Codes from embeddings of the strong product of triangular graphs and K_2 and certain induced subgraphs

Washiela Fish, Khumbo Kumwenda and Eric Mwambene
Department of Mathematics and Applied Mathematics,
University of the Western Cape,
Private Bag X17, Bellville 7535, South Africa.
Emails: wfish@uwc.ac.za, khumbo@aims.ac.za, emwambene@uwc.ac.za

Abstract

We introduce vertex-transitive graphs Γ_n that are also embeddings of the strong product of triangular graphs $L(K_n)$ and the complete graph K_2. For any prime p, linear codes obtained from the row span of incidence matrices of the graphs over $\mathbb{F}_p$ are considered; their main parameters (length, dimension and minimum distance) and automorphism groups are determined. Unlike most codes that have been obtained from incidence and adjacency matrices of regular graphs by others, binary codes from the row span of incidence matrices of Γ_n have other minimum words apart from the rows of the matrices. Using a specific information set, PD-sets for full permutation decoding of the codes are exhibited.

Keywords: Automorphism group, incidence design, error-correcting code, strong product, permutation decoding, triangular graph.

MSC 94B05, 94A45

1 Introduction

Considerable effort, with significant success, has been directed towards the description of properties of linear codes generated by adjacency and incidence matrices of various regular graphs. Graphs that have been studied include complete graphs [14], triangular graphs and their complements [5, 6, 15, 19], Hamming graphs and their line graphs [7, 8], the Johnson graphs and the Odd graphs [5]. What has been appealing in all this is that some codes obtained so far are amenable to permutation decoding. In this paper, we employ this philosophy on embeddings

Γ_n of the strong product of triangular graphs $L(K_n)$ and K_2. Some properties of the graphs including their automorphisms are determined. These graphs are serendipity by-products of our study of codes from the row span of incidence matrices of the iterated line graphs $L^2(K_{n+1})$. Complements of the graphs and corresponding codes have been studied in [16].

The codes from Γ_n have some properties similar to those shown by codes from incidence matrices of complete graphs [14]. For instance, automorphisms of the codes are isomorphic to those of the graphs and their minimum words include scalar multiples of the rows of the matrices. However, unlike codes from the various graphs mentioned above, the binary codes from incidence matrices of Γ_n have other minimum words apart from the rows of the matrices. These minimum words have been established in Proposition 3(b).

Further, we consider complete porcupines (see [9] and Definition 2), graphs that are induced subgraphs of Γ_n and offer some interesting codes in their own right. Codes from incidence matrices of complete porcupines are therefore considered first. These codes have minimum weight one in as much as they are not full spaces.

The graphs Γ_n are given in Definition 1. Our main results are summarised in Theorem 1. Note that a vertex $(\{a,b\},\{a\})$ of Γ_n is written as (ab,a) for short. $[u,v]$ denotes an edge between vertices u and v and it also represents a coordinate position of the code indexed by the edge.

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

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

(b) *$C_2(G_n)$ is an $\left[(n-1)\binom{n}{2}, 2\binom{n}{2}-1, n-1\right]_2$ code. Its minimum words are the rows of G_n and the n codewords of the form $\sum_{x\neq a} v^{\overline{(ax,a)}}$ where $v^{\overline{(ax,a)}}$ is the row of G_n indexed by the vertex (ax,a).*

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

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

(e) *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.

The proof of Theorem 1 follows from a series of lemmas and propositions in the sections below. The rest of the paper is organised as follows. In Section 2 we define terminology and give an overview of results that will be used. In Section 3 we consider some properties of Γ_n including automorphism groups. Codes from incidence matrices of complete porcupines and Γ_n are discussed in Section 4. In Section 6 we consider automorphism groups of codes from incidence matrices of Γ_n and exhibit their PD-sets using specific information sets.

2 Preliminaries

Codes considered in this paper are linear and the graphs are finite, connected and undirected having no loops nor multiple edges. Coding theory, graph theory and design theory terminology not defined in this section is used in the sense of MacWilliams and Sloane [17], Bondy and Murty [3] and Assmus and Key [2], respectively.

A q-ary linear code C of length n, dimension k and minimum distance d will be denoted $[n, k, d]_q$. The **permutation automorphism group** of C is the set of coordinate permutations that map C to itself. It will be denoted $\mathrm{Aut}(C)$.

Permutation decoding is a method due to MacWilliams [18] and has also been described in [17, 11]. It has been used to decode, among others, linear codes generated by incidence and adjacency matrices of various regular graphs (see [5, 14, 15, 7, 8, 16, 12] for specific examples). The method uses a subset S of $\mathrm{Aut}(C)$ called a **PD-set**. If C is a t-error-correcting-code then S has the property that every vector of weight at most t is mapped by at least one member of S to a vector where errors occur only in check positions. The minimum size of S is given by the Gordon bound [10] (see also [11, Theorem 10.2.2, p. 404]). An algorithm for the method is given in [11, p. 403-404].

A graph is a pair $\Gamma = (V, E)$ of sets satisfying $E \subseteq V^{\{2\}}$, i.e., the pairs of E are 2-element subsets of V. A complete subgraph of Γ is called a **clique**. A clique is maximal if it is not contained in a larger 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. The largest clique in a graph is a maximum clique. Let $P = \{V_i : i \in I\}$ be a partition of $V(\Gamma)$. The **quotient graph** of Γ modulo P, written Γ/P, is defined by $V(\Gamma/P) = P$ and $[V_i, V_j] \in E(\Gamma/P)$ if there exist u in V_i and v in V_j, $i \neq j$, such that $[u, v] \in E(\Gamma)$. The **strong product** of two graphs Γ and H, written $\Gamma \boxtimes H$, is defined by $V(\Gamma \boxtimes H) = V(\Gamma) \times V(H)$ and $[(u, v), (u', v')] \in E(\Gamma \boxtimes H)$ if $u = u'$ and $[v, v'] \in E(H)$; or $[u, u'] \in E(\Gamma)$ and $v = v'$; or $[u, u'] \in E(\Gamma)$ and $[v, v'] \in E(H)$.

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

is bijective, then α is an **automorphism** of Γ. The automorphism group of Γ will be written as $\mathrm{Aut}(\Gamma)$. Γ is **vertex-transitive** if for every pair of vertices u and v, there is an automorphism α in $\mathrm{Aut}(\Gamma)$ such that $\alpha(u) = v$.

A $t-(v,k,\lambda)$ **design** $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is a finite incidence structure such that $\mathcal{P}$ has v *points*, every **block** B in $\mathcal{B}$ has k points and every size-t subset of $\mathcal{P}$ is incident on exactly λ blocks. An **incidence matrix** of $\mathcal{D}$ is a $|\mathcal{B}| \times |\mathcal{P}|$ matrix G such that $g_{ij} = 1$ if $(p_j, B_i) \in \mathcal{I}$ and $g_{ij} = 0$ otherwise. The **incidence vector** v^P of any subset P of $\mathcal{P}$ is the characteristic vector of P, i.e., the vector such that $v^P(i) = 1$ if $i \in P$ and $v^P(i) = 0$ otherwise. The rows of G are incidence vectors of the blocks of $\mathcal{D}$. The q-ary linear code of the design is the space spanned over $\mathbb{F}_q$ by the incidence vectors where $q = p^t$, p a prime and $t \in \mathbb{N}$. 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. Its incidence matrix G is the same as that of Γ.

Let $C_p(G)$ be the linear code obtained from the row span of G over $\mathbb{F}_p$ where p is a prime. One is often interested in determining the existence of the all-one vector $\jmath$ in a given code or its dual. If $p = 2$ then it is clear that $\jmath \in C_2(G)^\perp$ if $C_2(G)$ is even. If p is odd then $\jmath \in C_p(G)$ since the sum of all rows of G is equal to $2\jmath$.

We also note that for any p, $C_p(G)$ is not self-orthogonal. This is because the inner product of any pair of rows indexed by adjacent vertices of the corresponding graph is 1.

3 The graphs Γ_n

The graphs Γ_n that we have been alluding to are defined as follows.

Definition 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 $X = \Omega^{\{2\}} \times \Omega^{\{1\}}$. The graph Γ_n is defined by

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

Observe that Γ_n has $2\binom{n}{2}$ vertices. The neighbourhood of each vertex (ab, a) is the set $N = \{(ab,b)\} \cup \{(ax,a) : x \neq a\}$. Hence Γ_n is $(n-1)$-regular. Γ_4 is illustrated in Figure 1.

Identifying $V(L(K_n))$ with $\Omega^{\{2\}}$ and $V(K_2)$ with $\{0,1\}$, we have the following.

Lemma 1. *Γ_n is an embedding of $L(K_n) \boxtimes K_2$.*

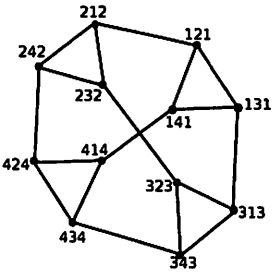

Figure 1: Γ_4 (iji denotes the vertex (ij, i))

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

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

Defined this way, ϕ is easily seen to be an injective homomorphism. □

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 $\sigma_\alpha((ab, a)) = (\alpha(a)\alpha(b), \alpha(a))$.

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

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 $u = (ab, a)$ is adjacent to $v = (ab, b)$ and to $n-2$ vertices of the form $w = (ax, a)$ 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. The graphs Γ_n are vertex-transitive. To see this, consider any two distinct vertices (ab, a) and $(a'b', a')$ of Γ_n. It is always possible to find 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 $\sigma_\alpha((ab, a)) = (a'b', a')$.

Let $X_a = \{(ax, a) : x \neq a\}$. There are n such sets and they partition $V(\Gamma_n)$. Also note that if $P = \{X_a : a \in \Omega\}$ then the quotient graph Γ_n/P is isomorphic to the complete graph K_n.

Lemma 2. *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 $N[v] = \{(ab, b)\} \cup \{(ax, a) : x \neq a\}$ of a vertex $v = (ab, a) \in X_a$. 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 (ab, b) is adjacent only to v. The remaining vertices in $N[v] \setminus \{(ab, b)\} = X_a$ are pairwise adjacent. Hence X_a is the largest clique in $N[v]$. □

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

Proposition 1. $\mathrm{Aut}(\Gamma_n) \cong S_n$.

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 $u = (ab, a) \in V(\Gamma_n)$. 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 Codes from incidence matrices of Γ_n

For any prime p, we now consider the p-ary codes $C_p(G_n)$ obtained from the row span over $\mathbb{F}_p$ of incidence matrices G_n of the graphs Γ_n. Since G_n contains an incidence matrix M_{n-1} of H_{n-1}, a complete porcupine, we first study the codes $C_p(M_n)$ in Proposition 2 before describing the codes $C_p(G_n)$ in Proposition 3.

In the following let $V_1 = \{(ab, a), (ab, b) : a, b \in \{1, 2, 3\}, a < b\}$. For $4 \leq i \leq n$, let $V_{i-2} = \{(ai, a), (ai, i) : 4 \leq i \leq n, a < i\}$. Write G_n as follows. Order the rows of G_n so that for given values of a and i, a row corresponding to the vertex (ai, a) is followed by a row corresponding to the vertex (ai, i). Columns are ordered by first constructing edges between vertices in $\bigcup_{i=1}^{n-3} V_i$, then edges between vertices in $\bigcup_{i=1}^{n-3} V_i$ and V_{n-2} and, lastly, edges between vertices in V_{n-2}. The resulting matrix is a $2\binom{n}{2} \times (n-1)\binom{n}{2}$ matrix of the form

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

where:

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

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

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

(d) M_{n-1} is an incidence matrix of the complete porcupine H_{n-1}. These graphs are given in Definition 2.

Example 1. The 12 vertices of Γ_4 are ordered as follows: $(12,1), (12,2), (13,1), (13,3), (23,2), (23,3), (14,1), (14,4), (24,2), (24,4), (34,3), (34,4)$. Its incidence matrix is

$$G_4 = \left[\begin{array}{c|c|c} 110000 & 100000 & 000000 \\ 101000 & 010000 & 000000 \\ 010100 & 001000 & 000000 \\ 000110 & 000100 & 000000 \\ 001001 & 000010 & 000000 \\ 000011 & 000001 & 000000 \\ \hline 000000 & 101000 & 100000 \\ 000000 & 000000 & 111000 \\ 000000 & 010010 & 000100 \\ 000000 & 000000 & 010110 \\ 000000 & 000101 & 000001 \\ 000000 & 000000 & 001011 \end{array}\right]. \tag{2}$$

We now define complete porcupines. As in Definition 1, Ω denotes the set $\{1, \cdots, n\}$.

Definition 2. Let $A = \{(a,0) : a \in \Omega\}$ and $B = \{(b,1) : b \in \Omega\}$. Denote by K_A the complete graph with vertex set 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*.

These are also the graphs simply defined as porcupines in [9]. Denote by M_n an incidence matrix of 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 the quills of the graph. This way, M_n takes the form

$$\left[\begin{array}{c|c} L_n & I \\ \hline \mathbf{0} & I \end{array}\right] \tag{3}$$

where L_n is an incidence matrix of K_A. Codes generated by L_n have been considered in [14].

Proposition 2. *For $n \geq 3$, let $C_p(M_n)$ denote the p-ary code from the row span of M_n. Then $C_2(M_n)$ is a $\left[\binom{n+1}{2}, 2n-1, 1\right]_2$ code and, if p is any odd prime, $C_p(M_n)$ is an $\left[\binom{n+1}{2}, 2n, 1\right]_p$ code.*

Proof. The length of the code is the order of $E(H_n) = E(K_A) \cup E_Q$. Since the minimum weight is easy to see, we only check the dimension of the codes.

H_n is connected and hence by [1, Theorem 10, p. 140], M_n has dimension $2n-1$ over $\mathbb{F}_2$. Since the graph is not bipartite (having even cycles in K_A), it follows from Result 2 in [13] that its incidence matrix 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 2. *For any prime p, let $\overline{C}_p(M_n)$ denote the subcode of $C_p(M_n)$ obtained from the row span over $\mathbb{F}_p$ of the submatrix $[L_n|I]$ of M_n in Equation (3). Then $\overline{C}_p(M_n)$ is an $\left[\binom{n+1}{2}, n, n\right]_p$ code.*

Proof. The length and dimension are clear. For the minimum weight, let $c \in \bar{C}_p(M_n)$. Then c can be written as a concatenation of two vectors, c_1 and c_2, from the two column blocks in $[L_n|I]$. By Theorem 1 of [14], we know that $\mathrm{wt}(c_1) \geq n-1$. Since $\mathrm{wt}(c_2) \geq 1$, we have the result. □

We note the following in relation to incidence designs of the graphs Γ_n. The block corresponding to a vertex $v = (ab, b)$ is the set

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

and it has incidence vector

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

These vectors have Hamming weight $n-1$.

We now turn to the main issue at hand, namely, the description and permutation decoding of the codes $C_p(G_n)$ from the span over $\mathbb{F}_p$, p any prime, of these incidence vectors. The case of $n = 3$ is less interesting; Γ_3 being a 6-cycle. It is stated in the lemma below.

Lemma 3. *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 over $\mathbb{F}_p$ where p is any prime. Then $C_p(G_3)$ is a $[6,5,2]_p$ code.*

Proof. The dimension of the binary codes is obtained from [1, Theorem 10, p. 140] since the 6-cycle is connected. Since the 6-cycle is also bipartite, G_3 has dimension 5 over $\mathbb{F}_p$, p odd, by Result 2 in [13].

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 odd.

Write G_3 as the left uppermost submatrix of G_4 in Equation (2). Partition the 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 the rows of G_3 are considered, one obtains $\mathrm{wt}(c_1) \geq 1$ and $\mathrm{wt}(c_2) \geq 1$. Hence $\mathrm{wt}(c) \geq 2$. 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:

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

Proposition 3. *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 over $\mathbb{F}_p$ where p is any prime.*

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

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

Proof. Recall that the complete porcupine H_{n-1} is an induced subgraph of Γ_n. Since H_{n-1} contains the complete graph, it has odd cycles. Hence Γ_n is not bipartite. By Result 2 of [13], G_n has full rank over $\mathbb{F}_p$. On the other hand, the binary codes have dimension $2\binom{n}{2} - 1$ [1, Theorem 10, p. 140].

We use induction to prove the assertion about the minimum weight of the codes noting that it holds for $n = 3$ in Lemma 3. Suppose the result holds for $n-1$ where $n \geq 4$. Suppose the result holds for $n-1$. Write G_n as in Equation (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., $R_1 = [G_{n-1}|I|0]$ and $R_2 = [0|J|M_{n-1}]$.

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 $k_3 = \binom{n}{2}$.

Let $c \in C_p(G_n)$. Suppose c is obtained from a linear combination of r of the first $(n-1)(n-2)$ rows. Then c is a concatenation of three vectors, c_1, c_2 and c_3, from the three column blocks in the submatrix $[G_{n-1}|I|0]$ of G_n. Hence

$c_1 = \sum \alpha_i g_i$ 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}. Since $\mathrm{wt}(c_1) \geq n-2$ and $\mathrm{wt}(c_2) = r$, we see that $\mathrm{wt}(c) \geq n-2+r$. $\mathrm{wt}(c) = n-1$ if c is a constant multiple of a row of G_n.

(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, $\mathrm{wt}(c_1) \geq n-2$. Since $\mathrm{wt}(c_2) = r_1$, we have $\mathrm{wt}(c) \geq n-2+r_1 \geq n-1$. From the form of G_n, it is clear that $\mathrm{wt}(c) = n-1$ if c is a constant 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 $j_i \neq 0$ for any i then $\mathrm{wt}(c_2) \geq n-2$ 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 constant multiple of a row of R_2. If c is a linear combination of rows corresponding to vertices of the form (an, n) then $c_2 = 0$. By Corollary 2, $\mathrm{wt}(c) = \mathrm{wt}(c_3) \geq n-1$ with equality if c is a multiple of an (an, 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 2, $\mathrm{wt}(c_3) \geq 1$. If $\mathrm{wt}(c_3) = 1$ then it is clear that $c_2 \neq 0$. Hence $\mathrm{wt}(c) \geq (n-1) + \mathrm{wt}(c_2) > n-1$.

(b) 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

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

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

If $r_2' < n-1$ then at least one (an, 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 (an, 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 besides the 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 $v^{(ax,a)}$, where $(ax, a) \in X_a$, are pairwise commonly incident at exactly $\binom{n-1}{2}$ coordinate positions. Therefore the codeword $\sum_{x \neq a} v^{(ax,a)}$ has weight $(n-1)^2 - 2\binom{n-1}{2} = n-1$. This way, we determine n more minimum words. □

5 The duals $C_p(G_n)^\perp$

We now present some results on the duals $C_p(G_n)^\perp$ where p is any prime and $n \geq 3$.

A generalisation of Lemma 3 of [8] shows that if a regular graph has an m-cycle $(u_0, \cdots, u_{m-1})$ where $m \geq 4$ is even then the dual of the code generated by its incidence matrix has codewords of the form

$$v^{[u_0,u_1]} - v^{[u_1,u_2]} + \cdots - v^{[u_{m-1},u_0]}. \tag{4}$$

Recall that Γ_3 is the 6-cycle. Hence for any prime p, $C_p(G_3)^\perp$ has a weight-6 codeword. In fact, $C_p(G_3)^\perp = [6, 1, 6]_p$.

As seen in Figure 1, Γ_4 has four 6-cycles. Thus if p is odd then $C_p(G_4)$ has weight-6 codewords. Computations using Magma [4] for small values of p suggest that $C_p(G_4) = [18, 6, 6]_p$.

If $n \geq 5$ then Γ_n has 4-cycles in the maximum cliques X_a. Hence if p is odd then $C_p(G_n)^\perp$ has weight-4 codewords of the form

$$v^{[(ab,a),(ac,a)]} - v^{[(ac,a),(ad,a)]} + v^{[(ad,a),(ae,a)]} - v^{[(ae,a),(ab,a)]} \tag{5}$$

where a, b, c, d, e are distinct elements of Ω.

Over $\mathbb{F}_2$, the vectors in Equation (4) are in $C_2(G_n)^\perp$ if $m \geq 3$. If $n \geq 4$ then Γ_n has 3-cycles in the maximum cliques. So $C_2(G_n)^\perp$ contains weight-3 codewords of the form

$$v^{[(ab,a),(ac,a)]} + v^{[(ac,a),(ad,a)]} + v^{[(ad,a),(ab,a)]}. \tag{6}$$

We have the following result.

Proposition 4. *For any prime p, let $C_p(G_n)^\perp$ be the dual of the p-ary linear code from the row span of an incidence matrix G_n of the graph Γ_n. Then*

(a) *If $n \geq 4$ then $C_2(G_n)^\perp$ is an $[(n-1)\binom{n}{2}, (n-3)\binom{n}{2}+1, 3]_2$ code.*

(b) *If $n \geq 5$ and p is odd then $C_p(G_n)^\perp$ is an $[(n-1)\binom{n}{2}, (n-3)\binom{n}{2}, 4]_p$ code.*

Proof. We show that the minimum weight cannot be smaller. It is clear that the dual has no unit vectors.

(a) Let w be a weight-2 vector in $\mathbb{F}_2^k$ where $k = (n-1)\binom{n}{2}$. Then w has the form $v^{[x,y]} + v^{[x',y']}$ where x, y, x' and y' are distinct vertices of Γ_n. Let $v^{\overline{x}}$ be the incidence vector of the block $\overline{x}$ in the incidence design of Γ_n. If $[x,y]$ and $[x',y']$ are not adjacent then $(w, v^{\overline{x}}) = 1$. Suppose $[x,y]$ and $[x',y']$ are adjacent. Without loss of generality, let $x' = y$. Then again $(w, v^{\overline{x}}) = 1$. Hence $w \notin C_2(G_n)^\perp$. Since $C_2(G_n)^\perp$ contains the weight-3 codewords in Equation (6), it has minimum weight 3.

(b) A similar argument holds for $C_p(G_n)^\perp$ if p is odd. Hence we only need to show that $C_p(G_n)^\perp$ has no weight-3 codewords.

Let w be a weight-3 vector in $\mathbb{F}_p^k$ where $k = (n-1)\binom{n}{2}$ and p is odd. Then either w has the form $\alpha_1 v^{[x,y]} + \alpha_2 v^{[x',y']} + \alpha_3 v^{[x'',y'']}$ or $\alpha_1 v^{[x,y]} + \alpha_2 v^{[x,x']} + \alpha_3 v^{[x'',y'']}$ or $\alpha_1 v^{[x,y]} + \alpha_2 v^{[x,x']} + \alpha_3 v^{[x',y'']}$ or $\alpha_1 v^{[x,y]} + \alpha_2 v^{[x,x']} + \alpha_3 v^{[x,y']}$ or $\alpha_1 v^{[x,y]} + \alpha_2 v^{[x,x']} + \alpha_3 v^{[y,x']}$ where $\alpha_i \in \mathbb{F}_p^*$, x, y, x', y', x'' and y'' are distinct vertices of Γ_n.

In the first four cases, we have $(w, v^{\overline{y}}) = \alpha_1$. In the last case, $(w, v^{\overline{x}}) = \alpha_1 + \alpha_2$. If $\alpha_2 = -\alpha_1$ then $(w, v^{\overline{y}}) = \alpha_1 + \alpha_3$. If we further have $\alpha_3 = -\alpha_1$ then $(w, v^{\overline{x'}}) = -2\alpha_1 \neq 0$. Hence in all cases there exists an incidence vector u such that $(u, w) \neq 0$, i.e., $w \notin C_p(G_n)^\perp$. Since $C_p(G_n)^\perp$ contains the weight-4 codewords in Equation (5), it has minimum weight 4. □

6 Permutation decoding

For any prime p, we first determine automorphisms of $C_p(G_n)$. Information sets and corresponding PD-sets for the codes are given in Proposition 6.

Proposition 5. *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 the graph 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. By Lemma 1 of [8], we have $\mathrm{Aut}(\Gamma_n) = \mathrm{Aut}(\mathcal{D})$. Because $\mathrm{Aut}(\mathcal{D}) \subseteq \mathrm{Aut}(C_p(G_n))$, we only need to show that $\mathrm{Aut}(C_p(G_n)) \subseteq \mathrm{Aut}(\mathcal{D})$.

Case (i) p odd.

By Proposition 3, if p is odd then minimum words of $C_p(G_n)$ are scalar multiples of the 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 $v^{\overline{(ab,a)}}$ there exists an incidence vector $v^{\overline{(a'b',a')}}$ such that $\rho(v^{\overline{(ab,a)}}) = v^{\overline{(a'b',a')}}$. 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 3, minimum words of the binary codes are the rows of G_n and codewords of the form $\sum_{x \neq a} v^{\overline{(ax,a)}}$ 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 $\sum_{x \neq a} v^{\overline{(ax,a)}}$.

Let

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

A fixed element $[(ab,a),(ab,b)]$ of S_a is also in the support S_b of $\sum_{x \neq b} v^{\overline{(bx,b)}}$. This holds for every element of S_a. Therefore minimum words of the form $\sum_{x \neq a} v^{\overline{(ax,a)}}$ are pairwise commonly incident. This property is not satisfied by the 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 $\sum_{x \neq a} v^{\overline{(ax,a)}}$ 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 $\mathrm{Aut}(C_2(G_n) \subseteq \mathrm{Aut}(\mathcal{D})$. This completes the proof. □

Proposition 6. *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 the graph Γ_n. Let $A_1 = \{[(an,a),(ak,a)]|k \neq a,n\}$, $A_2 = \{[(bn,n),(bn,b)]|b \neq n\}$, $A_3 = \{[((n-1)n,n),(cn,n)]|c \neq n-1,n\}$.*

(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 (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

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

where I is the identity matrix of size $(n-1) \times (n-1)$ 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.

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

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 identity matrix of size $(n-2) \times (n-2)$ 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

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

Excluding the last row from consideration, columns with the identity matrices are 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 $A_4 = \{[(dn, n), (en, n)] | d, e \neq n-1, n\}$, $A_5 = \{[(fg, g), (fg, f)] | f, g \neq n\}$, $A_6 = \{[(hl, l), (jl, l)] | j, h, l \neq n\}$. 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 $t \leq \lfloor (n-2)/2 \rfloor$ errors occur. Let $\mathcal{E}$ be the set of error coordinates of y. There are three possible cases.

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

(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 $1 \leq i \leq 5$. Then $2\sum n_i \leq n-2$. 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

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

Since $2\sum n_i \leq n-2$, we have $|\mathcal{T}| \leq n-2$. 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 $\mathcal{C}$.

(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

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

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. In this case, 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 $1 \leq y \leq n-4$. □

References

[1] B. Andrásfai, *Graph Theory: Flows, Matrices*, New York: Taylor and Francis, 1991.

[2] E.F. Assmus 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] J.A. Bondy and U.S.R. Murty, *Graph Theory*, Vol. 244, Graduate Texts in Mathematics, Springer, 2008.

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

[5] W. Fish, *Codes from uniform subset graphs and cycle products*, PhD thesis, University of the Western Cape, 2007.

[6] W. Fish, R. Fray and E. Mwambene, Binary codes from the complements of the triangular graphs, *Quaest. Math.*, **33** (2010), 399-408.

[7] W. Fish, J.D. Key and E. Mwambene, Codes, designs and groups from the Hamming graphs, *J. Comb. Inf. Syst. Sci.*, **34** (2009), 169-182.

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

[9] Z. Füredi, Graphs of diameter 3 with the minimum number of edges, *Graphs Combin.*, **6** (1990), 333-337.

[10] D. M. Gordon, Minimal permutation sets for decoding the binary Golay codes, *IEEE Trans. Inform. Theory*, **28** (1982), 541-543.

[11] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge: Cambridge University Press, 2003.

[12] J.D. Key, Permutation decoding: an update, url: `www.ces.clemson.edu/~keyj/Key/PDupdate.pdf`, 2003.

[13] 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.

[14] J.D. Key, J. Moori and B.G. Rodrigues, Codes associated with triangular graphs and permutation decoding, *Int. J. Information and Coding Theory*, **1** (2010), 334-349.

[15] 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.

[16] K. Kumwenda and E. Mwambene, Codes from graphs related to the categorical product of triangular graphs and K_n, *Proceedings of IEEE Information Theory Workshop*, Dublin, Ireland, 2010.

[17] F.J. MacWilliams and N.J. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: New Holland, 1977.

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

[19] B.G. Rodrigues, *Codes of Designs and Graphs from Finite Simple Groups*, PhD Thesis, University of Natal, 2003.