prime p and $n \geq 3$, let $C_p(G_n)$ be the p-ary linear codes from the row span of G_n, an incidence matrix of the complement of the complete porcupine. Let $A_1 = \{[(1,1),(a,1)] : a \neq 1\}$, $A_2 = \{[(1,1),(b,0)] : b \neq 1\}$ and $A_3 = \{[(2,1),(1,0)]\}$.*

(a) $\mathcal{I}_n = \bigcup_{i=1}^{3} A_i$ *is an information set for* $C_2(G_n)$*. If* p *is odd then* $\mathcal{I}_n \cup \{[(2,1),(n,0)]\}$ *is an information set for* $C_p(G_n)$*;*

(b) $S = \{(1,x) : x \in \Omega\}$ *is a PD-set for* $C_2(G_n)$ *of* n *elements of* S_n*.*

If p *is odd then* $S \cup \{(1,2,n)\}$ *is a PD-set for* $C_p(G_n)$*.*

Proof. (a) We first show that columns of G_n indexed by edges in $\mathcal{I}_n$ are linearly independent over $\mathbb{F}_2$. Permute rows and columns of G_n as follows. Order rows of the matrix according to the following ordering of vertices of the graph.

$$(1,1), \cdots, (n,1), (2,0), \cdots, (n,0), (1,0).$$

First list columns indexed by edges between $(1,1)$ and vertices in the set

$$\{(a,1) : a \neq 1\} \cup \{(b,0) : b \neq 1\}.$$

These are followed by the column indexed by $[(2,1),(1,0)]$. The remaining columns are written in any order. In this way, the first $2n-1$ columns take the form

$$\left[\begin{array}{c|c} 111\cdots111 & \\ I_{2n-2} & u \\ 000\cdots000 & \end{array}\right]$$

where I_{2n-2} is the identity matrix of rank $2n-2$ and $u = 0100\cdots1$. Excluding the first row from consideration, columns indexed by points in $\mathcal{I}_n$ are seen to be linearly independent over $\mathbb{F}_2$. Hence $\mathcal{I}_n$ is an information set for the binary codes.

Over $\mathbb{F}_p$, p an odd prime, adding a column indexed by $[(2,1),(n,0)]$ to $\mathcal{I}_n$ gives a linearly independent set.

(b) Let $\mathcal{C}$ be the check set for $C_2(G_n)$. Then $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$ where

$$\mathcal{C}_1 = \{[(c,1),(d,1)] : c, d \neq 1\}$$

and

$$\mathcal{C}_2 = \{[(e,0),(f,1)] : e, f \in \Omega, f \neq 1\} \setminus \{[(2,1),(1,0)]\}.$$

Since the code has minimum distance $n-1$, it corrects up to $t \leq \left\lfloor \frac{n-2}{2} \right\rfloor$ errors. Suppose a codeword c is sent and a vector $y = c + e$ is received such that the error vector e has weight at most $n-1$. Let $\mathcal{E}$ be the set of error positions in y, i.e., the non-zero coordinates of e. There are two possible cases.

Case (i). $\mathcal{E} \subseteq \mathcal{C}$

Use the identity (1) of S_n to fix the errors in the check set $\mathcal{C}$.

Case (ii). $\mathcal{E} \subseteq \mathcal{I}_n \cup \mathcal{C}$

Suppose there are i errors in A_1, j errors in A_2, k errors in $\mathcal{C}_1$ and l errors in $\mathcal{C}_2 \cup A_3$ where $i + j + |A_3| \neq 0$, i.e., there is at least one error in the information positions. Let

$$\begin{aligned}\mathcal{E} = \{\, & [(1,1),(a_1,1)], \cdots, [(1,1),(a_i,1)], [(1,1),(b_1,0)], \cdots, [(1,1),(b_j,0)], \\ & [(c_1,1),(d_1,1)], \cdots, [(c_k,1),(d_k,1)], [(e_1,0),(f_1,1)], \cdots, [(e_l,0),(f_l,1)] \,\}.\end{aligned}$$

Let

$$\mathcal{T} = \{a_1, \cdots, a_i, b_1, \cdots, b_j, c_1, \cdots, c_k, d_1, \cdots, d_k, e_1, \cdots, e_l, f_1, \cdots, f_l\}.$$

Then

$$|\mathcal{T}| \leq i + j + 2k + 2l.$$

Since

$$i + j + k + l = t \leq \left\lfloor \frac{n-2}{2} \right\rfloor,$$

we have

$$2i + 2j + 2k + 2l \leq n - 2.$$

Hence $|\mathcal{T}| \leq n-2$. Since $\mathcal{T} \subseteq \Omega \setminus \{1\}$, there exists $x \in \Omega \setminus \{1\}$ such that $x \notin \mathcal{T}$. Use a transposition of the form $(1,x)$ to map the errors into $\mathcal{C}$ and fix the errors already in $\mathcal{C}$.

If p is odd and $x = n$ then $(1,n)$ maps $[(2,1),(1,0)]$ to $[(2,1),(n,0)]$, an information position. Use an automorphism of the form $(1,2,n)$ to map $[(2,1),(1,0)]$ to $[(n,1),(2,0)]$, a check position. It is sufficient to consider this case because at this point we have $n \notin \mathcal{T}$ and $[(2,1),(1,0)]$ is the only error coordinate that is mapped to an information position by $(1,n)$. □

We remark that the Gordon bound for PD-sets of $C_p(G_n)$ is $n/2$ if n is even and $(n-1)/2$ if n is odd. Hence the PD-set exhibited in Proposition 5.9 above is roughly twice the Gordon bound.

5.3 The graphs $\overline{\Gamma}_n$ and their codes

As has been alluded to, the complements $\overline{\Gamma}_n$ of embeddings Γ_n of $L^1(K_n)\boxtimes K_2$, the strong product of triangular graphs and K_2, have been considered in [48] where they are defined as follows.

Definition 5.10. For $n \geq 3$, let $\Omega = \{1, \cdots, n\}$ and let $X = \Omega^{\{2\}} \times \Omega^{\{1\}}$. Let $\overline{\Gamma}_n$ be the complement of the graph Γ_n of Definition 4.1. Then $\overline{\Gamma}_n$ is defined by

$$\begin{aligned} V(\overline{\Gamma}_n) =& \{(A,B) \in X : B \subset A\}; \\ [(A,B),(A',B')] \in E(\overline{\Gamma}_n) \Longleftrightarrow& |A \cap A'| = 1 \text{ and } B \neq B' \text{ or };\\ & A \cap A' = \emptyset. \end{aligned}$$

Hence $\overline{\Gamma}_n$ is (n^2-2n)-regular. By Proposition 4.8,if $n \geq 4$ then $\mathrm{Aut}(\overline{\Gamma}_n) \cong S_n$. If $n = 3$ then $\overline{\Gamma}_3$ is the 3-prism, the complement of the 6-cycle. The 3-prism is also defined as the line graph of the complete bipartite graph $K_{2,3}$; and also as the cartesian product $C_3 \square K_2$. It has automorphism group the dihedral group D_6. We illustrate the graph in Figure 5.2.

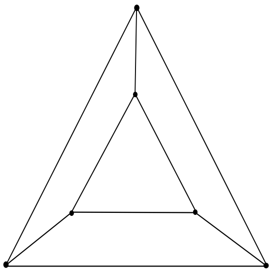

Figure 5.2: The 3-prism

We make the following observation.

Lemma 5.11. *Let $\overline{\Gamma}_n$ be the complement of the graph Γ_n of* Definition 4.1 *where $n \geq 3$. Then $\overline{\Gamma}_n$ is a subgraph of $(L^1(K_n) \times K_n) \cup (\overline{L^1(K_n)} \times K_n)$ where*

$\times$ *is the categorical product of graphs and* $\overline{L^1(K_n)}$ *is the complement of the triangular graph* $L^1(K_n)$*.*

Proof. Let $\Gamma'_n = (L^1(K_n) \times K_n) \cup (\overline{L^1(K_n)} \times K_n)$. We need to show that $V(\overline{\Gamma}_n) \subseteq V(\Gamma'_n)$ and that $E(\overline{\Gamma}_n) \subseteq E(\Gamma'_n)$.

By Definition 5.10, it is clear that there is a one-to-one correspondence between $V(\overline{\Gamma}_n)$ and the following subset of $V(\Gamma'_n)$.

$$\{([a,b],c) : [a,b] \in V(L^1(K_n)) \text{ and } c = a, b\}.$$

Hence $V(\overline{\Gamma}_n) \subseteq V(\Gamma'_n)$.

Let $[(A,B),(A',B')] \in E(\overline{\Gamma}_n)$. By Definition 5.10, either $|A \cap A'| = 1$ and $B \neq B'$ or $A \cap A' = \emptyset$. The first adjacency condition implies that each edge of $\overline{\Gamma}_n$ corresponds to an edge of $L^1(K_n) \times K_n$. The second adjacency condition implies that $[(A,B),(A',B')] \in E(\overline{L^1(K_n)} \times K_n)$. Hence $E(\overline{\Gamma}_n) \subseteq E(\Gamma'_n)$, completing the proof. □

5.3.1 Incidence matrices of $\overline{\Gamma}_n$

Let $\overline{\Gamma}_n$ be the graph of Definition 5.10 and let $\Omega = \{1, \cdots, n\}$ where $n \geq 3$. We now describe how incidence matrices of the graphs will be written.

Let

$$V_1 = \{(\{a,b\},\{a\}) : a, b \in \{1,2,3\}\}.$$

For $4 \leq i \leq n$, let

$$V_{i-2} = \{(\{a,i\},\{a\}), (\{a,i\},\{i\}) : a, i \in \Omega \text{ and } a < i\}.$$

Let M_n be an incidence matrix of $\overline{\Gamma}_n$. Write M_n as follows. Order rows of M_n so that, for given values of a and i, an incidence vector of the form $v^{\overline{(\{a,i\},\{i\})}}$ is preceded by an incidence vector of the form $v^{\overline{(\{a,i\},\{a\})}}$. Columns of the matrix are ordered beginning with those indexed by edges between vertices in $\bigcup_{i=1}^{n-3} V_i$. These are followed by columns indexed by edges between vertices in $\bigcup_{i=1}^{n-3} V_i$ and V_{n-2} and, lastly, columns indexed by edges between vertices in V_{n-2}. The resulting $2\binom{n}{2} \times (n^2 - 2n)\binom{n}{2}$ incidence matrix has the form

$$M_n = \left[\begin{array}{c|c|c} M_{n-1} & N & \mathbf{0} \\ \hline \mathbf{0} & P & G_{n-1} \end{array}\right] \tag{5.2}$$

where

(a) M_{n-1} is an incidence matrix of $\overline{\Gamma}_{n-1}$;

(b) N is a $2\binom{n-1}{2} \times 2(2n-3)\binom{n-1}{2}$ matrix such that each row has $2n-3$ consecutive entries 1 and no pair of row vectors is commonly incident;

(c) P is a $2(n-1) \times 2(2n-3)\binom{n-1}{2}$ matrix such that each column is a unit vector. Rows of P indexed by vertices of the form $(\{a,n\},\{n\})$ have weight $2\binom{n-1}{2}$ and those indexed by vertices of the form $(\{a,n\},\{a\})$ have weight $(n-2)^2$;

(d) G_{n-1} is an incidence matrix of the complement of the complete porcupine $\overline{H}_{n-1}$. Hence $\overline{H}_{n-1}$ is an induced subgraph of $\overline{\Gamma}_n$. For $a < n$, rows of G_{n-1} indexed by vertices of the form $(\{a,n\},\{n\})$ have weight $n-2$ and those indexed by vertices of the form $(\{a,n\},\{a\})$ have weight $2(n-2)$.

5.3.2 Codes from incidence matrices of the graphs $\overline{\Gamma}_n$

We now consider codes from incidence matrices M_n of $\overline{\Gamma}_n$. Unlike in the general case of M_n, order rows of M_3 as follows.

$$v^{\overline{(\{1,2\},\{1\})}}, v^{\overline{(\{1,3\},\{3\})}}, v^{\overline{(\{2,3\},\{2\})}}, v^{\overline{(\{2,3\},\{3\})}}, v^{\overline{(\{1,2\},\{2\})}}, v^{\overline{(\{1,3\},\{1\})}}.$$

Columns of M_3 are ordered according to the following ordering of edges of $\overline{\Gamma}_3$.

$$\begin{gathered}[(\{1,2\},\{1\}),(\{1,3\},\{3\})],[(\{1,2\},\{1\}),(\{2,3\},\{2\})],\\ [(\{1,3\},\{3\}),(\{2,3\},\{2\})],[(\{2,3\},\{3\}),(\{1,2\},\{2\})],\\ [(\{2,3\},\{3\}),(\{1,3\},\{1\})],[(\{1,2\},\{2\}),(\{1,3\},\{1\})].\end{gathered}$$

In this way, M_3 takes the form

$$\left[\begin{array}{c|c|c} L_3 & I_3 & \mathbf{0} \\ \hline \mathbf{0} & I_3 & L_3 \end{array}\right] \tag{5.3}$$

where L_3 is an incidence matrix of K_3 written as in Equation (3.1). I_3 is the rank-3 identity matrix. The following result is easily seen to hold.

Lemma 5.12. *Let* M_3 *be an incidence matrix of the* 3*-prism as presented in* Equation (5.3)*. Let* $C_p(M_3)$ *be the* p*-ary linear code from the row span of* M_3*. Then* $C_p(M_3)$ *is reversible.*

Parameters of $C_p(M_3)$ are obtained in the following lemma.

Lemma 5.13. *For any prime* p*, let* $C_p(M_3)$ *be the* p*-ary linear code from the row span of* M_3*, an incidence matrix of* $\overline{\Gamma}_3$*, the* 3*-prism.*

(a) $C_2(M_3) = [9,5,3]_2$ *and its minimum words are rows of* M_3*.*

(b) *If* p *is odd then* $C_p(M_3) = [9,6,2]_p$ *and its minimum words are scalar multiples of the following codewords.*

$$\begin{aligned}
&\left(v^{\overline{(12,1)}} + v^{\overline{(13,3)}} - v^{\overline{(23,2)}}\right) - \left(v^{\overline{(23,3)}} + v^{\overline{(12,2)}} - v^{\overline{(13,1)}}\right),\\
&\left(v^{\overline{(12,1)}} + v^{\overline{(23,2)}} - v^{\overline{(13,3)}}\right) - \left(v^{\overline{(23,3)}} + v^{\overline{(13,1)}} - v^{\overline{(12,2)}}\right),\\
&\left(v^{\overline{(13,3)}} + v^{\overline{(23,2)}} - v^{\overline{(12,1)}}\right) - \left(v^{\overline{(12,2)}} + v^{\overline{(13,1)}} - v^{\overline{(23,3)}}\right).
\end{aligned} \tag{5.4}$$

Proof. The 3-prism is connected. Since it has triangles, it is non-bipartite. Dimensions of the binary and non-binary codes of their incidence matrices are therefore obtained by Lemmas 2.22 and 2.23, respectively.

Let $c \in C_p(M_3)$. Then c is a concatenation of three vectors, c_1, c_2 and c_3, from the three column blocks of M_3 where $c_i \in \mathbb{F}_p^3$. Let R_1 and R_2 be the row blocks $[L_3|I_3|\mathbf{0}]$ and $[\mathbf{0}|I_3|L_3]$, respectively.

(a) Recall from the remark preceding Section 3.3.1 that $C_2(L_3) = [3,2,2]_2$ and its minimum words are rows of L_3. Let $c \in C_2(M_3)$. If c is a sum of rows of R_1 then $\text{wt}(c_1) \geq 2$ since $c_1 \in C_2(L_3)$. We also have $\text{wt}(c_2) \geq 1$. Hence $\text{wt}(c) \geq 3$ with equality if c is a row of R_1. A similar result is obtained if c is a sum of rows of R_2.

If c is a sum of rows of R_1 and R_2 then $\text{wt}(c_1) \geq 2$ and $\text{wt}(c_3) \geq 2$. Hence $\text{wt}(c) > 3$. This completes the proof for the binary codes.

(b) Suppose c is a linear combination of rows of R_1. Then $\text{wt}(c_1) \geq 1$ because $C_p(M_3) = [3,3,1]_p$ if p is odd. We also have $\text{wt}(c_2) \geq 1$. Minimum words of $C_p(L_3)$ are the difference between the sum of any two rows and the third row of L_3. Hence if $\text{wt}(c_1) = 1$ then $\text{wt}(c_2) = 3$, i.e., $\text{wt}(c) > 2$. If fewer than three rows of R_1 are added then $\mathrm{wt}(c_1) \geq 2$ and $\mathrm{wt}(c_2) \geq 1$. Again, $\mathrm{wt}(c) > 2$. A similar observation is made if c is a linear combination of rows of R_2.

Suppose c is a linear combination of rows of R_1 and R_2. Then $\mathrm{wt}(c_1) \geq 1$ and $\mathrm{wt}(c_3) \geq 1$. If $\mathrm{wt}(c_1) = 1 = \mathrm{wt}(c_3)$, it is possible to have $\mathrm{wt}(c_2) = 0$ if c is a scalar multiple of one of the vectors in Equation (5.4). Hence $\mathrm{wt}(c) \geq 2$. Since the code is small, an exhaustive search shows that scalar multiples of codewords in Equation (5.4) are the only minimum words. This completes the proof for $n = 3$. □

For any prime p and $n \geq 3$, the codes $C_p(M_3)$ are the only ones in the family $C_p(M_n)$ having different minimum weights depending on the parity of p. It will be shown in Lemma 5.15 and Proposition 5.16 that, in general, these codes have minimum weight $n(n-2)$. Meanwhile, we need to establish minimum weights of codes from the row span of $Q_n = \left[\frac{N}{P}\right]$ where matrices N and P are as in Equation (5.2). The result is used in the proof of Lemma 5.15 and Proposition 5.16. Q_n has the following general form.

$$Q_n = \left[\begin{array}{c|c|c|c} 1\cdots1 & & & \\ & 1\cdots1 & & \\ & & \cdots & \\ & & & 1\cdots1 \\ \hline P_1 & P_2 & \cdots & P_k \end{array}\right] \tag{5.5}$$

where $k = (n-1)(n-2)$ and each submatrix P_i is $2(n-1) \times (2n-3)$ having exactly $2n-3$ weight-1 rows and one zero vector. No pair of unit row vectors of P_i is commonly incident.

Lemma 5.14. *Let p be a prime. For $n \geq 4$, let $C_p(Q_n)$ be the p-ary code from the row span of Q_n, the matrix given in* Equation (5.5). *Then $C_p(Q_4)$ has minimum weight* 4 *with minimum words the weight-*4 *rows of P. If $n \geq 5$ then $C_p(Q_n)$ has minimum weight $2n-3$ with minimum words the rows of N.*

Proof. We only prove the case of $n \geq 5$. If $n = 4$, a similar proof shows that $C_p(Q_4)$ has minimum weight $(n-2)^2 = 4$ with minimum words the weight-4 rows of P.

Let $c \in C_p(Q_n)$. Then c is a concatenation of vectors c_i from the $(n-1)(n-2)$ column blocks of Q_n where $c_i \in \mathbb{F}_p^{(2n-3)}$. Let N and P be as in the discussion following Equation (5.2). By Equation (5.5), $P = [P_1|P_2|\cdots|P_k]$ where $k = (n-1)(n-2)$.

If c is a linear combination of n_1 rows of N then $\text{wt}(c) = (2n-3)n_1$ since no pair of rows of the matrix is commonly incident. Hence minimum words are rows of N.

Suppose c is a linear combination of rows of P. Let n_2 be the number of weight-$(n-2)^2$ rows of P and let n_3 be the number of weight-$(n-1)(n-2)$ rows of the matrix. Because no pair of rows of P is commonly incident, $\text{wt}(c) = (n-2)^2 n_2 + (n-1)(n-2)n_3 > 2n-3$ provided $n \geq 5$.

Suppose c is a linear combination of at least one row of N and one row of P. Since the submatrices P_i have unit row vectors, $\text{wt}(c_i) \geq 1$ for $1 \leq i \leq (n-1)(n-2)$. Hence $\text{wt}(c) \geq (n-1)(n-2) > 2n-3$.. This completes the proof of the lemma. □

We now determine parameters of $C_p(M_4)$ in Lemma 5.15. In the proof, we use an observation that if p is odd then $C_p(M_3)$, the code of Lemma 5.13, has other weight-3 codewords in addition to rows of M_3. For instance, the following is also a weight-3 codeword of $C_p(M_3)$.

$$\left(v^{\overline{(12,1)}} + v^{\overline{(13,3)}} - v^{\overline{(23,2)}}\right) + \left(v^{\overline{(23,3)}} - v^{\overline{(12,2)}} + v^{\overline{(13,1)}}\right). \qquad (5.6)$$

Lemma 5.15. *For any prime p, let $C_p(M_4)$ be the p-ary linear code from the row span of M_4, an incidence matrix of the graph $\overline{\Gamma}_4$ of* Definition 5.10.

(a) *If p is odd then $C_p(M_4) = [48, 12, 8]_p$ and its minimum words are the scalar multiples of the rows of M_4.*

(b) *$C_2(M_4) = [48, 11, 8]_2$ and its minimum words are rows of M_4.*

Proof. Again, we only prove the minimum weight.

Let $c \in C_p(M_4)$ where p is any prime. Then c is a concatenation of three vectors, c_1, c_2 and c_3, from the three column blocks of M_4 where $c_1 \in \mathbb{F}_p^9$, $c_2 \in \mathbb{F}_p^{30}$ and $c_3 \in \mathbb{F}_p^9$. Let R_1 be the row block $[M_3|N|\mathbf{0}]$ and R_2 the block $[\mathbf{0}|P|G_3]$.

(a) Suppose c is a linear combination of r_1 rows of R_1. By Lemma 5.13, $\mathrm{wt}(\mathrm{c}_1) \geq 2$. We also have $\mathrm{wt}(c_2) = 5r_1$. However, this does not imply that it is possible to obtain $\mathrm{wt}(c) = 7$. By Lemma 5.13, $\mathrm{wt}(c_1) = 2$ only if c_1 is a scalar multiple of any of the codewords in Equation (5.4). Because no two rows of N are commonly incident, this gives $\mathrm{wt}(c_2) = 30 > 8$.

Now, $\mathrm{wt}(c) = 8$ if c is a row of R_1. To see this, note that if $\mathrm{wt}(c_1) = 3$ and c_1 is not a row of M_3 then it is a linear combination of $r_1 > 1$ rows of the matrix as in Equation (5.6). Since no two rows of N are commonly incident, this gives $\mathrm{wt}(c_2) = 5r_1 > 8$.

Suppose c is a linear combination of rows of R_2. Let r be the number of weight-4 rows indexed by vertices of the form $(\{4, a\}, \{a\})$ and s the number of rows indexed by vertices of the form $(\{4, a\}, \{4\})$ where $a < 4$. Because no pair of rows of P is commonly incident, we have $\mathrm{wt}(\mathrm{c}) = 4r + 6s + \mathrm{wt}(c_3)$. We need to examine possibilities for r and s.

If r and s are both non-zero then the result is easily seen to hold. Suppose $r = 0$ and $s \neq 0$. Then no two rows of G_3 have a non-zero entry in the same coordinate position. Hence $\mathrm{wt}(c_3) = 2s$. This gives $\mathrm{wt}(c) = 8s \geq 8$ with equality if c is a row corresponding to a vertex of the form $(\{4, a\}, \{4\})$. If $r \neq 0$ and $s = 0$ then $\mathrm{wt}(c) = 4r + \mathrm{wt}(c_3)$. In this case, rows of G_3 are commonly incident in exactly $\binom{r}{2}$ coordinate positions. Hence $\mathrm{wt}(\mathrm{c}) \geq 8r - 2\binom{r}{2} \geq 8$ since $1 \leq r \leq 3$. If $r = 1$ then $2\binom{r}{2} = 0$ so that $\mathrm{wt}(\mathrm{c}) = 8$ if c is a row of R_2 corresponding to a vertex of the form $(\{4, a\}, \{a\})$.

Suppose c is a linear combination of r_1 rows of R_1 and r_2 rows of R_2. Then $\mathrm{wt}(c_1) \geq 2$ by Lemma 5.13. By Proposition 5.7, $\mathrm{wt}(c_3) \geq 2$. From the proof of the case of $n = 4$ in Lemma 5.14, one obtains $\mathrm{wt}(c_2) > 4$ if c_2 is a linear combination of rows from the two row blocks of the matrix. Hence $\mathrm{wt}(c) > 8$.

(b) We now turn to the binary codes $C_2(M_4)$. In addition to cases considered in (a) above, we need to examine values of $\mathrm{wt}(c)$ if c is a sum of all rows of R_1 or R_2. These cases give $c_1 = \mathbf{0}$ and $c_3 = \mathbf{0}$, respectively.

Suppose c is a sum of all rows of R_1 and $r_2 < 6$ rows of R_2. By Lemma 5.14, $\mathrm{wt}(c_2) \geq 4$. By Proposition 5.3, $\mathrm{wt}(c_3) \geq 2$. If $r_2 = 1$ then either $\mathrm{wt}(c_2) = 4$ or $\mathrm{wt}(c_2) = 6$. If $\mathrm{wt}(c_2) = 4$ then $\mathrm{wt}(c_3) = 4$, i.e., c is a row of P corresponding a vertex $(\{a, 4\}, \{a\})$, $a < 4$. If $\mathrm{wt}(c_2) = 6$ then $\mathrm{wt}(c_3) = 2$, i.e., c is a row of P corresponding to $(\{a,4\},\{4\})$. If at least two rows are added then $\mathrm{wt}(c_2) \geq 10 > 8$.

Suppose c is a sum of all rows of R_2 and r_1 rows of R_1. Then $\mathrm{wt}(c_1) \geq 3$ by Lemma 5.13. Since no two rows of R_1 are commonly incident, $\mathrm{wt}(c_1) = 5r_1$. Thus $\mathrm{wt}(c) = 3 + 5r_1 \geq 8$ with equality if c is a row of R_1. This completes the proof for $n = 4$. □

For $n \geq 5$, parameters of $C_p(M_n)$ are now determined in Proposition 5.16. The proof of minimum weights of the codes is by induction with base the case of $n = 4$ considered in Lemma 5.15.

Proposition 5.16. *For any prime p and $n \geq 4$, let $C_p(M_n)$ be the p-ary code from the row span of M_n, an incidence matrix of the graph $\overline{\Gamma}_n$ of* Definition 5.10*.*

(a) *If p is odd then $C_p(M_n) = \left[(n^2-2n)\binom{n}{2}, 2\binom{n}{2}, n(n-2)\right]_p$ and its minimum words are the scalar multiples of the rows of M_n.*

(b) *$C_2(M_n) = \left[(n^2-2n)\binom{n}{2}, 2\binom{n}{2}-1, n(n-2)\right]_2$ and its minimum words are the rows of M_n.*

Proof. Since the graphs are connected and, having triangles, are non-bipartite, dimensions of the codes follow from Lemmas 2.22 and 2.23. We therefore only need to prove the minimum weight of the codes.

Write M_n as in Equation (5.2). Let R_1 and R_2 be the row blocks $[M_{n-1}|N|\mathbf{0}]$ and $[\mathbf{0}|P|G_{n-1}]$, respectively. For any prime p, let $c \in C_p(M_n)$. Then c is a concatenation of three vectors, c_1, c_2 and c_3, from the three column blocks of M_n where $c_i \in \mathbb{F}_p^{k_i}$, $k_1 = (n-1)(n-3)\binom{n-1}{2}$, $k_2 = 2(2n-3)\binom{n-1}{2}$ and $k_3 = 3\binom{n-1}{2}$.

We prove the assertion about the minimum weight by induction. For $n \geq 5$ we assume that $C_p(M_{n-1})$ has minimum weight $(n-1)(n-3)$ and that minimum words are scalar multiples of the rows of M_{n-1}. The induction base is the content of Lemma 5.15.

Case (a). Minimum weight of $C_p(M_n)$, p an odd prime.

Suppose c is a sum of r_1 rows of R_1. Then $\mathrm{wt}(\mathrm{c}_1) \geq (n-1)(n-3)$. Since $\mathrm{wt}(\mathrm{c}_2) = (2n-3)r_1$, we have $\mathrm{wt}(c) \geq n(n-2)$ with equality if c is a row of R_1.

Suppose c is a sum of rows of R_2. Let r and s be the number of rows corresponding to vertices of the form $(\{a,n\},\{a\})$ and $(\{a,n\},\{n\})$, respectively, where $a < n$. If r and s are both non-zero then, because no two rows of P are commonly incident, $\mathrm{wt}(\mathrm{c}_2) = (n-2)^2 r + 2\binom{n-1}{2}s \geq (2n-3)(n-2) > n(n-2)$ provided $n \geq 4$.

Suppose $r \neq 0$ and $s = 0$. Note that rows of G_{n-1} indexed by vertices of the form $(\{a,n\},\{a\})$ can be written in the form $[L_{n-1}|K]$ where L_{n-1} is an incidence matrix of the complete graph K_{n-1} and K is a matrix such that each column is a unit vector and each row has weight $n-2$. By Theorem 2.35, we have $\mathrm{wt}(c_3) \geq (n-2) + (n-2)r \geq 2(n-2)$. Hence $\mathrm{wt}(c) \geq (n-2)^2 r + (n-2)r + (n-2) = ((n-1)r+1)(n-2) \geq n(n-2)$. Equality holds if c is a row of R_2.

If $r = 0$ and $s \neq 0$ then $\mathrm{wt}(c_2) = 2\binom{n-1}{2}s$. Since no two row vectors of G_{n-1} indexed by vertices of the form $(\{a,n\},\{n\})$ are commonly incident, $\mathrm{wt}(c_3) = (n-2)s$. Hence $\mathrm{wt}(c) = n(n-2)s$. Again, $\mathrm{wt}(c) = n(n-2)$ if c is a row of R_2.

Suppose c is a sum of r_1 rows of R_1 and r_2 rows of R_2 where $r_i \neq 0$. By the induction hypothesis, $\mathrm{wt}(c_1) \geq (n-1)(n-3)$. By Lemma 5.14, $\mathrm{wt}(c_2) \geq 2n-3$ and, by Proposition 5.7, $\mathrm{wt}(c_3) \geq n-2$. Hence $\mathrm{wt}(c) \geq n^2 - n - 2 > n(n-2)$.

It is possible to have $c_2 = \mathbf{0}$ if c is the difference of a scalar multiple of the sum of all rows of R_1 and that of all rows of R_2. In this case, $\mathrm{wt}(c_1) = (n-1)(n-3)\binom{n-1}{2} > n(n-2)$. This proves the minimum weights of the non-binary codes.

Case (b). Minimum weight of $C_2(M_n)$.

For the binary codes, in addition to cases considered above, we also need to check cases when all rows of R_1 or R_2 are added as these give, respectively, $c_1 = \mathbf{0}$ or $c_3 = \mathbf{0}$.

Suppose c is a sum of all rows of R_1 and r_2 rows of R_2. Let r and s be as in (a) above.

If r and s are both non-zero then $\mathrm{wt}(c_2) = 2(2n-3)\binom{n-1}{2} - 2\binom{n-1}{2}s - (n-2)^2r$ where $r+s < 2(n-1)$. By Proposition 5.7, $\mathrm{wt}(c_3) \geq n-2$.

If $r = 0$ and $s \neq 0$ then $\mathrm{wt}(c_2) = 2(2n-3)\binom{n-1}{2} - 2\binom{n-1}{2}s$ and $\mathrm{wt}(c_3) = (n-2)s$ where $s \leq n-1$. Hence in the worst case, $\mathrm{wt}(c_2) = (2n-3)(n-1)(n-2) - (n-1)^2(n-2) = (n-1)(n-2)^2 > n(n-2)$ provided $n \geq 4$.

If $r \neq 0$ and $s = 0$ then $\mathrm{wt}(c_2) = 2(2n-3)\binom{n-1}{2} - (n-2)^2r$. From the proof of (a) above, $\mathrm{wt}(c_3) \geq (n-2) + (n-2)r$ where $r \leq n-1$. In the worst case, $\mathrm{wt}(c_2) = 2(2n-3)\binom{n-1}{2} - (n-2)^2(n-1) = (n-1)^2(n-2) > n(n-2)$ provided $n \geq 4$.

Suppose c is a sum of all rows of R_2 and $r_1 < (n-1)(n-2)$ rows of R_1. By the induction hypothesis, $\mathrm{wt}(c_1) \geq (n-1)(n-3)$. By Lemma 5.14, $\mathrm{wt}(c_2) \geq 2n-3$. Hence $\mathrm{wt}(c) \geq n(n-2)$ with equality if c is a row of R_1. This completes the proof for all $n \geq 5$. □

5.3.3 Automorphisms of the codes

We now determine permutation automorphism groups of p-ary codes $C_p(M_n)$ from the row span of M_n, an incidence matrix of the graphs $\overline{\Gamma}_n$ of Definition 5.10 where p is any prime and $n \geq 4$.

Proposition 5.17. *Let $C_p(M_n)$ be the p-ary code from the row span of M_n, an incidence matrix of $\overline{\Gamma}_n$, the graphs of* Definition 5.10 *where $n \geq 4$ and p is any prime. Let $\mathcal{D}$ be the incidence design of $\overline{\Gamma}_n$. Then* $\mathrm{Aut}(C_p(M_n)) \cong \mathrm{Aut}(\mathcal{D}) \cong S_n$.

Proof. As in Propositions 3.7, 4.16 and 5.3, we only need to show that $\mathrm{Aut}(C_p(M_n)) \subseteq \mathrm{Aut}(\mathcal{D})$. Let $\sigma \in \mathrm{Aut}(C_p(M_n))$. By definition, σ preserves minimum words of the code. By Proposition 5.16, minimum words of $C_p(M_n)$ are scalar multiples of the incidence vectors of blocks of $\mathcal{D}$. Hence there exist incidence vectors $v^{\overline{(\{a,b\},\{a\})}}$ and $v^{\overline{(\{a',b'\},\{a'\})}}$ such that $\sigma(v^{\overline{(\{a,b\},\{a\})}}) = v^{\overline{(\{a',b'\},\{a'\})}}$. Since σ acts on coordinate positions, it induces a permutation $\bar{\sigma}$ such that $\bar{\sigma}(q_1) = q_2$ and $\bar{\sigma}(\overline{(\{a,b\},\{a\})}) = \bar{\sigma}(\overline{(\{a',b'\},\{a'\})})$ where $q_1 \in \overline{(\{a,b\},\{a\})}$ and $q_2 \in \overline{(\{a',b'\},\{a'\})}$. Hence $\bar{\sigma} \in \mathrm{Aut}(\mathcal{D})$. □

5.3.4 Partial permutation decoding for binary codes

We now consider partial permutation decoding for the binary codes $C_2(M_n)$ where $n \geq 4$. An information set for the codes is given in Proposition 5.18. In the proposition, we also exhibit an $\lfloor\frac{n^2-5n+6}{4}\rfloor$-PD-set for the codes.

Proposition 5.18. *Let* $A_1 = \{[(\{1,2\},\{1\}),u] : u \in N((\{1,2\},\{1\}))\}$ *and* $A_2 = \{[(\{1,2\},\{2\}),(\{1,x\},\{1\})] : 3 \leq x \leq n\}$ *where* $n \geq 4$*. Let* $C_2(M_n)$ *be the binary code from the row span of* M_n*, an incidence matrix of the graphs* $\overline{\Gamma}_n$ *of* Definition 5.10*. Then*

(a) $\mathcal{I}_n = A_1 \cup A_2 \cup \{[(\{1,2\},\{2\}),(\{1,3\},\{3\})]\}$ *is an information set for* $C_2(M_n)$*;*

(b) *The set*

$$S = \{(1),(1,x)(2,y) : x,y \neq 1,2\}$$

of $\binom{n-2}{2}+1$ *elements of* S_n *is an* $\left\lfloor\frac{n^2-5n+6}{4}\right\rfloor$*-PD-set for* $C_2(M_n)$ *with* $\mathcal{I}_n$ *as information set.*

Proof. (a) We first show that $\mathcal{I}_n$ is an information set. We do this by permuting rows and columns of M_n as follows. Write the row indexed by $(\{1,2\},\{1\})$ followed by rows indexed by its neighbours. Then write the row indexed by $(\{1,2\},\{2\})$ followed by the remaining $n-2$ vertices of the form $(\{1,x\},\{1\})$ where $3 \leq x \leq n$. Write columns of the matrix so that the first $n(n-2)$ are indexed by the edges of the form $[(\{1,2\},\{1\}),u]$ where $u \in N((\{1,2\},\{1\}))$, the neighbourhood of $(\{1,2\},\{1\})$. These are followed by columns indexed by the edges $[(\{1,2\},\{2\}),(\{1,3\},\{3\})]$ and $[(\{1,2\},\{2\}),(\{1,x\},\{1\})]$ where $3 \leq x \leq n$. The remaining columns are written in any order. In this way, the first $2\binom{n}{2}-1$ columns of the incidence matrix take the form

$$\left[\begin{array}{c|c|c} 1\cdots1 & 0 & 0\cdots0\\ \cline{1-1} & 1 & 0\cdots0\\ \cline{3-3} I_{(n^2-2n)} & & \mathbf{0}\\ \cline{3-3} & 1 & 1\cdots1\\ \cline{1-1} \mathbf{0} & & I_{n-2} \end{array}\right]$$

where I_k is the identity matrix of dimension k. Excluding the first row from consideration, columns of the remaining upper triangular matrix are seen to be linearly independent over $\mathbb{F}_2$.

(b) Suppose a codeword $c \in C_2(M_n)$ is sent and a vector $y = c + e$ is received such the error vector e has weight at most $t = \left\lfloor \frac{n^2-5n+6}{4} \right\rfloor$. Let $\mathcal{C}$ be the check set of the code and $\mathcal{E}$ the set of error coordinates. We need to show that for any such e, there exists an automorphism $\alpha \in S$ such that $\alpha(\mathcal{E}) \subseteq \mathcal{C}$.

First observe the following. Let $\overline{\Omega}^{\{2\}}$ be the set of subsets of size two of $\Omega \setminus \{1,2\}$. Consider the set

$$A = \left(\overline{\Omega}^{\{2\}} \setminus \{\{a,b\}\}\right) \cup \{\{1,2\}\}$$

for some fixed $\{a,b\} \in \overline{\Omega}^{\{2\}}$. Since coordinate positions of $C_2(M_n)$ correspond to edges of $\overline{\Gamma}_n$ and $|A| = \binom{n-2}{2}$, at most $\frac{1}{2}\binom{n-2}{2}$ coordinate positions are obtained using each element of A exactly once as an edge-endpoint.

There are two main cases to consider for $\mathcal{E}$.

Case (i). $\mathcal{E} \subseteq \mathcal{C}$.

Use the identity (1) to fix the errors in the check set $\mathcal{C}$.

Case (ii). $\mathcal{E} \subseteq \mathcal{I}_n \cup \mathcal{C}$.

From the preceding remarks, there exists a subset $\{a,b\} \in \overline{\Omega}^{\{2\}}$ such that $\{1,2\} \cap \{a,b\} = \emptyset$ and both $(\{a,b\},\{a\})$ and $(\{a,b\},\{b\})$ are not endpoints of any edge in $\mathcal{E}$.

Let $\alpha = (1,a)(2,b)$. Consider errors in information positions of the form $[(\{1,2\},\{1\}),u]$ where $u \in N((\{1,2\},\{1\}))$. These are mapped by α to coordinate positions of the form $[(\{a,b\},\{a\}),u']$ where $u' = \alpha(u) \in N((\{a,b\},\{a\}))$. Since $u \neq (\{a,b\},\{a\})$, we have $\alpha(u) \neq (\{1,2\},\{1\})$. Also, $\alpha(u) \neq (\{1,2\},\{2\})$ because $u \neq (\{a,b\},\{b\})$. Hence $[(\{a,b\},\{a\}),u'] \in \mathcal{C}$. A similar observation is made if errors occur in information positions of the form $[(\{1,2\},\{2\}),(\{2,3\},\{3\})]$ and $[(\{1,2\},\{2\}),(\{1,x\},\{1\})]$ where $3 \leq x \leq n$.

It is not possible for errors in $\mathcal{C}$ to be mapped into $\mathcal{I}_n$ because $\alpha = (1,a)(2,b)$ is chosen such that there are no errors in any coordinate position corresponding to an edge with either $(\{a,b\},\{a\})$ or $(\{a,b\},\{b\})$ as endpoint. $\square$

From computations using Magma [7], the Gordon bound for the size of an $\left\lfloor \frac{n^2-5n+6}{4} \right\rfloor$-PD-set of $C_2(M_n)$ appears to be $\left\lceil \dfrac{n^2-5n+8}{4} \right\rceil$; roughly, half the size of S.

5.3.5 Partial permutation decoding for the non-binary codes

In this section we use Lemma 2.33 to show that S_n is an $\left(\left\lceil \frac{n-2}{2} \right\rceil - 1\right)$-PD-set for non-binary codes from incidence matrices of $\overline{\Gamma}_n$. We first make some observations regarding neighbours of a given vertex $(\{a,b\},\{a\})$ of $\overline{\Gamma}_n$. In this way, it is possible to determine forms of edges of the graph and hence coordinate positions of the codes.

Let $[(\{a,b\},\{a\}),(\{c,d\},\{c\})]$ be a coordinate position of $C_p(M_n)$. Then:

1. By the first adjacency condition in Definition 5.10, either $a = d$ or $b = c$ or $b = d$. Hence $(\{c,d\},\{c\})$ is equal to either $(\{a,c\},\{c\})$ or $(\{b,d\},\{b\})$ or $(\{b,c\},\{c\})$. There are $n-2$ possibilities for each of these vertices. The graph therefore has $(n-2)\binom{n}{2}$ edges of each of the forms $[(\{a,b\},\{a\}),(\{a,c\},\{c\})]$, $[(\{a,b\},\{a\}),(\{b,d\},\{b\})]$ and $[(\{a,b\},\{a\}),(\{b,c\},\{c\})]$;

2. By the second adjacency condition in Definition 5.10, $\{a,b\}\cap\{c,d\} = \emptyset$. Since there are $2\binom{n-2}{2}$ vertices $(\{c,d\},\{c\})$ such that $c,d \neq a,b$ for a given vertex $(\{a,b\},\{a\})$, the code has $2\binom{n-2}{2}\binom{n}{2}$ coordinate positions of this form.

Consider the sets

$$\begin{aligned}
O_1 &= \{[(\{a,b\},\{a\}),(\{a,c\},\{c\})] : a,b,c \in \Omega\}\,,\\
O_2 &= \{[(\{a,b\},\{a\}),(\{b,d\},\{b\})] : a,b,d \in \Omega\}\,,\\
O_3 &= \{[(\{a,b\},\{a\}),(\{b,c\},\{c\})] : a,b,c \in \Omega\}\,,\\
O_4 &= \{[(\{a,b\},\{a\}),(\{c,d\},\{c\})] : a,b,c,d \in \Omega\}\,.
\end{aligned} \tag{5.7}$$

From the discussion above, it is clear that $\bigcup_{i=1}^{4} O_i = \mathcal{P} = E(\overline{\Gamma}_n)$.

Lemma 5.19. *S_n has three orbits in its induced action on $\mathcal{P}$.*

Proof. Let $\alpha \in S_n$. Define a map $\alpha : \mathcal{P} \to \mathcal{P}$ by

$$\begin{aligned}\alpha([(\{a,b\},\{a\}),&(\{c,d\},\{c\})]) = \\ &[(\{\alpha(a),\alpha(b)\},\{\alpha(a)\}),\{(\alpha(c),\alpha(d)\},\{\alpha(c)\})].\end{aligned}$$

Let O_i be as in Equations (5.7). Let $p_1 = [(\{a,b\},\{a\}),(\{a,c\},\{c\})] \in O_1$ and let $p_2 = [(\{a,b\},\{a\}),(\{b,d\},\{b\})] \in O_2$. If $\alpha = (c,a,b,d)$ then $\alpha(p_1) = p_2$. Hence for every coordinate position $p_1 \in O_1$ there exists an automorphism α in S_n such that $\alpha(p_1) \in O_2$. Thus points in $O_1 \cup O_2$ are in one orbit under the action of S_n.

Notice that each coordinate position in O_3 is identified by three distinct elements of Ω and each such element belongs to exactly two sets. Coordinate positions in O_3 are the only ones with this property. Because α is bijective, $\alpha(p_3) \in O_3$ for each $p_3 \in O_3$. Since points in O_4 are the only ones identified by four distinct elements of Ω, $\alpha(p_4) \in O_4$ whenever $p_4 \in O_4$. Hence $\mathcal{P}$ has three orbits under the action of S_n. These are $\mathcal{O}_1 = O_1 \cup O_2$, $\mathcal{O}_2 = O_3$ and $\mathcal{O}_3 = O_4$. $\square$

In the proposition below, the ratios $\frac{|\mathcal{O}_i \cap \mathcal{I}_n|}{|\mathcal{O}_i|}$, $i = 1,2,3$, are calculated. Lemma 2.33 is then used to determine the number of errors correctable by permutation decoding with PD-set S_n.

Proposition 5.20. *For $n \geq 5$ and p an odd prime, let $C_p(M_n)$ be the p-ary code from the row span of M_n, an incidence matrix of the graphs $\overline{\Gamma}_n$ of* Definition 5.10*. Then S_n is an $\left(\lceil\frac{n-2}{2}\rceil - 1\right)$-PD-set for $C_p(M_n)$.*

Proof. Let $\mathcal{O}_i$ be the orbits of $\mathcal{P}$ under the action of $\mathrm{Aut}(C_p(M_n)) = S_n$ obtained in Lemma 5.19. Let $\mathcal{I}_n$ be an information set for the codes. In the worst case, $\mathcal{O}_i \cap \mathcal{I}_n = \mathcal{I}_n$. Hence

$$\begin{aligned} n_1 &= \frac{|\mathcal{O}_1 \cap \mathcal{I}_n|}{\mathcal{O}_1} = \frac{1}{n-2}, \\ n_2 &= \frac{|\mathcal{O}_2 \cap \mathcal{I}_n|}{\mathcal{O}_2} = \frac{2}{n-2}, \\ n_3 &= \frac{|\mathcal{O}_1 \cap \mathcal{I}_n|}{\mathcal{O}_1} = \frac{1}{\binom{n-2}{2}}. \end{aligned}$$

Let $N = \max(n_1, n_2, n_3)$. Then $N = n_2$. By Lemma 2.33, S_n is an s-PD-set for $C_p(M_n)$ where

$$\begin{aligned} s &= \min\left(\left\lceil \frac{1}{N} \right\rceil - 1, \left\lfloor \frac{n(n-2)-1}{2} \right\rfloor\right) \\ &= \min\left(\left\lceil \frac{n-2}{2} \right\rceil - 1, \left\lfloor \frac{n(n-2)-1}{2} \right\rfloor\right) \\ &= \left\lceil \frac{n-2}{2} \right\rceil - 1. \end{aligned}$$

□

Chapter 6

Codes from incidence matrices of line graphs of triangular graphs

6.1 Introduction

We now use results obtained in Chapter 3 and Chapter 4 to describe linear codes from the row span of incidence matrices of line graphs of triangular graphs $L^2(K_n)$ where $n \geq 4$. The triangular graphs and the embeddings Γ_n of $L^1(K_n) \boxtimes K_2$, the strong product of triangular graphs and K_2, are both induced subgraphs of $L^2(K_n)$. We determine parameters of both binary and non-binary codes of incidence matrices of $L^2(K_n)$. We show that the codes have permutation automorphism group S_n. We also exhibit $\lfloor \frac{n-3}{3} \rfloor$-PD-sets in S_n for partial permutation decoding of the codes. If S_n is used as a PD-set with the given information set, the codes are shown to correct up to $\lceil \frac{n}{2} \rceil - 1$ errors by permutation decoding.

As intimated, the vertex-set of $L^2(K_n)$ is the edge set of the triangular graph. Because every vertex $\{\{a,b\},\{b,c\}\}$ is also a path of length one in the triangular graph, it will be denoted (ab, bc). Since edges of $L^2(K_n)$ are paths of length two in the triangular graph, an edge $\{\{\{a,b\},\{b,c\}\},\{\{b,c\},\{c,d\}\}\}$ will be denoted (ab, bc, cd). By definition, this is also the form of coordinate positions of the corresponding code. Notice that $bc = \{b, c\}$ in (ab, bc, cd) is the common endpoint of vertices (ab, bc) and (bc, cd).

Our main results are summarised in Theorem 6.1 below.

Theorem 6.1. *For any prime p and $n \geq 4$, let $C_p(M_n)$ be the p-ary linear code from the row span of an incidence matrix M_n of $L^2(K_n)$, the line graph of the triangular graph $L^1(K_n)$. Let*

$$\begin{aligned}
A_1 &= \{(b_1c_1, a_1b_1, b_1n) : a_1, b_1, c_1 \in \Omega \setminus \{n\}, a_1 < c_1\}\,,\\
A_2 &= \{(a_2b_2, a_2n, b_2n) : a_2, b_2 \in \Omega \setminus \{n\}, a_2 < b_2\}\,,\\
A_3 &= \{(b_3n, a_3n, (n-1)n) : a_3, b_3 \in \Omega \setminus \{n-1, n\}, a_3 < b_3\}\,,\\
A_4 &= \{((n-2)n, (n-1)n, a_4n) : a_4 \leq n-3\}\,.
\end{aligned}$$

(a) *If p is odd then $C_p(M_n) = \left[(2n-5)(n-2)\binom{n}{2}, (n-2)\binom{n}{2}, 4n-10\right]_p$ and its minimum words are the scalar multiples of the rows of M_n.*

(b) *$C_2(M_n) = \left[(2n-5)(n-2)\binom{n}{2}, (n-2)\binom{n}{2} - 1, 4n-10\right]_2$ and its minimum words are the rows of M_n.*

(c) *If $n \geq 5$ then $\mathrm{Aut}(C_p(M_n)) \cong S_n$.*

(d) *The set $S = \{(n, x) : x \in \Omega\}$ of n elements of S_n is an $\left\lfloor \frac{n-3}{3} \right\rfloor$-PD-set for the binary code $C_2(M_n)$ with information set $\mathcal{I}_n = \bigcup_{i=1}^{4} A_i$.*

If p is odd then S is also an $\left\lfloor \frac{n-3}{3} \right\rfloor$-PD-set for the non-binary codes $C_p(M_n)$ with information set $\mathcal{I}_n \cup \{(1n, 2n, 3n)\}$.

(e) *With $\mathcal{I}_n$ and $\mathcal{I}_n \cup \{(1n, 2n, 3n)\}$ as information sets for $p = 2$ and p an odd prime, respectively, and S_n as PD-set, $C_p(M_n)$ corrects up to $\left\lceil \dfrac{n}{2} \right\rceil - 1$ errors by permutation decoding.*

The theorem is proved in the various sections below using a series of lemmas and propositions. In Section 6.2 we describe how we write incidence matrices M_n of $L^2(K_n)$. We also describe incidence vectors of the incidence design of the graph and the neighbourhood design of its line graph. Codes from incidence matrices of the graphs are considered in Section 6.4. In Section 6.4.3 we determine parameters of binary codes from adjacency matrices of $L^3(K_n)$ using results obtained in Section 6.4. Partial permutation decoding for the codes is considered in Section 6.5.

6.2 Incidence matrices of $L^2(K_n)$ and related codes

In this section we first describe how incidence matrices M_n of the graphs $L^2(K_n)$ will be written. Let

$$X_n = \{(ab, an) : a, b \in \Omega \setminus \{n\}\} \tag{6.1}$$

and let

$$Y_n = \{(an, bn) : a, b \in \Omega \setminus \{n\}\}. \tag{6.2}$$

Order vertices of $L^2(K_n)$ using the ordering of edges of the triangular graph $L^1(K_n)$ obtained in Chapter 3. Thus the $(n-3)\binom{n-1}{2}$ vertices of $L^2(K_{n-1})$ are listed first followed by the $2\binom{n-1}{2}$ vertices in X_n and, lastly, the $\binom{n-1}{2}$ vertices in Y_n. In each case, vertices are ordered lexicographically (see Example (6.2)). Additional columns of M_n are indexed by edges between vertices in $V(L^2(K_{n-1}))$ and X_n. These are followed by columns indexed by edges between vertices in X_n, then edges between vertices in X_n and Y_n and, lastly, edges between vertices in Y_n. The resulting $(n-2)\binom{n}{2} \times (2n-5)(n-2)\binom{n}{2}$ incidence matrix M_n takes the form

$$\left[\begin{array}{c|c|c|c|c} M_{n-1} & N_1 & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & P_1 & Q_n & N_2 & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} & \mathbf{0} & P_2 & T_{n-1} \end{array}\right] \tag{6.3}$$

where

(a) M_{n-1} is an incidence matrix of $L^2(K_{n-1})$;

(b) N_1 is an $(n-3)\binom{n-1}{2} \times 4(n-3)\binom{n-1}{2}$ matrix. Each row has four consecutive entries equal to 1 since every vertex (ab, ac) of $L^2(K_{n-1})$ is incident with the four edges of the form (ab, ac, an), (ab, ac, cn), (ac, ab, an) and (ac, ab, bn);

(c) P_1 is a $2\binom{n-1}{2} \times 4(n-3)\binom{n-1}{2}$ matrix in which every column is a unit vector. Each row has weight $2n-6$ since every vertex (ab, an) in X_n indexing rows of P_1 is incident with edges of the form (an, ab, ax) and (an, ab, by) where $x, y \neq a, b, n$;

(d) Q_n is a $2\binom{n-1}{2} \times (n-2)\binom{n-1}{2}$ incidence matrix of the induced subgraph $L^2(K_n)[X_n]$, an $(n-2)$-regular graph that is isomorphic to an embedding of the strong product $L^1(K_{n-1}) \boxtimes K_2$ (see Definition 4.1 and Lemma 6.3) considered in Chapter 4;

(e) N_2 is a $2\binom{n-1}{2} \times 2(n-2)\binom{n-1}{2}$ matrix. Each row has weight $n-2$ since every vertex (ab, an) corresponding to a row of N_2 is incident with edges of the form (ab, an, xn) where $x \neq a, n$. The $n-2$ non-zero entries in each row are consecutive;

(f) P_2 is an $\binom{n-1}{2} \times 2(n-2)\binom{n-1}{2}$ matrix with the property that every row vector has weight $2n-4$ and every column is a unit vector;

(g) T_{n-1} is an incidence matrix of the triangular graph $L^1(K_{n-1})$.

In the example below we give an ordering of vertices of $L^2(K_4)$ and write its incidence matrix M_4 as per the discussion above.

Example 6.2. Rows of M_4, an incidence matrix of the graph $L^2(K_4)$, are ordered according to the following ordering of vertices of the graph. $(12, 13)$, $(12, 23)$, $(13, 23)$, $(12, 14)$, $(12, 24)$, $(13, 14)$, $(13, 34)$, $(23, 24)$, $(23, 34)$, $(14, 24)$, $(14, 34)$ and $(24, 34)$. Therefore

$$M_4 = \left[\begin{array}{c|c|c|c|c}
110 & 111100000000 & 000000 & 000000000000 & 000 \\
101 & 000011110000 & 000000 & 000000000000 & 000 \\
011 & 000000001111 & 000000 & 000000000000 & 000 \\
\hline
000 & 100010000000 & 110000 & 110000000000 & 000 \\
000 & 010001000000 & 101000 & 001100000000 & 000 \\
000 & 001000001000 & 010100 & 000011000000 & 000 \\
000 & 000100000100 & 000110 & 000000110000 & 000 \\
000 & 000000100010 & 001001 & 000000001100 & 000 \\
000 & 000000010001 & 000011 & 000000000011 & 000 \\
\hline
000 & 000000000000 & 000000 & 101010001000 & 110 \\
000 & 000000000000 & 000000 & 010001100010 & 101 \\
000 & 000000000000 & 000000 & 000100010101 & 011
\end{array}\right]. \tag{6.4}$$

We denote the incidence design of $L^2(K_n)$ by $\mathcal{D}_n$. For any prime p, the p-ary linear code from the row span of M_n is denoted $C_p(M_n)$. Let $\overline{(ab,bc)}$ be the block of $\mathcal{D}_n$ comprising edges incident with vertex (ab,bc). Then

$$\begin{aligned}\overline{(ab,bc)} =&\{(ab,bc,bw),(ab,bc,cx) : w \neq a,b,c \text{ and } x \neq b,c\}\\ &\cup \{(bc,ab,by),(bc,ab,az) : y \neq a,b,c \text{ and } z \neq a,b\}.\end{aligned}$$

Hence

$$v^{\overline{(ab,bc)}} = \sum_{w\neq a,b,c} v^{(ab,bc,bw)} + \sum_{x\neq b,c} v^{(ab,bc,cx)} + \sum_{y\neq a,b,c} v^{(bc,ab,by)} + \sum_{z\neq a,b} v^{(bc,ab,az)}$$

is the weight-$(4n-10)$ incidence vector of the block $\overline{(ab,bc)}$. We also have

$$C_p(M_n) = \left\langle v^{\overline{(ab,bc)}} : (ab,bc) \in V(L^2(K_n))\right\rangle.$$

Let A_n be an adjacency matrix of $L^3(K_n)$. As alluded to, we also consider the binary code $C_2(A_n)$ from the row span of A_n. Recall from Corollary 2.26 that $C_2(A_n) = E_2(M_n)$ where $E_2(M_n)$ is the binary code from the span of differences of rows of M_n. Hence

$$C_2(A_n) = \left\langle v^{\overline{u}} + v^{\overline{w}} : u,w \text{ adjacent vertices of } L^2(K_n)\right\rangle. \tag{6.5}$$

6.3 The graphs Γ_{n-1} and $L^2(K_n)[X_n]$ are isomorphic

Let Γ_n be an embedding of the strong product $L^1(K_n) \boxtimes K_2$ as given in Definition 4.1 where $n \geq 4$. We now show that Γ_{n-1} is isomorphic to the induced subgraph $L^2(K_n)[X_n]$ where X_n is the set given in Equation (6.1). This allows us to use Theorem 4.2 to determine parameters of the p-ary codes $C_p(Q_n)$ from the row span of Q_n in proofs of Lemma 6.4 and Proposition 6.5.

Lemma 6.3. *Let $\Omega = \{1,\cdots,n\}$ and $X_n = \{(ab,an) : a,b \in \Omega \setminus \{n\}\}$ where $n \geq 4$. Let Γ_{n-1} be an embedding of $L^1(K_{n-1}) \boxtimes K_2$ presented in* Definition 4.1. *Let $L^2(K_n)[X_n]$ be the induced subgraph of $L^2(K_n)$ with vertex set X_n. Then Γ_{n-1} and $L^2(K_n)[X_n]$ are isomorphic.*

Proof. By Definition 4.1, $V(\Gamma_{n-1}) = \{(\{a,b\},\{a\}) : a,b \in \Omega \setminus \{n\}\}$. Define a map $\phi : V(\Gamma_{n-1}) \to X_n$ by $\phi((\{a,b\},\{a\})) = (ab, an)$. Since ϕ is clearly injective and $|V(\Gamma_{n-1})| = |X_n|$, ϕ is bijective. Because $e \in E(\Gamma_{n-1})$ if and only if $\phi(e) \in E(L^2(K_n)[X_n])$, ϕ also preserves adjacency in the graphs. Hence Γ_{n-1} and $L^2(K_n)[X_n]$ are isomorphic. □

6.4 The code $C_p(M_n)$ from an incidence matrix of $L^2(K_n)$

Let $C_p(M_n)$ be the p-ary code from the row span of M_n, an incidence matrix of the graph $L^2(K_n)$ where $n \geq 4$. Parameters of $C_p(M_4)$ are obtained in Lemma 6.4. This lemma is used as a base for the inductive proof in Proposition 6.5 on the minimum weight and words of the codes.

6.4.1 The code $C_p(M_4)$

We now determine the parameters of $C_p(M_4)$.

Lemma 6.4. *Let p be any prime and let $C_p(M_4)$ be the p-ary code from the row span of M_4, an incidence matrix of $L^2(K_4)$.*

(a) *If p is odd then $C_p(M_4) = [36, 12, 6]_p$ and minimum words are the scalar multiples of the rows of M_4.*

(b) *If $p = 2$ then $C_2(M_4) = [36, 11, 6]_2$ and minimum words are the rows of M_4.*

Proof. Since $L^2(K_4)$ is a line graph of a connected graph, it is also connected. As seen from its incidence matrix in Equation (6.4), $L^2(K_4)$ contains the triangle $L^1(K_3)$, an odd cycle. Hence by Proposition 2.3, $L^2(K_4)$ is non-bipartite. Dimensions of $C_p(M_4)$, for any p, hence follow from Lemmas 2.22 and 2.23.

Write M_4 as in Equation (6.4). Label the submatrix comprising the first three rows of M_4 by R_1, the next six rows by R_2 and the last three rows by R_3. Let $c \in C_p(M_4)$. Then c is a concatenation of five vectors from the five column blocks of M_4, i.e., $c = c_1c_2c_3c_4c_5$ where $c_1, c_5 \in \mathbb{F}_p^3$, $c_2, c_4 \in \mathbb{F}_p^{12}$ and $c_3 \in \mathbb{F}_p^6$. We show that $\mathrm{wt}(c) \geq 6$. The non-binary case is considered first.

(a) Suppose c is a linear combination of r_1 rows of R_1. Since $C_p(M_3) = [3, 3, 1]_p$ if p is odd, we have $\mathrm{wt}(c_1) \geq 1$. It is clear that $\mathrm{wt}(c_2) = 4r_1$. Now, $\mathrm{wt}(c_1) = 1$ only if the sum of any two rows of M_3 is subtracted from the third row. This possibility gives $\mathrm{wt}(\mathrm{c}_2) = 12 > 6$. Otherwise, $\mathrm{wt}(c_1) = 2$ or $\mathrm{wt}(c_1) = 3$. In either case, $\mathrm{wt}(c) \geq 6$. Equality occurs if c is a multiple of a row of R_1. Similarly, $\mathrm{wt}(c) \geq 6$ if c is a linear combination of rows of R_3.

Suppose c is a linear combination of r_2 rows of R_2. Since no two row vectors of R_2 are commonly incident at any coordinate position, $\mathrm{wt}(c_2) = \mathrm{wt}(c_4) = 2r_2$. By Lemma 4.14, $\mathrm{wt}(c_3) \geq 2$. Hence $\mathrm{wt}(c) \geq 4r_2 + 2 \geq 6$. Equality holds if c is a row of R_2. There are two further cases to consider.

Case (i).

By Lemma 4.14 and the remark following it, $C_p(Q_4)$ has other weight-2 codewords apart from rows of Q_4. By the remark following Lemma 4.14, these codewords are a linear combination of at least two rows of Q_4. However, this gives $\mathrm{wt}(c_2) \geq 4$ and $\mathrm{wt}(c_4) \geq 4$. Thus $\mathrm{wt}(c) > 6$.

Case (ii).

Since Q_4 is an incidence matrix of the 6-cycle, a bipartite graph, its rows are linearly dependent over $\mathbb{F}_p$. Any linear combination of rows of Q_4 giving the zero vector uses more than one row. Hence $\mathrm{wt}(c_2) = \mathrm{wt}(c_4) = 2r_2$. We get $\mathrm{wt}(c) \geq 4r_2 > 6$ since $r_2 \geq 2$.

Next, suppose c is a linear combination of r_1 rows of R_1 and r_2 rows of R_2. Then $\mathrm{wt}(c_1) \geq 1$ and, by Lemma 4.14, $\mathrm{wt}(c_3) \geq 2$. We also have $\mathrm{wt}(c_4) = 2r_2$. If $\mathrm{wt}(c_4) = 2$ then c_2 is non-zero, in fact, $\mathrm{wt}(c_2) > 2$. Hence $\mathrm{wt}(c) > 6$.

Since $\left[\frac{N_1}{P_1}\right]$ is an incidence matrix of a bipartite graph, it is possible to have $c_2 = \mathbf{0}$ if the sum of all rows of N_1 is subtracted from that of all rows of P_1. This implies that $\mathrm{wt}(c_4) = 12 > 6$.

If c is a linear combination of r_1 rows of R_1 and r_3 rows of R_3 then $\mathrm{wt}(c_2) = 4r_1$ and $\mathrm{wt}(c_4) = 4r_3$. Hence $\mathrm{wt}(c) > 6$.

If c is a linear combination of rows of R_2 and R_3 then $\mathrm{wt}(c_2) \geq 2$, $\mathrm{wt}(c_3) \geq 2$ (by Lemma 4.14) and $\mathrm{wt}(c_5) \geq 1$. We need to examine possibilities for c_4. It is possible to have $c_4 = \mathbf{0}$ if the sum of all rows of N_2 is subtracted from that of all rows of P_2. This however gives $\mathrm{wt}(c_2) = 12 > 6$. If $c_4 \neq \mathbf{0}$ then $\mathrm{wt}(c) \geq 6$. It is however not possible to have $\mathrm{wt}(c) = 6$ because if $\mathrm{wt}(c_5) = 1$ then c_5 is obtained from the difference between the sum of any two rows of P_2 and the third row, a case which clearly gives $\mathrm{wt}(c_4) \geq 2$ and $\mathrm{wt}(c) > 6$. If $\mathrm{wt}(c_5) \geq 2$ then we have $\mathrm{wt}(c) > 6$.

Suppose c is a linear combination of r_1, r_2 and r_3 rows of R_1, R_2 and R_3, respectively. Then $\mathrm{wt}(c_1) \geq 1$, $\mathrm{wt}(c_5) \geq 1$ and, by Lemma 4.14, $\mathrm{wt}(c_3) \geq 2$. $\mathrm{wt}(c_1) = 1$ if a scalar multiple of the sum of any two rows of R_1 is subtracted from that of the third row. This gives $\mathrm{wt}(c_2) \geq 2$. Similarly, if $\mathrm{wt}(c_5) = 1$ then $\mathrm{wt}(c_4) \geq 2$. Hence $\mathrm{wt}(c) > 6$.

Since $\left[\frac{N_i}{P_i}\right]$ are incidence matrices of bipartite graphs, it is possible to have $c_2 = c_4 = \mathbf{0}$ if the sum of all rows of N_i is subtracted from that of all rows of P_i. In this case, $\mathrm{wt}(c_3) = 6$. Since c_1 and c_5 are both non-zero, we have $\mathrm{wt}(c) > 6$.

It is possible to have $c_3 = \mathbf{0}$ since Q_4 is an incidence matrix of the 6-cycle, a bipartite graph. This only happens if the sum of any three rows of Q_4 that are not pairwise commonly incident at any point is subtracted from the sum of the remaining three rows. As seen from the form of the matrices, this gives $\mathrm{wt}(c_2) > 2$ and $\mathrm{wt}(c_4) > 2$. Hence we also have $\mathrm{wt}(c) > 6$. This concludes the proof for the minimum weight of the non-binary codes $C_p(M_4)$.

(b) We now consider the minimum weight of the binary codes $C_2(M_4)$. Note that $C_2(M_3) = [3, 2, 2]_2$.

In addition to observations made above for non-binary codes, we show that $\mathrm{wt}(c) \geq 6$ if $\mathrm{wt}(c_i) \geq 2$ for $i = 1, 5$ or if all rows of R_1 or R_2 or R_3 are added since these give, respectively, $c_1 = 000$, $c_2 = 000000$ and $c_3 = 000$.

Suppose c is a sum of r_1 rows of R_1. Since $\mathrm{wt}(c_1) \geq 2$ and $\mathrm{wt}(c_2) = 4r_1$, we have $\mathrm{wt}(c) \geq 6$. It is clear that equality holds if c is a row of R_1. If all rows of R_1 are added then $\mathrm{wt}(c_2) = 12 > 6$. Similar observations are made if c is a sum of rows of R_3.

If c is a sum of all six rows of R_2 then $\mathrm{wt}(c_2) = 12 = \mathrm{wt}(c_4)$. Hence $\mathrm{wt}(c) > 6$.

Suppose c is a sum of rows of R_1 and R_2. If c is a sum of all rows of R_1 and $r_2 < 6$ rows of R_2 then, because $C_2([\frac{N_1}{P_1}])$ is even, $\mathrm{wt}(c_2) \geq 2$. By Lemma 4.14, $\mathrm{wt}(c_3) \geq 2$. We also have $\mathrm{wt}(c_4) \geq 2$. Now, $\mathrm{wt}(c_2) = 2$ if five rows of R_2 are added giving $\mathrm{wt}(c_4) = 10$. Otherwise, $\mathrm{wt}(c_2) > 2$. Hence $\mathrm{wt}(c) > 6$. If $r_1 < 3$ and all rows of R_2 are added then $\mathrm{wt}(c_4) = 12 > 6$.

Suppose c is a sum of rows of R_1 and R_3. If $r_1 = 3$ and $r_3 < 3$ then $\mathrm{wt}(c_2) = 12 > 6$. If all rows of R_3 are added and $r_1 < 3$ then $\mathrm{wt}(c_4) = 12 > 6$.

Suppose c is a sum of rows of R_2 and R_3. If all rows of R_2 are added and $r_3 < 3$ then $\mathrm{wt}(c_2) = 12 > 6$. If all rows of R_3 are added and $r_2 < 6$ then $\mathrm{wt}(c_2) \geq 2$ and, by Lemma 4.14, $\mathrm{wt}(c_3) \geq 2$. Since $\mathrm{wt}(c_4) \geq 2$, the result follows. It is possible to have $\mathrm{wt}(c) = 6$ if $r_2 = 5$, i.e., if c is a row of R_2.

Suppose c is a sum of r_1, r_2 and r_3 rows of R_1, R_2 and R_3, respectively. There are six cases.

Case (i). $r_1 = 3$, $r_2 < 6$ and $r_3 < 3$. Then $\mathrm{wt}(c_2) \geq 2$ and $\mathrm{wt}(c_5) \geq 2$. By Lemma 4.14, $\mathrm{wt}(c_3)$. Since any 8 rows of $\frac{N_2}{P_2}$ are independent, $C_4 \neq \mathbf{0}$. Hence $\mathrm{wt}(c) > 6$;

Case (ii). $r_1 < 3$, $r_2 = 6$ and $r_3 < 3$. Then $\mathrm{wt}(c_1) \geq 2$, $\mathrm{wt}(c_2) \geq 4$ and $\mathrm{wt}(c_5) \geq 2$. Hence $\mathrm{wt}(c) > 6$;

Case (iii). $r_1 < 3$, $r_2 < 6$ and $r_3 = 3$. Then $\mathrm{wt}(c_i) \geq 2$ for $i = 1, 2, 3, 4$. Hence $\mathrm{wt}(c) > 6$;

Case (iv). $r_1 = 3$, $r_2 = 6$ and $r_3 < 3$. Then $\mathrm{wt}(c_4) \geq 4$ and $\mathrm{wt}(c_5) \geq 2$. If $r_3 = 2$ then $\mathrm{wt}(c) = 6$ and c is the row of R_3 that is not added;

Case (v). $r_1 = 3$, $r_2 < 6$ and $r_3 = 3$. Then $\mathrm{wt}(c_i) \geq 2$ for $i = 2, 3, 4$. We can have $\mathrm{wt}(c) = 6$ if $r_2 = 5$. In this case, c is the row of R_2 that is not in the sum. Otherwise, $\mathrm{wt}(c_2) > 2$.

Case (vi). $r_1 < 3$, $r_2 = 6$ and $r_3 = 3$. Then $\mathrm{wt}(c_1) \geq 2$ and $\mathrm{wt}(c_2) \geq 4$. It is possible to have $\mathrm{wt}(c) = 6$ if $r_1 = 2$. In this case, c is the row of R_1 that is not added.

In all cases, we have $\mathrm{wt}(c) \geq 6$. This completes the proof for $n = 4$. □

6.4.2 The $C_p(M_n)$ where $n \geq 5$

We now consider the codes $C_p(M_n)$ for any prime p and $n \geq 5$. The minimum weight is established by induction using $C_p(M_4)$ as the base case.

Proposition 6.5. *Let $C_p(M_n)$ be the p-ary linear code from the row span of M_n where $n \geq 5$ and p is any prime.*

(a) *If p is odd then $C_p(M_n) = [(2n-5)(n-2)\binom{n}{2}, (n-2)\binom{n}{2}, 4n-10]_p$ and its minimum words are the scalar multiples of the rows of M_n.*

(b) *$C_2(M_n) = [(2n-5)(n-2)\binom{n}{2}, (n-2)\binom{n}{2} - 1, 4n-10]_2$ and its minimum words are the rows of M_n.*

Proof. As done elsewhere, we only need to prove the assertion about the minimum weight of the codes. We do this by induction using the case of $n = 4$ considered in Lemma 6.4 as the base. We assume that $C_p(M_{n-1})$ has minimum weight $4n-14$ and that its minimum words are the scalar multiples of the rows of M_{n-1}.

Write M_n as in Equation (6.3) and label it as follows. Let R_1 be the submatrix of M_n comprising the first $(n-3)\binom{n-1}{2}$ rows, R_2 the next $2\binom{n-1}{2}$ rows and R_3 the last $\binom{n-1}{2}$ rows. Thus $R_1 = [M_{n-1}|N_1|\mathbf{0}|\mathbf{0}|\mathbf{0}]$, $R_2 = [\mathbf{0}|P_1|Q_n|N_2|\mathbf{0}]$ and $R_3 = [\mathbf{0}|\mathbf{0}|\mathbf{0}|P_2|T_{n-1}]$. Let $c \in C_p(M_n)$. Then c is a concatenation of five vectors from the five column blocks of M_n, i.e., $c = c_1c_2c_3c_4c_5$ where $c_i \in \mathbb{F}_p^{k_i}$, $k_1 = (2n-7)(n-3)\binom{n-1}{2}$, $k_2 = 4(n-3)\binom{n-1}{2}$, $k_3 = (n-2)\binom{n-1}{2}$, $k_4 = 2(n-2)\binom{n-1}{2}$ and $k_5 = (n-3)\binom{n-1}{2}$.

(a) Suppose c is a linear combination of r_1 rows of R_1. By assumption, $\mathrm{wt}(c_1) \geq 4n-14$. It is also clear that $\mathrm{wt}(c_2) = 4r_1$. If c is a linear combination of r_2 rows of R_2 then, because no pair of rows of P_1 is commonly incident, $\mathrm{wt}(c_2) = (2n-6)r_2$. Similarly, $\mathrm{wt}(c_4) = (n-2)r_2$. By Proposition 4.15, $\mathrm{wt}(c_3) \geq n-2$. If c is a linear combination of r_3 rows of R_3 then, because no pair of rows of P_2 is commonly incident, $\mathrm{wt}(c_4) = (2n-4)r_2$. By Proposition 3.3, $\mathrm{wt}(c_5) \geq 2n-6$. In all cases, $\mathrm{wt}(c) \geq 4n-10$ with equality if $r_i = 1$, i.e., if c is a row of R_i.

Suppose c is a linear combination of rows of R_1 and R_2. Then $\mathrm{wt}(c_1) \geq 4n-14$ and $\mathrm{wt}(c_4) = (n-2)r_2$. Hence $\mathrm{wt}(c) > 4n-10$. It is possible to have $c_2 = \mathbf{0}$ if the sum of all rows of N_1 is subtracted from that of all rows of P_1. Since no pair of rows of N_2 is commonly incident, this gives $\mathrm{wt}(c_4) = (n-1)(n-2)^2 > 4n-10$ for $n \geq 4$.

If c is a linear combination of rows of R_1 and R_3 then $\mathrm{wt}(c_1) \geq 4n-14$ and, by Proposition 3.3, $\mathrm{wt}(c_5) \geq 2n-6$. Hence $\mathrm{wt}(c) > 4n-10$.

If c is a linear combination of rows of R_2 and R_3 then $\mathrm{wt}(c_2) = (2n-6)r_2$. By Proposition 4.15, $\mathrm{wt}(c_3) \geq n-2$ and, by Proposition 3.3, $\mathrm{wt}(c_5) \geq 2n-6$. Hence $\mathrm{wt}(c) > 4n-10$. Note that this also holds even if $c_4 = \mathbf{0}$.

If c is a linear combination of rows of R_1, R_2 and R_3 then, by the induction hypothesis, $\mathrm{wt}(c_1) \geq 4n-14$ and, by Proposition 3.3, $\mathrm{wt}(c_5) \geq 2n-6$. Hence $\mathrm{wt}(c) > 4n-10$. This completes the proof if p is odd.

(b) In addition to observations made above, if the code is binary then we also need to examine cases when all rows of R_1 or R_2 or R_3 are added as these give, respectively, $c_1 = \mathbf{0}$, $c_3 = \mathbf{0}$ and $c_5 = \mathbf{0}$.

Let $c \in C_2(M_n)$. If c is a sum of all rows of R_1 then $\mathrm{wt}(c) = \mathrm{wt}(c_2) = 4(n-3)\binom{n-1}{2} > 4n-10$. If c is a sum of all rows of R_2 then $\mathrm{wt}(c_2) = 2(2n-6)\binom{n-1}{2} > 4n-10$. If c is a sum of all rows of R_3 then $\mathrm{wt}(c) = \mathrm{wt}(c_4) = (2n-4)\binom{n-1}{2} > 4n-10$.

Suppose c is a sum of rows from any two row blocks of M_n. There are six possible cases.

Case (i). c is a sum of all rows of R_1 and $r_2 < 2\binom{n-1}{2}$ rows of R_2. Then $\mathrm{wt}(c_2) \geq 2n-6$, $\mathrm{wt}(c_3) \geq n-2$ and $\mathrm{wt}(c_4) \geq n-2$. It is possible to have $\mathrm{wt}(c) = 4n-10$ if $r_2 = 2\binom{n-1}{2} - 1$. In this case c is the row of R_2 that is not in the sum.

Case (ii). c is a sum of $r_1 < (n-3)\binom{n-1}{2}$ rows of R_1 and all rows of R_2. Then $\text{wt}(c_4) = 2(n-2)\binom{n-1}{2} > 4n-10$.

Case (iii). c is a sum of all rows of R_1 and $r_3 < \binom{n-1}{2}$ rows of R_3. Then $\text{wt}(c_2) = 4(n-3)\binom{n-1}{2} > 4n-10$.

Case (iv). c is a sum of $r_1 < (n-3)\binom{n-1}{2}$ rows of R_1 and all rows of R_3. Then $\text{wt}(c_4) = 2(n-2)\binom{n-1}{2} > 4n-10$.

Case (v). c is a sum of all rows of R_2 and $r_3 < \binom{n-1}{2}$ rows of R_3. Then $\text{wt}(c_2) = 4(n-3)\binom{n-1}{2} > 4n-10$.

Case (vi). c is a sum of $r_2 < 2\binom{n-1}{2}$ rows of R_2 and all rows of R_3. Since no pair of rows of P_1 is commonly incident, $\text{wt}(c_2) = (2n-6)r_2$. By Proposition 4.15, $\text{wt}(c_3) \geq n-2$. We also have $\text{wt}(c_4) \geq (n-2)$. Hence $\text{wt}(c) \geq 4n-10$. It is possible to have $\text{wt}(c) = 4n-10$ if $r_2 = 2\binom{n-1}{2} - 1$. In this case, c is the row of R_2 that is not in the sum.

Lastly, suppose c is a sum of r_1 rows of R_1, r_2 rows of R_2 and r_3 rows of R_3. There are six possible cases.

Case (i). c is a sum of all rows of R_1, $r_2 < 2\binom{n-1}{2}$ rows of R_2 and $r_3 < \binom{n-1}{2}$ rows of R_3. Then $\text{wt}(c_2) \geq 2n-6$ and, by Proposition 4.15, $\text{wt}(c_3) \geq n-2$. By Proposition 3.3, $\text{wt}(c_5) \geq 2n-6$. Hence $\text{wt}(c) > 4n-10$.

Case (ii). c is a sum of all rows of R_2, $r_1 < (n-3)\binom{n-1}{2}$ rows of R_1 and $r_3 < \binom{n-1}{2}$ rows of R_3. Then, by assumption, $\text{wt}(c_1) \geq 4n-14$ and, by Proposition 3.3, $\text{wt}(c_5) \geq 2n-6$. Hence $\text{wt}(c) > 4n-10$.

Case (iii). c is a sum of all rows of R_3, $r_1 < (n-3)\binom{n-1}{2}$ rows of R_1 and $r_2 < 2\binom{n-1}{2}$ rows of R_2. Then $\text{wt}(c_1) \geq 4n-14$ and, by Proposition 3.3, $\text{wt}(c_3) \geq n-2$. Hence $\text{wt}(c) > 4n-10$.

Case (iv). All rows of R_1 and R_2 are added and $r_3 < \binom{n-1}{2}$. Then $\mathrm{wt}(c_4) \geq 2n-4$ and, by Proposition 3.3, $\mathrm{wt}(c_5) \geq 2n-6$. Hence $\mathrm{wt}(c) \geq 4n-10$ with equality if $r_3 = \binom{n-1}{2} - 1$. In this case, c is the row of R_3 that is not in the sum.

Case (v). All rows of R_1 and R_3 are added and $r_2 < 2\binom{n-1}{2}$. Then $\mathrm{wt}(c_2) \geq 2n-6$ and $\mathrm{wt}(c_4) \geq n-2$. By Proposition 4.15, $\mathrm{wt}(c_3) \geq n-2$. Hence $\mathrm{wt}(c) \geq 4n-10$. Equality occurs if $r_2 = 2\binom{n-1}{2} - 1$. In this case, c is the row of R_2 that is not in the sum.

Case (vi). All rows of R_2 and R_3 are added and $r_1 < (n-3)\binom{n-1}{2}$. Then $\mathrm{wt}(c_1) \geq 4n-14$ and $\mathrm{wt}(c_2) \geq 4$. Hence $\mathrm{wt}(c) \geq 4n-10$ with equality if $r_1 = (n-3)\binom{n-1}{2} - 1$. Again equality occurs if c is the row of R_1 not in the sum.

□

6.4.3 Codes from adjacency matrices of $L^3(K_n)$

We now the result of Proposition 6.5 to determine parameters of binary codes generated by adjacency matrices A_n of the iterated line graphs $L^3(K_n)$.

Proposition 6.6. *Let A_n be an adjacency matrix of the iterated line graph $L^3(K_n)$ and let $C_2(A_n)$ be the binary code from the row span of A_n. If $n \equiv 0, 1, 2 \pmod 4$ then $C_2(A_n) = [(2n-5)(n-2)\binom{n}{2}, (n-2)\binom{n}{2} - 2, 8n-22]_2$ and its minimum words are the rows of A_n. If $n \equiv 3 \pmod 4$ then $C_2(A_n) = C_2(M_n)$.*

Proof. We first determine the dimension of $C_2(A_n)$.

Consider the binary code $E_2(M_n)$ generated by differences of rows of M_n, an incidence matrix of $L^2(K_n)$ (see Equation (6.3)). By Lemma 2.26, $E_2(M_n) = C_2(A_n)$ for all n. By Corollary 2.29, $E_2(M_n)$ has codimension 1 in $C_2(M_n)$ if and only if $\jmath \in C_2(M_n^T)$ where $\jmath$ is the all-one vector of length $(n-2)\binom{n}{2}$. Otherwise, $E_2(M_n) = C_2(M_n)$. We hence need to determine when $\jmath \in C_2(M_n^T)$.

Being a line graph of an edge transitive graph, $L^3(K_n)$ is vertex-transitive. Hence by Theorem 2.16, the graph is 0-covered if it is even. This is satisfied if $n \equiv 0, 1, 2 \pmod 4$. By Corollary 2.31, for these values of n, there exists a perfect matching, say M, in the graph. In the dual design with incidence matrix M_n^T, this implies that $\sum_{e_i \in M} v^{\overline{e}_i} = \jmath$ where $\overline{e}_i$ is the block comprising the two endpoints of edge e_i. Therefore $\jmath \in C_2(M_n^T)$ if $n \equiv 0, 1, 2 \pmod 4$.

$(n-2)\binom{n}{2}$ is odd if $n \equiv 3 \pmod 4$. Hence $\jmath \notin C_2(M_n^T)$ if $n \equiv 3 \pmod 4$ since the code is even. By Corollary 2.29, we therefore have $C_2(A_n) = C_2(M_n)$.

At this point, we need to determine the minimum weight of $C_2(A_n)$ if $n \equiv 0, 1, 2 \pmod 4$. Let $c \in C_2(A_n)$. Since $C_2(A_n) = E_2(M_n)$ by Corollary 2.26, we use Equation (6.5) to write

$$c = \sum_{(a_ib_i, b_ic_i) \in S} \left(v^{\overline{(a_ib_i, b_ic_i)}} + v^{\overline{(a_0b_0, b_0c_0)}} \right)$$

for some $S \subseteq V(L^2(K_n))$ and fixed incidence vector $v^{\overline{(a_0b_0, b_0c_0)}}$. This simplifies to

$$c = \sum_{1 \leq i \leq s} v^{\overline{(a_ib_i, b_ic_i)}} + s v^{\overline{(a_0b_0, b_0c_0)}}$$

where $s = |S|$. Hence c is a sum of s or $s+1$ incidence vectors of $\mathcal{D}_n$, the incidence design of $L^2(K_n)$, depending on whether s is even or odd. Without loss of generality, suppose s is odd. Then

$$c = \sum_{0 \leq i \leq s} v^{\overline{(a_ib_i, b_ic_i)}}.$$

Hence

$$\text{Supp}(c) = \left(\cdots \left(\left(\overline{(a_0b_0, b_0c_0)} \triangle \overline{(a_1b_1, b_1c_1)} \right) \triangle \overline{(a_2b_2, b_2c_2)} \right) \cdots \triangle \overline{(a_sb_s, b_sc_s)} \right)$$

where $\triangle$ is the symmetric difference of sets. In the worst case, the pairwise intersection of the blocks is non-empty, i.e., corresponding incidence vectors are pairwise commonly incident. Hence

$$|\text{Supp}(c)| \geq (4n-10)(s+1) - 2\binom{s+1}{2} \geq 8n - 22.$$

Note that $\text{wt}(c) = 8n - 22$ if $s = 1$ and the two vectors are commonly incident. Hence $C_2(A_n)$ has minimum words of the form

$$v^{\overline{(a_ib_i, b_ic_i)}} + v^{\overline{(b_ic_i, xd_i)}} = v^{\overline{(a_ib_i, b_ic_i, xd_i)}},$$

the rows of A_n, where $x = b_i, c_i$. □

6.5 Partial permutation decoding of $C_p(M_n)$

In this section, we show that S_n is the permutation automorphism group of the codes $C_p(M_n)$ for any prime p and $n \geq 5$. Using a specific information set, we determine $\lfloor (n-3)/3 \rfloor$-PD-sets for partial permutation decoding of the codes. With this information set and S_n as PD-set, we show using Lemma 2.33 that the codes correct up to $\lceil \frac{n}{2} \rceil - 1$ errors by permutation decoding.

Proposition 6.7. *For any prime p and $n \geq 5$, let $C_p(M_n)$ be the p-ary linear code from the row span of M_n, an incidence matrix of the line graph of the triangular graph $L^2(K_n)$. Let $\mathcal{D}_n$ be the incidence design of the graph. Then* $\mathrm{Aut}(C_p(M_n)) \cong \mathrm{Aut}(\mathcal{D}_n) = \mathrm{Aut}(L^2(K_n)) = S_n$.

Proof. That $\mathrm{Aut}(\mathcal{D}_n) = \mathrm{Aut}(L^2(K_n)) = S_n$ follows from Proposition 2.11 and Lemma 2.20. It remains to show that $\mathrm{Aut}(C_p(M_n)) \subseteq \mathrm{Aut}(\mathcal{D}_n)$.

Let u be a minimum word of the code. By Proposition 6.5, u is a scalar multiple of a row of M_n. Let $\rho \in \mathrm{Aut}(C_p(M_n))$. Then there exist minimum words $v^{\overline{(ab,bc)}}$ and $v^{\overline{(a'b',b'c')}}$ such that $\rho(v^{\overline{(ab,bc)}}) = v^{\overline{(a'b',b'c')}}$. Thus ρ induces a permutation $\overline{\rho}$ of blocks of $\mathcal{D}$ such that $\overline{\rho}(\overline{(ab,bc)}) = \overline{(a'b',b'c')}$. Hence $\mathrm{Aut}(C_p(M_n)) \subseteq \mathrm{Aut}(\mathcal{D})$. □

We now give an information set for the codes $C_p(M_n)$, p any prime.

Lemma 6.8. *For $n \geq 5$ and any prime p, let $C_p(M_n)$ be the p-ary code from the row span of M_n, an incidence matrix of the graph $L^2(K_n)$. Let*

$$\begin{aligned}
A_1 &= \{(b_1c_1, a_1b_1, b_1n) : a_1, b_1, c_1 \in \Omega \setminus \{n\}, a_1 < c_1\}\,,\\
A_2 &= \{(a_2b_2, a_2n, b_2n) : a_2, b_2 \in \Omega \setminus \{n\}\}\,,\\
A_3 &= \{(b_3n, a_3n, (n-1)n) : a_3, b_3 \in \Omega \setminus \{n-1, n\}, a_3 < b_3\}\,,\\
A_4 &= \{((n-2)n, (n-1)n, a_4n) : 1 \leq a_4 \leq n-3\}\,.
\end{aligned}$$

Then

(a) $\bigcup_{i=1}^{4} A_i$ *is an information set for* $C_2(M_n)$.

(b) *If p is odd then* $\bigcup_{i=1}^{4} A_i \cup \{(1n, 2n, 3n)\}$ *is an information set for* $C_p(M_n)$.

Proof. Write M_n as in Equation (6.3). By permuting rows and columns of M_n, we show that columns of the matrix indexed by points in $\bigcup_{i=1}^4 A_i$ are linearly independent over $\mathbb{F}_2$.

Consider the submatrix N_1 of M_n. It is possible to permute columns of N_1 such that the matrix takes the form $\left[I|N_1^{(3)}\right]$ where I is the identity matrix of rank $(n-3)\binom{n-1}{2}$ with columns indexed by points in A_1. $N_1^{(3)}$ has weight-3 row vectors such that no pair is commonly incident at any point. A similar observation is made for points in A_2. In this case, it is possible to write N_2 in the form $\left[I|N_2^{(n-3)}\right]$ where I is the rank-$2\binom{n-1}{2}$ identity matrix and $N_2^{(n-3)}$ is such that each row vector has weight $(n-3)$ and no pair of rows is commonly incident at any point.

Permute rows corresponding to vertices in Y_n so that they begin with $\binom{n-2}{2}$ rows indexed by vertices of the form (an, bn) where $a, b \neq n-1, n$. These are followed by rows indexed by $n-2$ vertices of the form $(an, (n-1)n)$ where $a < n-1$. With this ordering, T_{n-1} takes the form

$$\left[\begin{array}{c|c|c} T_{n-2} & A & \mathbf{0} \\ \hline \mathbf{0} & B & G_{n-2} \end{array}\right] \tag{6.6}$$

where:

(i) T_{n-2} is an incidence matrix of the triangular graph $L^1(K_{n-2})$;

(ii) A is an $\binom{n-2}{2} \times (n-3)(n-2)$ matrix such that each row has weight two and each column is a unit vector;

(iii) B is an $(n-2) \times (n-3)(n-2)$ matrix such that each row is a vector of weight $n-3$ and each column is a unit vector;

(iv) G_{n-2} is an incidence matrix of the complete graph K_{n-2}.

Permute columns of A so that the matrix takes the form $[I|I]$ where I is the rank $\binom{n-2}{2}$ identity matrix. Then one of the identity matrices is indexed by points in A_3.

Write G_{n-2} as follows. Order rows of G_{n-2} according to the following ordering of vertices of the form $(an, (n-1)n)$ where $n \geq n-2$.

$$(1n, (n-1)n), (2n, (n-1)n), \cdots, ((n-3)n, (n-1)n), ((n-2)n, (n-1)n).$$

Columns of G_{n-2} are ordered by first obtaining edges joining vertices of the form $(an,(n-1)n)$, $a \leq n-3$, and the vertex $((n-2)n,(n-1)n)$. These are followed by edges between the vertices $(an,(n-1)n)$ where $1 \leq a \leq n-3$. This is similar to the way incidence matrices of complete graphs are written in Equation (2.6). Hence G_{n-2} takes the form

$$\left[\begin{array}{c|c} I & G_{n-3} \\ \hline 1\cdots 1 & 0\cdots 0 \end{array}\right]$$

where G_{n-3} is an incidence matrix of K_{n-3}.

With these permutations of rows and columns of M_n, the matrix takes the form

$$\left[\begin{array}{c|c|c|c|c|c|c|c|c}
M_{n-1} & N_1^3 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & I & \mathbf{0} & \mathbf{0} \\ \hline
\mathbf{0} & P_{12} & Q_n & N_2^{(n-3)} & \mathbf{0} & \mathbf{0} & P_{11} & I & \mathbf{0} \\ \hline
\mathbf{0} & \mathbf{0} & \mathbf{0} & P_{22} & \begin{array}{c|c} T_{n-2} & I \\ \hline \mathbf{0} & B_2 \end{array} & \begin{array}{c} \mathbf{0} \\ \hline G_{n-3} \\ \hline 0\cdots 0 \end{array} & \mathbf{0} & P_{21} & \begin{array}{c|c} I & \mathbf{0} \\ \hline B_1 & \begin{array}{c} I \\ \hline 1\cdots 1 \end{array} \end{array}
\end{array}\right],$$

where the last three main column blocks are indexed by points in $\mathcal{I}_n$. Excluding the last row from consideration, it is clear that columns indexed by points in $\mathcal{I}_n$ are linearly independent over $\mathbb{F}_2$. Hence $\mathcal{I}_n$ is an information set for the binary codes.

If p is odd, adding the point $(1n, 2n, 3n)$ to $\mathcal{I}_n$ gives a set of linearly independent columns over $\mathbb{F}_p$. This completes the proof. □

Let $\mathcal{C}$ be the check set of the code. Then $\mathcal{C}$ is written as a union of the following sets.

(a) A_5, a set of $(2n-7)(n-3)\binom{n-1}{2}$ points corresponding to columns of M_{n-1}. $(n-4)(n-3)\binom{n-1}{2}$ of these points have the form (a_5c_5, a_5b_5, a_5x) while the remaining $(n-3)^2\binom{n-1}{2}$ have the form (a_5c_5, a_5b_5, b_5y) where $a_5, b_5, c_5, x, y \in \Omega \setminus \{n\}$, $x \neq a_5, b_5, c_5$ and $y \neq a_5, b_5$;

(b) A_6, a set of $2(n-3)\binom{n-1}{2}$ points of the form (b_6c_6, a_6b_6, a_6n) and $(n-3)\binom{n-1}{2}$ of the form (a_6b_6, b_6c_6, b_6n) where a_6, b_6, $c_6 \in \Omega \setminus \{n\}$. These points are indices of columns of $N_1^{(3)}$;

(c) A_7, a set of $2(n-3)\binom{n-1}{2}$ points of the form (a_7b_7, xn, yn) where $x = a_7, b_7$ and $y \neq a_7, b_7, n$. These points correspond to columns of $N_2^{(n-3)}$.

(d) A_8, a set of $(n-2)\binom{n-1}{2}$ points corresponding to columns of the submatrix Q_n. These have the form (a_8n, a_8b_8, b_8n) and (a_8b_8, a_8n, a_8c_8) where a_8, b_8, $c_8 \in \Omega \setminus \{n\}$ and $a_8 < b_8$;

(e) A_9, a set of points of the form (b_9n, a_9n, c_9n) corresponding to the $(n-4)\binom{n-2}{2}$ columns of T_{n-2} where a_9, b_9, $c_9 \in \Omega \setminus \{n-1, n\}$;

(f) A_{10}, a set of $\binom{n-2}{2}$ points of the form $(a_{10}n, b_{10}n, (n-1)n)$ where $a_{10} < b_{10}$. These points correspond to columns of matrix A in Equation (6.6) that are not used in the information set;

(g) A_{11}, a set of points corresponding to the $\binom{n-3}{2}$ columns of G_{n-3}. These have the form $(a_{11}n, (n-1)n, b_{11}n)$ where $a_{11} < b_{11} \leq n-3$.

In the proposition below, we exhibit PD-sets for partial permutation decoding of codes $C_p(M_n)$.

Proposition 6.9. *For any prime p, let $C_p(M_n)$ be the p-ary code from the row span of M_n, an incidence matrix of the graph $L^2(K_n)$. For $i = 1, \cdots, 11$, let A_i be as in* Lemma 6.8 *and the discussion above. Then*

$$S = \{(n, x) : 1 \leq x \leq n\}$$

is an $\lfloor \frac{n-3}{3} \rfloor$-PD-set for $C_2(M_n)$ of n elements of S_n with $\mathcal{I}_n = \bigcup_{i=1}^{n} A_i$ as information set. If p is odd then S is also a PD-set for $C_p(M_n)$ with information set $\mathcal{I}_n \cup \{(1n, 2n, 3n)\}$.

Proof. Suppose a codeword c is sent and a vector $y = c + e$ is received such that $\mathrm{wt}(e) \leq \lfloor \frac{n-3}{3} \rfloor$, i.e., at most $\lfloor \frac{n-3}{3} \rfloor$ errors occur. Let $\mathcal{E}$ be the set of error coordinates. From the discussion above, the binary code has check set $\mathcal{C} = \bigcup_{i=5}^{11} A_i$. We examine two main cases.

Case 1. $\mathcal{E} \subseteq \mathcal{I}_n$.

Suppose there are i errors in A_1, j errors in A_2, k errors in A_3 and l errors in A_4 where $i+j+k+l \leq \frac{n-3}{3}$. Let the respective error positions be

$$\begin{aligned}
&(b_{11}c_{11}, a_{11}b_{11}, b_{11}n), \cdots, (b_{1i}c_{1i}, a_{1i}b_{1i}, b_{1i}n),\\
&(a_{21}b_{21}, a_{21}n, b_{21}n), \cdots, (a_{2j}b_{2j}, a_{2j}n, b_{2j}n),\\
&(b_{31}n, a_{31}n, (n-1)n), \cdots, (b_{3k}n, a_{3k}n, (n-1)n),\\
&(1n, (n-1)n, a_{41}n), \cdots, (1n, (n-1)n, a_{4l}n).
\end{aligned}$$

Let

$$\begin{aligned}
\mathcal{T} = \{&b_{11}, \cdots, b_{1i}, c_{11}, \cdots, c_{1i}, a_{21}, \cdots, a_{2j}, b_{21}, \cdots, b_{2j}, b_{31}, \cdots, b_{3k},\\
&a_{41}, \cdots, a_{4l}\}.
\end{aligned}$$

Then

$$|\mathcal{T}| \leq 2i + 2j + k + l.$$

Since

$$i + j + k + l \leq \frac{n-3}{3},$$

we have $|\mathcal{T}| \leq n-3$. Hence there exists $\alpha \in \Omega \setminus \{n\}$ such that $\alpha \notin \mathcal{T}$. Use an automorphism of the form (n, α) to map errors from $\mathcal{I}_n$ into $\mathcal{C}$.

Case 2. $\mathcal{E} \subseteq \mathcal{I}_n \cup \mathcal{C}$.

Suppose there is at least one error in $\mathcal{I}_n$ and at least one error in $\mathcal{C}$, i.e., at most $\frac{n-6}{3}$ errors in $\mathcal{C}$. We need to show that for errors in each of the sets A_i, $5 \leq i \leq 10$, it is possible to use an automorphism of the form (n, α) to keep the errors in $\mathcal{C}$. The method naturally extends to errors in $\bigcup_{i=5}^{10} A_i$. Since this is similar to the way errors in $\mathcal{I}_n$ are corrected above, it further extends to correction errors in $\mathcal{I} \cup \mathcal{C}$.

(a) Errors in A_5. Suppose there are errors in coordinates of the form (a_5c_5, a_5b_5, b_5x). Consider the set

$$\mathcal{T}_5 = \{a_{51}, \cdots, a_{5t}, b_{51}, \cdots, b_{5t}\}. \tag{6.7}$$

Since $|\mathcal{T}_5| \leq 2t$ and $t \leq \frac{n-6}{3}$, we have $2t \leq n-6$. There exists $\alpha \in \Omega \setminus \{n\}$ such that $\alpha \notin \mathcal{T}$, i.e., $\alpha \neq a_{5i}$ and $\alpha \neq b_{5i}$ for any i. Use an automorphism of the form (n, α).

Notice that if $\alpha = c_{5i}$ in any error position then

$$(n, \alpha) : (a_{5i}\alpha, a_{5i}b_{5i}, b_{5i}x) \mapsto (a_{5i}n, a_{5i}b_{5i}, b_{5i}x)$$

which is in $\mathcal{C}$ since $\{a_{5i}, b_{5i}\} \cap \{b_{5i}, x\} \neq \{a_{5i}, b_{5i}\} \cap \{a_{5i}, n\}$.

Suppose at most $\bar{t}_5 \leq \frac{n-6}{3}$ errors occur in coordinate positions of the form (a_5c_5, a_5b_5, a_5x). Let

$$\overline{\mathcal{T}}_5 = \{a_{51}, \cdots, a_{5\bar{t}}, c_{51}, \cdots, c_{5\bar{t}}, x_1, \cdots, x_{\bar{t}}\}.$$

Since $|\overline{\mathcal{T}}_5| \leq 3\bar{t}$ and $\bar{t} \leq \frac{n-6}{3}$, we have $|\overline{\mathcal{T}}_5| \leq n - 6$. Hence there exists $\alpha \in \Omega \setminus \{n\}$ such that $\alpha \notin \{\overline{\mathcal{T}}_5\}$, i.e., $\alpha \neq a_5, c_5, x$. Use an automorphism of the form (n, α) to fix these errors in $\mathcal{C}$.

(b) Errors in A_6. Suppose at most i_1 errors occur in coordinate positions of the form (b_6c_6, a_6b_6, a_6n) and i_2 errors in coordinate positions of the form $(\bar{a}_6\bar{b}_6, \bar{b}_6\bar{c}_6, \bar{b}_6n)$ such that $i_1 + i_2 \leq \frac{n-6}{3}$. Consider the set

$$\mathcal{T}_6 = \{a_{61}, \cdots, a_{6i_1}, b_{61}, \cdots, b_{6i_1}, \bar{a}_{61}, \cdots, \bar{a}_{6i_2}, \bar{b}_{61}, \cdots, \bar{b}_{6i_2}\}.$$

Since $|\mathcal{T}| \leq 2i_1 + 2i_2$ and $i_1 + i_2 \leq \frac{n-6}{3}$, we have that $3i_1 + 3i_2 \leq n - 6$. Hence there exists at least one element α in $\Omega \setminus \{n\}$ such that $\alpha \notin \mathcal{T}$. Use an automorphism of the form (n, α).

(c) Errors in A_7. Any automorphism of the form (n, α), $\alpha \neq n$, will do. Without loss of generality, let $x = a$. Then (n, α) maps points of the form (ab, an, yn) to points of the form $(ab, an, y\alpha)$. These are in A_8. If $\alpha = y$ then $(ab, an, \alpha n)$ is mapped to $(ab, a\alpha, \alpha n)$, a point in A_6. The cases $\alpha = a$ and $\alpha = b$ are also seen to hold.

(d) Errors in A_8. Suppose there are k_1 and k_2 errors in coordinate positions of the form (a_8n, a_8b_8, b_8n) and (a_8b_8, a_8n, a_8c_8), respectively. As done in other cases above, there exists an element $\alpha \in \Omega \setminus \{n\}$ such that $\alpha \neq a_8, b_8$ in error positions of the form (a_8n, a_8b_8, b_8n) and $\alpha \neq a_8, b_8, c_8$ in error positions of the form (a_8b_8, a_8n, a_8c_8). Use an automorphism of the form (n, α).

(e) Errors in A_9. In this case, it is possible to find $\alpha \in \Omega \setminus \{n-1, n\}$ such that $x \neq b_9, c_9$ in any error position. Hence (n, α) will do.

(f) Errors in A_{10}. Use (n, α) where $\alpha \in \Omega \setminus \{n\}$ and $\alpha \neq a_{10}$.

(g) Errors in A_{11}. Use the automorphism $(n, n-1)$.

If p is odd, a transposition of the form (n, α) will do. The only error position that is mapped to $(1n, 2n, 3n)$ by (n, α) is $(1\alpha, 2\alpha, 3\alpha)$. However, notice that the choice of α in 1 above assumes that $(1\alpha, 2\alpha, 3\alpha)$ is not in error. □

6.5.1 Partial permutation decoding with PD-set S_n

For any prime p and $n \geq 5$, we now determine to what extent permutation decoding can be used for the codes $C_p(M_n)$ with the information set given in Lemma 6.8. To do this, we take for PD-set the permutation automorphism group S_n of $C_p(M_n)$ and use Lemma 2.33.

Recall that coordinate positions of $C_p(M_n)$ have the form (uv, wx, yz) and that, by definition, $|\{u, v\} \cap \{w, x\}| = 1 = |\{w, x\} \cap \{y, z\}|$. The following are possible cases for a given coordinate position (uv, wx, yz).

Case 1. $\{u, v\} \cap \{w, x\} = \{w, x\} \cap \{y, z\}$.

Without loss of generality, suppose $\{u, v\} \cap \{w, x\} = \{w, x\} \cap \{y, z\} = \{x\}$. Hence $(uv, wx, yz) = (ux, wx, yx)$. Since there are $\binom{n}{2}$ possibilities for $\{w, x\}$, $n-2$ for u and $n-3$ for y, there are $2\binom{n-2}{2}\binom{n}{2}$ coordinate positions of the form (ux, wx, yx).

Case 2. $\{u, v\} \cap \{w, x\} \neq \{w, x\} \cap \{y, z\}$.

There are two possibilities. Either $\{u, v\} \cap \{y, z\} = \emptyset$ or $|\{u, v\} \cap \{y, z\}| = 1$.

Case 2(a). $\{u, v\} \cap \{y, z\} = \emptyset$.

Without loss of generality, let $\{u, v\} \cap \{w, x\} = \{x\}$ and $\{w, x\} \cap \{y, z\} = \{w\}$. Then the coordinate position takes the form (ux, wx, wy). Since there are $\binom{n}{2}$ possibilities for $\{w, x\}$, $n-2$ for u and $n-3$ for y, the code has $2\binom{n-2}{2}\binom{n}{2}$ coordinate positions of this form.

Case 2(b). $|\{u, v\} \cap \{y, z\}| = 1$.

The coordinate positions take the form (uw, wx, ux). Since there are $\binom{n}{2}$ possibilities for $\{w, x\}$ and $n-2$ for u, the code has $(n-2)\binom{n}{2}$ coordinate positions of this form.

Consider the sets

$$\begin{aligned} \mathcal{O}_1 &= \{(ux, wx, yx) : u, w, x, y \in \Omega\}, \\ \mathcal{O}_2 &= \{(ux, wx, wy) : u, w, x, y \in \Omega\}, \\ \mathcal{O}_3 &= \{(uw, wx, ux) : u, w, x \in \Omega\}. \end{aligned} \tag{6.8}$$

From the discussion above, it is clear that $\mathcal{O}_1$, $\mathcal{O}_2$ and $\mathcal{O}_3$ partition $E(L^2(K_n)) = \mathcal{P}$, the set of coordinate positions of the code.

Lemma 6.10. *S_n has three orbits in its induced action on $\mathcal{P}$.*

Proof. Since the graph is connected, it follows from Whitney's theorem [64, Theorem 8] (also see Theorem 2.8) that edge-automorphisms are induced by graph automorphisms. By Theorem 6.7, $\mathrm{Aut}(L^2(K_n)) \cong S_n$. Let $\alpha \in S_n$. Then α induces an edge-automorphism σ. Define a map $\sigma : \mathcal{P} \to \mathcal{P}$ by $\sigma((uv, wx, yz)) = (\sigma(u)\sigma(v), \sigma(w)\sigma(x), \sigma(y)\sigma(z))$.

Let $p \in \mathcal{P}$. Either p is of the form (ux, wx, yx) or (ux, wx, wy) or (uw, wx, ux) for some $u, w, x, y \in \Omega$. Consider the element $\sigma(p)$. Let $\mathcal{O}_1$, $\mathcal{O}_2$ and $\mathcal{O}_3$ be as in Equation (6.8). Because σ respects intersections of subsets of Ω, we must have $\sigma(p) \in \mathcal{O}_1$ if p has the form (ux, wx, yx). Also, $\sigma(p) \in \mathcal{O}_2$ if $p \in \mathcal{O}_2$ and $\sigma(p) \in \mathcal{O}_3$ if $p \in \mathcal{O}_3$. Hence S_n partitions $\mathcal{P}$ into the orbits $\mathcal{O}_1$, $\mathcal{O}_2$ and $\mathcal{O}_3$. □

We now use Lemma 2.33 to determine the number of errors $C_p(M_n)$ corrects by permutation decoding with PD-set S_n.

The discussion below is for the binary codes but the result also holds if the code is non-binary. Recall that $C_2(M_n)$ has information set $\mathcal{I}_n = \bigcup_{i=1}^{4} A_i$ where the sets A_i are as in Lemma 6.8.

Let $n_i = \frac{|\mathcal{O}_i \cap \mathcal{I}_n|}{|\mathcal{O}_i|}$ where $i = 1, 2, 3$. Then $n_2 = 0$. We also have

$$\begin{aligned} n_1 &= \frac{|A_1| + |A_3| + |A_4|}{|\mathcal{O}_1|} \\ &= \frac{(n-3)\binom{n-1}{2} + \binom{n-2}{2} + (n-3)}{n(n-1)\binom{n-2}{2}} \\ &= \frac{n^2 - 2n + 2}{n^3 - 3n^2 + 2n}, \end{aligned}$$

and

$$n_3 = \frac{|A_2|}{|\mathcal{O}_3|} = \frac{2\binom{n-1}{2}}{(n-2)\binom{n}{2}} = \frac{2}{n}.$$

Let $N = \max(n_1, n_2, n_3)$. Since $n_3 - n_1 > 0$, we have $N = n_3 = \frac{2}{n}$. Let

$$s = \min\left(\left\lceil \frac{1}{N} \right\rceil - 1, 2n - 6\right) = \left\lceil \frac{n}{2} \right\rceil - 1.$$

Then, by Lemma 2.33, S_n is an $\left(\lceil \frac{n}{2} \rceil - 1\right)$-PD-set for $C_2(M_n)$.

Notice that much as we are able to correct more errors by using S_n as PD-set, S_n is much larger than the PD-set exhibited in Proposition 6.9.

Appendix A

Computer programs

We now present programs that were used to investigate some of the codes obtained in this thesis.

A.1 Gordon bound

The program below is written in Python [15]. It calculates the Gordon bound (see Equation (2.5)) for the PD-set of a given linear code. Parameters used in the program (length, dim and dist) are of codes from embeddings of the strong product of triangular graphs and K_2 considered in Chapter 4. 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 triangular graphs and differences of rows of their incidence matrices

The Magma [7] program below examines codes from incidence matrices of triangular graphs and differences of rows of the matrices.

```
n            := 4;
omega        := {1..n};
omegasubsets := Subsets(omega,2);
p            := 2;

// f  := Open("C:\\Users\\khumbo\\Desktop\\magma\\results.txt","w");
// Overwrite := true;

// Triangular Graph
triangular   := Graph<omegasubsets|{{u,v}: u,v in omegasubsets|
                #(u meet v) eq 1}>;
vertexset    := VertexSet(triangular);
edgeset      := EdgeSet(triangular);
genmatrix    := IncidenceMatrix(triangular);
M            := KMatrixSpace(FiniteField(p), #vertexset, #edgeset);
Gen          := M!genmatrix;
// Codes obtained from incidence matrices of triangular graphs
// are C:= LinearCode(Gen). Their properties can now be
// investigated using standard magma commands.

// In the loop below we obtain differences of rows of incidence
// matrices of triangular graphs.
len          := NumberOfRows(Gen);
S            := [];
for i in [1..len] do
    a := Gen[1] - Gen[i];
    Append(~S,a);
end for;

// Below, we generate the codes En from differences of rows of
// incidence matrices of triangular graphs.
NewGen       := M!Matrix(#vertexset,#edgeset,S);
En           := LinearCode(NewGen);
len          := Length(En);
dim          := Dimension(En);
mindist      := MinimumDistance(En);
```

A.3 Codes from embeddings of strong products of triangular graphs and K_2

The Magma [7] program in this section investigates properties of linear codes from embeddings of strong products and K_2 considered in Chapter 4.

```
// constants
n     := 5;
p     := 3;
Omega := {1..n};

// V is the vertex set of the graph. Each vertex is written
// as a list of 3 elements. Thus [a,b,b] represents the
// vertex ({a,b},{b}).
V   := {[a,b,b]: a,b in Omega | a ne b};

// E1 and E2 are sets of edges of the graphs. Edges in E1
// satisfy the first adjacency condition of Definition 4.1.
// Edges in E2 satisfy the second adjacency condition.
E1  := {{u,v}: u,v in V | {u[1],u[2]} eq {v[1],v[2]} and u ne v};
E2  := {{u,v}: u,v in V | #({u[1],u[2]} meet {v[1],v[2]}) eq 1
          and u[3] eq v[3]};
E   := E1 join E2;

Gamman  := Graph<V|E>;
// Generate the graph $\Gamma_{n}$ of  Chapter 4. The command
// Gamman :=Complement(Gamman) switches  the investigation to that
// of codes from complements of $\Gamma_{n}$ considered in Chapter 5.

// Properties of the graph and codes from its incidence
// matrices can now be investigated using standard magma commands.
Gn    := IncidenceMatrix(Gamman);
M     := KMatrixSpace(FiniteField(p), #V, #E);
Gn    := M!Gn;
C     := LinearCode(Gn);
AutC  := AutomorphismGroup(C);
```

A.4 Codes from incidence matrices of line graphs of triangular graphs

The Magma [7] program below examines the action of the automorphism group $G = S_n$ on coordinate positions of binary codes from incidence matrices of line graphs of triangular graphs considered in Section 6.5.1. G-orbits of the action are obtained. Using Lemma 2.33, the program computes the maximum of the ratios $\frac{|\mathcal{I}_n \cap \mathcal{O}|}{|\mathcal{O}|}$ where $\mathcal{I}_n$ is an information set and $\mathcal{O}$ is a G-orbit. The output of the program is a number s of errors that the codes correct by permutation decoding with G as PD-set.

```
// Constants
n         := 5;
p         := 2;
Omega     := {1..n};
Omega1    := {1..n-1};
Omega2    := {1..n-2};
Omega3    := {1..n-3};
Omegatwo  := Subsets(Omega,2);  // 2-element subsets of Omega
G         := Sym(n);            // Symmetric Group on n elements.

//Open file to write results to, full path to file required.
f         := Open("C:\\Documents and Settings\\khumbo
              \\Desktop\\mymagma\\orbitsresults.txt","w");
overwrite := true;

// Generate coordinate positions of the code of $L^{2}(K_{n})$ and
// print output in file orbitsresults.txt
points    := {{{u,v},{v,w}}: u,v,w in Omegatwo
             | #(u meet v) eq 1 and #(v meet w) eq 1 and u ne w};
Put(f,Sprint(points));

// Find G-orbits when G acts on the set of coordinate positions.
orbits       := {};
```

```
for p in points do
     porbit  := p^G;
     orbits  := orbits join {porbit};
     points  := points diff porbit;
     if #points eq 0 then break; end if;
end for;
// print G-orbits to file
Put(f,Sprint(orbits));

// Information set of the binary codes is the union of
// A1, A2, A21, A3 and A4 below.
A1      := {{{{a,b},{b,c}},{{a,b},{b,n}}} :a,b,c in
             Omega1 | a ne b and b ne c and a lt c};
A2      := {{{{a,b},{b,n}},{{a,n},{b,n}}}:a,b in Omega1| a lt b};
A21     := {{{{a,b},{a,n}},{{a,n},{b,n}}}:a,b in Omega1| a lt b};
A3      := {{{{a,n},{b,n}},{{a,n},{n-1,n}}}:a,b in Omega2| a lt b};
A4      := {{{{n-2,n},{n-1,n}},{{a,n},{n-1,n}}}: a in Omega3};
infoset := A1 join A2 join A21 join A3 join A4;

//Calculate the ratios $|\mathcal{O}\cap \mathcal{I}|/|\mathcal{O}|$
// where $\mathcal{O}$ is a G-orbit.
N       :={};
for Gorbit in orbits do;
    nn  := #(infoset meet Gorbit)/ #Gorbit;
    Include(~N,nn);
end for;
max     := Maximum(N);

// maximum number of errors $t$ correctable by the code.
t       := Floor((4*n-11)/2);

// number of errors correctable by permutation decoding
s     := Minimum(Ceiling(1/max)-1, t);
s;
```

Bibliography

[1] B́. Andrásfai, *Graph Theory: Flows, Matrices.* New York: Taylor and Francis, 1991.

[2] 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).

[3] R. Balakrishnan and K. Ranganathan, *A Textbook of Graph Theory.* New York: Springer-Verlag, 2000.

[4] L.D. Baumert, R.J. McEliece and G. Solomon, Decoding with mulipliers, *JPL Deep Space Network Progress Report 42-34,* (1976), 43-46.

[5] T. Beth, D. Jungnickel and H. Lenz, *Design Theory.* Cambridge: Cambridge University Press, 1993.

[6] J.A. Bondy and U.S.R. Murty, *Graph Theory*, Vol. 244, Graduate Texts in Mathematics, Springer, 2008.

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

[8] 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.

[9] P.J. Cameron and J.H. van Lint, *Designs, Graphs, Codes and their Links.* Cambridge: Cambridge University Press, 1991.

[10] 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.

[11] G.C. Clark, Jr. and J .B. Cain, *Error-correction for digital communications.* New York: Plenum Press, 1981.

[12] J.T. Coffey and R.M. Goodman, The complexity of information set decoding, *IEEE Trans. Inform. Theory*, 36 (1990), 1031-1037.

[13] P. Dankelman, J.D. Key and B.G. Rodrigues, Codes from incidence matrices of graphs, *in preparation.*

[14] R. Diestel, *Graph Theory.* New York: Springer, 1997.

[15] A. Downey, J. Elkner and C. Meyers, *How to think like a computer scientist: Learning with Python.* Massachusetts: Green Tea Press, 2002.

[16] W. Fish, *Codes from Uniform Subset Graphs and Cycle Products.* PhD Thesis, University of the Western Cape, 2007.

[17] W. Fish, R. Fray and E. Mwambene, Binary codes from the complements of the triangular graphs, *Quaest. Math.*, 33 (2010), 399-408.

[18] 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.

[19] W. Fish, J.D. Key and E. Mwambene, Codes from incidence matrices and line graphs of Hamming graphs, *Discrete Math.*, 310 (13-14) (2010), 1884-1897.

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

[21] W. Fish, J.D. Key and E. Mwambene, Binary codes from the line graph of the n-cube, *J. Symbolic Comput.*, 45 (7) (2010), 800-812.

[22] W. Fish, J.D. Key and E. Mwambene, Codes from the incidence matrices of graphs on 3-sets, *Discrete Math.*, 311 (2011), 1823-1840.

[23] W. Fish, K. Kumwenda and E. Mwambene, Codes and designs from triangular graphs and their line graphs, *Cent. Eur. J. Math.*, to appear.

[24] W. Fish, K. Kumwenda and E. Mwambene, Codes from embeddings of the strong product of triangular graphs and K_2 and certain induced subgraphs, *Ars Combin.*, to appear.

[25] R. Frucht, On the groups of repeated graphs, *Bull. Amer. Math. Soc.*, 55 (1949), 418-420.

[26] Z. Füredi, Graphs of diameter 3 with the minimum number of edges, *Graphs Combin.*, 6 (1990) 333-337.

[27] C. Godsil and G. Royle, *Algebraic Graph Theory.* New York: Springer, Vol. 207 of Graduate Texts in Mathematics, 2001.

[28] D.M. Gordon, Minimal permutation sets for decoding the binary Golay codes, *IEEE Trans. Inform. Theory*, IT-28 (1982), 541-543.

[29] W.H. Haemers, R. Peeters and J. van Rijckevorsel, Binary codes of strongly regular graphs, *Des. Codes Cryptogr.*, 17 (1999), 187-209.

[30] R.L. Hemminger, On Whitney's line graph theorem, *Amer. Math. Monthly*, 79(4) (1972) 374-378.

[31] R. Hill, *A First Course in Coding Theory.* Oxford: Oxford University Press, 1986.

[32] W. C. Huffman, Codes and Groups, in: V. S. Pless and W. C. Huffman (eds.), *Handbook of Coding Theory*, Vol. 2. Amsterdam: Elsevier, (1998), 1345-1440.

[33] W. C. Huffman and V. S. Pless, *Fundamentals of Error-Correcting Codes.* Cambridge: Cambridge University Press, 2003.

[34] W. Imrich and H. Izbicki, Associative products of graphs, *Monatsh. Math*, 80 (1975) 277-281.

[35] T. Kasami, A decoding procedure for multiple-error-correcting cyclic codes, *IEEE Trans. Inform. Theory*, IT-10 (1964) 134-138.

[36] J. D. Key, Permutation decoding: An update. Available from http://www.ces.clemson.edu/~keyj/Key/PDupdate.pdf, 2003.

[37] 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

[38] J. D. Key, Recent developments in permutation decoding, available from http://www.ces.clemson.edu/~keyj/Key/SAMS05b.pdf.

[39] 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.

[40] 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.

[41] 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.

[42] J.D. Key, J. Moori and B.G. Rodrigues, Codes associated with triangular graphs and permutation decoding, *Int. J. Information and Coding Theory*, 1 (3) (2010), 334-349.

[43] J.D. Key and P. Seneviratne, Permutation decoding for binary codes from lattice graphs, *Discrete Math.*, 308 (2008), 2862-2867.

[44] J.D. Key and P. Seneviratne, Binary codes from rectangular lattice graphs and permutation decoding, *European J. Combin.*, 28 (1) (2007), 121-126.

[45] 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.

[46] J. D. Key, W. Fish and E. Mwambene, *Codes from incidence matrices and line graphs of Hamming graphs $H^k(n, 2)$ for $k \geq 2$*, Adv. Math. Commun., **5** (2011), 373-394.

[47] H-J. Kroll and R. Vincenti, Antiblocking decoding, *Discrete Appl. Math.*, 158 (2010), 1461-1464.

[48] K. Kumwenda and E. Mwambene, Codes from graphs related to the categorical product of triangular graphs and K_n, *Proceedings of 2010 IEEE Information Theory Workshop*, Dublin, August 30-September 3, 2010, 1-5, doi:10.1109/CIG.2010.5592662.

[49] J. Limbupasiriporn, *Partial permutation decoding for codes from designs and finite geometries*, Ph.D Thesis, Clemson University, 2005.

[50] C.H.C. Little, D.D. Grant and D.A. Holton, On defect-d matchings in graphs, *Discrete Math.*, 13 (1975), 41-54.

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

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

[53] J.L. Massey, Reversible codes, *Inform. and Control*, 7 (1964), 369-380.

[54] 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.

[55] E. Prange, The use of information sets in decoding cyclic codes, *IRE Trans.*, 8 (1962), S5-S9.

[56] B.G. Rodrigues, *Codes of Designs and Graphs from Finite Simple Groups*, PhD Thesis, University of Natal, 2003.

[57] G. Sabidussi, Graph multiplication, *Math. Z.*, 72 (1) (1960), 446-457.

[58] J. Schönheim, On coverings, *Pacific J. Math.*, 14 (1964), 1405-1411.

[59] P. Seneviratne, *Permutation Decoding of Codes from Graphs and Designs*, PhD Thesis, Clemson University, 2007.

[60] 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.

[61] 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.

[62] V.G. Vizing, The cartesian product of graphs (Russian), *Vychisl. Sistemy*, 9 (1963) 30-43.

[63] D.B. West, *Introduction to Graph Theory* (Second Edition). Patparganj: Pearson Education Pte. Ltd., 2001.

[64] H. Whitney, Congruent graphs and the connectivity of graphs, *Amer. J. Math.*, 54 (1932), 150-168.

Index