Graphs, designs and codes related to the n-cube

W. Fish, J.D. Key and E. Mwambene*
Department of Mathematics and Applied Mathematics
University of the Western Cape
7535 Bellville, South Africa

August 22, 2008

Abstract

For integers $n \geq 1, k \geq 0$, and $k \leq n$, the graph Γ_n^k has vertices the 2^n vectors of $\mathbb{F}_2^n$ and adjacency defined by two vectors being adjacent if they differ in k coordinate positions. In particular Γ_n^1 is the n-cube, usually denoted by Q_n. We examine the binary codes obtained from the adjacency matrices of these graphs when $k = 1, 2, 3$, following results obtained for the binary codes of the n-cube in Fish [6] and Key and Seneviratne [12]. We find the automorphism groups of the graphs and of their associated neighbourhood designs for $k = 1, 2, 3$, and the dimensions of the ternary codes for $k = 1, 2$. We also obtain 3-PD-sets for the self-dual binary codes from Γ_n^2 when $n \equiv 0 \pmod 4$, $n \geq 8$.

1 Introduction

In Fish [6] and Key and Seneviratne [12], the binary codes obtained from the row span over $\mathbb{F}_2$ of an adjacency matrix for the n-cube Q_n were examined, and the codes in the case of n even found to be self-dual with minimum weight n. Further, 3-PD-sets were found in [12] for partial permutation decoding. The n-cubes belong to the class of graphs Γ_n^k, for $n \geq 1, k \geq 0$ integers and $k \leq n$, with vertices the 2^n vectors of $\mathbb{F}_2^n$ and adjacency defined by two vectors being adjacent if they differ in k coordinate positions. The n-cube is Γ_n^1, which is also a Hamming graph, $H(n, 2)$.

In this paper we will examine the binary codes from an adjacency matrix for the graphs Γ_n^k for $k = 2, 3$. We show that for $n \equiv 0 \pmod 4$ the codes from Γ_n^2 are self-dual and, when the same point ordering is used, distinct from those from the n-cube $\Gamma_n^1 = Q_n$: see Proposition 1, Lemma 3 and Proposition 8. We obtain the dimensions of these codes, and also those of the ternary codes for Γ_n^1 and Γ_n^2: see Propositions 6, 7. The automorphism groups of the codes (see Section 2 for our terminology) contain those of the defining graph and design; we identify the groups of the graphs and designs in Propositions 3, 4.

We summarize in a theorem what we have found for the dimensions of the binary codes for $k = 1, 2, 3$, including the result for the binary codes for $k = 1$ for completeness (see Result 2). We also include our results on the ternary codes for $k = 1, 2$, noting that the ternary codes for $k = 3$ seem to be quite different and to merit separate study. We include our results on the automorphism groups of the graphs and designs. In the theorem we have used the same point ordering for the vectors of $\mathbb{F}_2^n$ for the graphs Γ_n^k for distinct k in order to compare the codes.

*E-mail: wfish@uwc.ac.za, keyj@clemson.edu, emwambene@uwc.ac.za

Theorem 1 *For integers $n \geq 1, k \geq 0$, and $n \geq k$, let Γ_n^k denote the graph with vertices the 2^n vectors of $\mathbb{F}_2^n$ and adjacency defined by two vectors being adjacent if they differ in k coordinate positions. Let $C_p(\Gamma_n^k)$ denote the p-ary code obtained by the row span of an adjacency matrix for Γ_n^k over $\mathbb{F}_p$ where p is a prime. Let $\mathcal{D}_n^k$ denote the 1-design with points the vertices of Γ_n^k and blocks given by the set of neighbours of each vertex.*

1. *For $p = 2$:*

   (a) *$C_2(\Gamma_n^1)$ has dimension 2^n for n odd, and dimension 2^{n-1} for n even. Further, the code is self-dual and has minimum weight n if n is even.*

   (b)
$$\dim(C_2(\Gamma_n^2)) = \begin{cases} 2^{n-1} & \text{for } n \equiv 0 \pmod 4 \\ 2^n & \text{for } n \equiv 2, 3 \pmod 4 \\ 2^{n-1} - 2^{\frac{n-1}{2}} & \text{for } n \equiv 1 \pmod 4 \end{cases}$$

   Furthermore, $C_2(\Gamma_n^2)$ is self-dual for $n \equiv 0 \pmod 4$, self-orthogonal for $n \equiv 1 \pmod 4$. For $n \equiv 0 \pmod 4$, $n \geq 8$, $\dim(C_2(\Gamma_n^1) \cap C_2(\Gamma_n^2)) = 2^{n-2} + 2^{\frac{n}{2}-1}$.

   (c) *For $n \geq 2$,*
$$\dim(C_2(\Gamma_n^3)) = \begin{cases} 2^{n-1} & \text{for } n \equiv 0 \pmod 4,\ C_2(\Gamma_n^3) = C_2(\Gamma_n^1) \\ 2^{n-1} - 2^{\frac{n-1}{2}} & \text{for } n \equiv 1 \pmod 4,\ C_2(\Gamma_n^3) = C_2(\Gamma_n^2) \\ 2^{n-2} - 2^{\frac{n-2}{2}} & \text{for } n \equiv 2 \pmod 4,\ C_2(\Gamma_n^3) \subset C_2(\Gamma_n^1) \\ 2^n & \text{for } n \equiv 3 \pmod 4 \end{cases}$$

2. *For $p = 3$:*

   (a)
$$\dim(C_3(\Gamma_n^1)) = \begin{cases} \frac{2}{3}(2^n - 1) & \text{if } n \text{ is even} \\ \frac{2}{3}(2^n + 1) & \text{if } n \text{ is odd} \end{cases}$$

   (b)
$$C_3(\Gamma_n^2) = \begin{cases} C_3(\Gamma_n^1) & \text{for } n \equiv 0 \pmod 3 \\ C_3(\Gamma_n^1)^\perp & \text{for } n \equiv 1 \pmod 3 \\ \mathbb{F}_3^{2^n} & \text{for } n \equiv 2 \pmod 3 \end{cases}$$

   Furthermore $C \cap C^\perp = \{0\}$ for C any of these ternary codes.

3. *If T denotes the translation group on the vector space $\mathbb{F}_2^n$, T^* the subgroup of T of translations of even weight vectors, and S_n is the symmetric group of degree n, then $\mathrm{Aut}(\Gamma_n^1) = T \rtimes S_n$, and, for $n \geq 6$,*
$$\mathrm{Aut}(\mathcal{D}_n^1) = \mathrm{Aut}(\mathcal{D}_n^2) = \mathrm{Aut}(\Gamma_n^2) = (T^* \rtimes S_n) \wr S_2,$$
   and for $n \geq 8$,
$$\mathrm{Aut}(\mathcal{D}_n^3) = \mathrm{Aut}(\mathcal{D}_n^1),\ \mathrm{Aut}(\Gamma_n^3) = \mathrm{Aut}(\Gamma_n^1).$$

The proof of the theorem follows from the propositions in the following sections. In addition, as in [6, 12], we obtain 2- and 3-PD-sets for the self-dual binary codes from Γ_n^2 in Proposition 5.

Sections 2 and 3 give the necessary background material and definitions. Sections 4 and 5 give the results for the binary codes of Γ_n^k for $k = 1, 2$. Section 6 finds the automorphism groups of the designs and graphs. In Section 7 we find 3-PD-sets for the self-dual binary code of Γ_n^2 when $n \equiv 0 \pmod 4$. Sections 8 and 9 deal with the ternary codes for Γ_n^k for $k = 1, 2$, and the final sections look at the dual codes in the binary and ternary cases.

2 Background and terminology

The notation for designs and codes is as in [1]. An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{J})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{J}$ is a t-(v, k, λ) design, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks. The design is **symmetric** if it has the same number of points and blocks. The **code $C_F(\mathcal{D})$ of the design** $\mathcal{D}$ over the finite field F is the space spanned by the incidence vectors of the blocks over F. If $\mathcal{Q}$ is any subset of $\mathcal{P}$, then we will denote the **incidence vector** of $\mathcal{Q}$ by $\boldsymbol{v^{\mathcal{Q}}}$. If $\mathcal{Q} = \{P\}$ where $P \in \mathcal{P}$, then we will write v^P instead of $v^{\{P\}}$. Thus $C_F(\mathcal{D}) = \langle v^B \mid B \in \mathcal{B} \rangle$, and is a subspace of $F^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to F. If $F = \mathbb{F}_p$ then the **p-rank** of the design, written $\text{rank}_p(\mathcal{D})$, is the dimension of its code $C_F(\mathcal{D})$, which we usually write as $C_p(\mathcal{D})$.

All the codes here are **linear codes**, and the notation $[n, k, d]_q$ will be used for a q-ary code C of length n, dimension k, and minimum weight d, where the **weight $\mathbf{wt}(\boldsymbol{v})$** of a vector v is the number of non-zero coordinate entries. The **distance $\mathbf{d}(\boldsymbol{u}, \boldsymbol{v})$** between two vectors u, v is the number of coordinate positions in which they differ, i.e., $\text{wt}(u - v)$. If $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$, then we write $\boldsymbol{u \cap v = (u_1v_1, \ldots, u_nv_n)}$. A **generator matrix** for C is a $k \times n$ matrix made up of a basis for C, and the **dual** code $C^\perp$ is the orthogonal under the standard inner product $(,)$, i.e. $C^\perp = \{v \in F^n | (v, c) = 0 \text{ for all } c \in C\}$. A code C is **self-dual** if $C = C^\perp$ and, if C is binary, **doubly-even** if all codewords have weight divisible by 4. A **check matrix** for C is a generator matrix for $C^\perp$. The **all-one vector** will be denoted by $\boldsymbol{\jmath}$, and is the vector with all entries equal to 1. Two linear codes of the same length and over the same field are **isomorphic** if they can be obtained from one another by permuting the coordinate positions. An **automorphism** of a code C is an isomorphism from C to C. The automorphism group will be denoted by $\text{Aut}(C)$. Any code is isomorphic to a code with generator matrix in so-called **standard form**, i.e. the form $[I_k \,|\, A]$; a check matrix then is given by $[-A^T \,|\, I_{n-k}]$. The first k coordinates in the standard form are the **information symbols** and the last $n - k$ coordinates are the **check symbols**.

The **graphs**, $\Gamma = (V, E)$ with vertex set V and edge set E, discussed here are undirected with no loops. A graph is **regular** if all the vertices have the same valency. An **adjacency matrix** A of a graph of order n is an $n \times n$ matrix with entries a_{ij} such that $a_{ij} = 1$ if vertices v_i and v_j are adjacent, and $a_{ij} = 0$ otherwise. The **neighbourhood design** of a regular graph is the 1-design formed by taking the points to be the vertices of the graph and the blocks to be the sets of neighbours of a vertex, for each vertex. The **code** of a graph Γ over a finite field F is the row span of an adjacency matrix A over the field F, denoted by $C_F(\Gamma)$ or $C_F(A)$. The dimension of the code is the rank of the matrix over F, also written $\text{rank}_p(A)$ if $F = \mathbb{F}_p$, in which case we will speak of the **p-rank** of A or Γ, and write $C_p(\Gamma)$ or $C_p(A)$ for the code.

Permutation decoding, first developed by MacWilliams [14], involves finding a set of automorphisms of a code called a PD-set. The method is described fully in MacWilliams and Sloane [15, Chapter 16, p. 513] and Huffman [10, Section 8]. In [11] and [13] the definition of PD-sets was extended to that of s-PD-sets for s-error-correction:

Definition 1 *If C is a t-error-correcting code with information set $\mathcal{I}$ and check set $\mathcal{C}$, then a* **PD-set** *for C is a set $\mathcal{S}$ of automorphisms of C which is such that every t-set of coordinate positions is moved by at least one member of $\mathcal{S}$ into the check positions $\mathcal{C}$.*

*For $s \le t$ an s-**PD-set** is a set $\mathcal{S}$ of automorphisms of C which is such that every s-set of coordinate positions is moved by at least one member of $\mathcal{S}$ into $\mathcal{C}$.*

The algorithm for permutation decoding is given in [10] and requires that the generator matrix is in standard form. Thus an information set needs to be known. The property of having a PD-set will not, in general, be invariant under isomorphism of codes, i.e. it depends on the choice of information set. Furthermore, there is a bound on the minimum size of $\mathcal{S}$ (see [8],[18], or [10]):

Result 1 *If $\mathcal{S}$ is a PD-set for a t-error-correcting $[n,k,d]_q$ code C, and $r = n-k$, then*

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

This result can be adapted to s-PD-sets for $s \leq t$ by replacing t by s in the formula.

3 The graphs Γ_n^k and designs $\mathcal{D}_n^k$

The graph Γ_n^k, for n,k integers, $n \geq 1$, $k \geq 0$, and $k \leq n$, has vertices the 2^n vectors of $V_n = \mathbb{F}_2^n$ and adjacency defined by two vectors being adjacent if they differ in k coordinate positions. Thus x is adjacent to y in Γ_n^k if and only if $\mathrm{wt}(x+y) = k$ where $\mathrm{wt}(v)$ denotes the weight of $v \in V_n$. Let $\mathcal{D}_n^k$ be the neighbourhood design for Γ_n^k, i.e. the 1-design with point set V_n and whose block set, denoted by $\mathcal{B}_n^k$, is given by the rows of an adjacency matrix for Γ_n^k, i.e. the neighbours of the vertex defined by each row. This is a symmetric 1-$(2^n, \binom{n}{k}, \binom{n}{k})$ design unless $n = 2k$, in which case there are repeated blocks. We will denote the block of the design $\mathcal{D}_n^k$ defined by $x \in V_n$ by $\bar{x}_k$, so that

$$\bar{x}_k = \{y \mid y \in V_n,\ \mathrm{wt}(x+y) \ = k\}.$$

The adjacency matrix for Γ_n^k is an incidence matrix for the design $\mathcal{D}_n^k$ (including repeated blocks in the $n = 2k$ case). For $k = 1$, Γ_n^1 is also the Hamming graph $H(n,2)$ and the n-cube Q_n.

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

The complement of $v \in V_n$ will be denoted by v_c. Thus $v_c(i) = 1 + v(i)$ for $1 \leq i \leq n$, where $v(i)$ denotes the i^{th} coordinate entry of v. Similarly, for $\alpha \in \mathbb{F}_2$, $\alpha_c = \alpha + 1$. Clearly $v_c = v + \mathbf{2^n} - \mathbf{1}$, i.e. $v_c = v + \boldsymbol{\jmath}_n$, where $\boldsymbol{\jmath}_n$ is the all-one vector of V_n. Then note that

$$\begin{aligned} \overline{(x_c)}_k &= \{y \mid y \in V_n,\ \mathrm{wt}(x+y+\boldsymbol{\jmath}_n) \ = k\} \\ &= \{y \mid y \in V_n,\ \mathrm{wt}(x+y) \ = n-k\} = \bar{x}_{n-k}, \end{aligned}$$

so $\mathcal{D}_n^k = \mathcal{D}_n^{n-k}$.

In this paper we will concentrate on $k = 1,2,3$. For these cases, for $n > 2$, $\mathcal{D}_n^1$ is a 1-$(2^n, n, n)$ symmetric design with the property that two distinct blocks meet in zero or two points and similarly any two distinct points are together on zero or two blocks. Similarly, for $n > 4$, $\mathcal{D}_n^2$ is a 1-$(2^n, \binom{n}{2}, \binom{n}{2})$ symmetric design. We will show in Lemma 3 that any two distinct blocks meet in zero, six or $2(n-2)$ points and dually for any two distinct points. For $n > 6$, $\mathcal{D}_n^3$ is a 1-$(2^n, \binom{n}{3}, \binom{n}{3})$ symmetric design. We will show in Lemma 5 that any two distinct blocks meet in zero, 20, $6(n-4)$ or $(n-2)(n-3)$ points and dually for points.

For the adjacency matrices for the graphs we will **always** (with the exception of Section 7) use the natural ordering of the vectors in $\mathbb{F}_2^n$ according to the ordering of the numbers between 0 and $2^n - 1$, in increasing order. With this ordering we denote the adjacency matrix of Γ_n^k by $M(n,k)$, for $n \geq 1, k \geq 0$ and $n \geq k$. Thus $M(n,0) = I$, the identity matrix, and $M(n,n)$ is the matrix with entries 1 on the reverse diagonal. Using block matrices, we have, for $k \geq 1$, $n \geq 2$,

$$M(n,k) = \begin{bmatrix} M(n-1,k) & M(n-1,k-1) \\ M(n-1,k-1) & M(n-1,k) \end{bmatrix}.$$

Lemma 1 *For any $n \geq 1$, $0 \leq k, l \leq n$, the matrices $M(n,k)$ and $M(n,l)$ commute over any field.*

Proof: This is true for $n = 1$ and all $0 \leq k, l \leq n$. Suppose it is true for some n and all $0 \leq k, l \leq n$. We use block matrices and the easily verified fact that if $X = \begin{bmatrix} X_1 & X_2 \\ X_2 & X_1 \end{bmatrix}$ and $Y = \begin{bmatrix} X_3 & X_4 \\ X_4 & X_3 \end{bmatrix}$, and all the X_i commute, then so do X and Y. Thus for $k, l \leq n$ we have $M(n+1,k)$ and $M(n+1,l)$ commuting by induction. For $l = n+1$ we have

$$M(n+1,k)M(n+1,n+1) = \begin{bmatrix} M(n,k) & M(n,k-1) \\ M(n,k-1) & M(n,k) \end{bmatrix} \begin{bmatrix} M(n,n+1) & M(n,n) \\ M(n,n) & M(n,n+1) \end{bmatrix} =$$

$$\begin{bmatrix} M(n,k) & M(n,k-1) \\ M(n,k-1) & M(n,k) \end{bmatrix} \begin{bmatrix} 0 & M(n,n) \\ M(n,n) & 0 \end{bmatrix},$$

and all the blocks commute, by induction. ■

For any prime p, integers n, k, $C_p(\mathcal{D}_n^k) = C_p(\Gamma_n^k) = C_p(M(n,k))$. A different ordering of the vectors of V_n (points of the design) will give an isomorphic code. We have a specific ordering as defined above so that we can use inductive procedures on the matrices to deduce the rank. We only consider $p = 2, 3$ in this paper but other primes could give interesting codes.

4 Binary codes for Γ_n^2

We will write $A_n = M(n,1)$, $B_n = M(n,2)$ and I for the identity matrix of the appropriate size. Then, for $n \geq 2$,

$$A_n = \begin{bmatrix} A_{n-1} & I \\ I & A_{n-1} \end{bmatrix} \text{ and } B_n = \begin{bmatrix} B_{n-1} & A_{n-1} \\ A_{n-1} & B_{n-1} \end{bmatrix}. \quad (1)$$

In [6, 12] the following result was obtained:

Result 2 *For $n \geq 1$, $C_2(\Gamma_n^1)$ is $[2^n, 2^n, 1]_2$ for n odd, and $[2^n, 2^{n-1}, n]_2$ and self-dual for n even.*

We now look at the binary codes for Γ_n^2, i.e. the row span of B_n over $\mathbb{F}_2$. Thus in this section all the matrices will be over $\mathbb{F}_2$. From Lemma 1, $A_nB_n = B_nA_n$ for all n.

Lemma 2 *For $n \geq 1$,*
(1) $A_n^2 = nI$; *(2)* $B_n^2 = \begin{cases} 0 & \text{if } n \equiv 0,1 \pmod 4 \\ I & \text{if } n \equiv 2,3 \pmod 4 \end{cases}$

Proof: (1) Use induction. It is true for $n = 1$. Assume that for $n \geq 2$, $A_{n-1}^2 = (n-1)I$. Then $A_n^2 = \begin{bmatrix} A_{n-1} & I \\ I & A_{n-1} \end{bmatrix}^2 = \begin{bmatrix} A_{n-1}^2 + I & 0 \\ 0 & A_{n-1}^2 + I \end{bmatrix} = nI$ by induction.
(2) $B_n^2 = \begin{bmatrix} B_{n-1} & A_{n-1} \\ A_{n-1} & B_{n-1} \end{bmatrix}^2 = \begin{bmatrix} B_{n-1}^2 & 0 \\ 0 & B_{n-1}^2 \end{bmatrix} + (n-1)I$. Since $B_1^2 = 0$, this gives $B_n^2 = \binom{n}{2}I$, which gives the stated result. ■

If we write $B = B_{n-2}$ and $A = A_{n-2}$, then using elementary row operations over $\mathbb{F}_2$ and $\sim$ to denote row equivalence, for $n \geq 3$,

$$B_n = \begin{bmatrix} B & A & A & I \\ A & B & I & A \\ A & I & B & A \\ I & A & A & B \end{bmatrix} \sim \begin{bmatrix} I & A & A & B \\ A & I & B & A \\ A & B & I & A \\ B & A & A & I \end{bmatrix}. \quad (2)$$

Proposition 1 *For $n \geq 1$,*

$$\mathrm{rank}_2(B_n) = \begin{cases} 2^{n-1} & \text{for } n \equiv 0 \pmod 4 \\ 2^{n-1} - 2^{\frac{n-1}{2}} & \text{for } n \equiv 1 \pmod 4 \\ 2^n & \text{for } n \equiv 2, 3 \pmod 4 \end{cases}$$

Proof: For $n \equiv 0 \pmod 4$, $n-1 \equiv 3 \pmod 4$, so $A_{n-1}^2 = I$ and $B_{n-1}^2 = I$, by Lemma 2. Also, by Lemma 1, $B_{n-1}A_{n-1} = A_{n-1}B_{n-1}$, so

$$B_n = \begin{bmatrix} B_{n-1} & A_{n-1} \\ A_{n-1} & B_{n-1} \end{bmatrix} \sim \begin{bmatrix} I & A_{n-1}B_{n-1} \\ A_{n-1} & B_{n-1} \end{bmatrix} \sim \begin{bmatrix} I & A_{n-1}B_{n-1} \\ 0 & 0 \end{bmatrix}, \tag{3}$$

which gives the result for $n \equiv 0 \pmod 4$.

For $n \equiv 2, 3 \pmod 4$, B_n is invertible from Lemma 2, so this follows immediately.

For $n \equiv 1 \pmod 4$, we first show that $\mathrm{rank}_2(B_n) = 2^{n-2} + 2\mathrm{rank}_2(B_{n-2} + I)$. Let $B = B_{n-2}$, $A = A_{n-2}$. Using the observation of Equation (2), note that now we have $B^2 = A^2 = I$. Thus, using elementary row operations,

$$B_n \sim \begin{bmatrix} I & A & A & B \\ 0 & 0 & B+I & A+AB \\ 0 & B+I & 0 & A+AB \\ 0 & A+AB & A+AB & 0 \end{bmatrix} \sim \begin{bmatrix} I & A & A & B \\ 0 & B+I & 0 & A+AB \\ 0 & 0 & B+I & A+AB \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

which proves the first assertion.

Now we show that for $n \equiv 3 \pmod 4$, $\mathrm{rank}_2(B_n + I) = 2^{n-2} + 2\mathrm{rank}_2(B_{n-2})$. Here we have $B^2 = 0$, $A^2 = I$ and $(B+I)^2 = I$. Using these and elementary row operations, we get

$$B_n + I = \begin{bmatrix} B+I & A & A & I \\ A & B+I & I & A \\ A & I & B+I & A \\ I & A & A & B+I \end{bmatrix} \sim \begin{bmatrix} I & A & A & B+I \\ 0 & B & 0 & AB \\ 0 & 0 & B & AB \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

as required.

Now we prove the result for $n \equiv 1 \pmod 4$ using induction on n, noting that it is true for $n = 5$. Suppose it is true for $5 \leq k < n$, $k \equiv 1 \pmod 4$.

For $n \equiv 1 \pmod 4$, we have $n-2 \equiv 3 \pmod 4$, and $n-4 \equiv 1 \pmod 4$ so that, by the above two deductions, $\mathrm{rank}_2(B_n) = 2^{n-2} + 2(2^{n-4} + 2(\mathrm{rank}_2(B_{n-4})))$ which can be solved as a recurrence relation or by induction to obtain $\mathrm{rank}_2(B_n) = 2^{n-1} - 2^{\frac{n-1}{2}}$.

This completes the proof of the proposition. ■

Lemma 3 *Let $n \geq 2$. For $x, y \in V_n$, if $\mathrm{wt}(x+y) = 2$, x and y are together in $2(n-2)$ blocks of $\mathcal{D}_n^2$, and if $\mathrm{wt}(x+y) = 4$, x and y are together in six blocks of $\mathcal{D}_n^2$; otherwise they are not together in any block of $\mathcal{D}_n^2$. Further, distinct blocks of $\mathcal{D}_n^2$ meet in $0, 6$ or $2(n-2)$ points.*

For $n \equiv 1 \pmod 4$, $C_2(\Gamma_n^2)$ is self-orthogonal, and for $n \equiv 0 \pmod 4$, $C_2(\Gamma_n^2)$ is self-dual.

Proof: First notice that for points $x, y \in V_n$, for the design $\mathcal{D}_n^2$, if $x, y \in \bar{z}_2$ then $\mathrm{wt}(x+y)$ is 2 or 4. For we have $\mathrm{wt}(x+z) = \mathrm{wt}(y+z) = 2$, so

$$\mathrm{wt}(x+y) = \mathrm{wt}(x+z+y+z) = \mathrm{wt}(x+z) + \mathrm{wt}(y+z) - 2\mathrm{wt}((x+z) \cap (y+z)) = 4 - 2\mathrm{wt}((x+z) \cap (y+z)).$$

For $x \neq y$, clearly $\mathrm{wt}((x+z) \cap (y+z))$ is 0 or 1, since these are weight-2 vectors. So $\mathrm{wt}(x+y)$ is 2 or 4.

If x, y are adjacent in Γ_n^2 then $\mathrm{wt}(x+y) = 2$. We show that x and y are together on $2(n-2)$ blocks of $\mathcal{D}_n^2$. This follows since, without loss of generality, we take $x = (x_1, x_2, x_3, \ldots, x_n)$, $y = (x_1+1, x_2+1, x_3, \ldots, x_n)$, since $\mathrm{wt}(x+y) = 2$. If $\mathrm{wt}(x+z) = \mathrm{wt}(y+z) = 2$, then $z = (x_1, x_2+1, x_3, \ldots, x_{i-1}, x_i+1, x_{i+1} \ldots, x_n)$ or $z = (x_1+1, x_2, \ldots, x_{i-1}, x_i+1, x_{i+1} \ldots, x_n)$ for some i in the range $3 \leq i \leq n$. This gives $2(n-2)$ blocks.

If $x, y \in V_n$ and $\mathrm{wt}(x+y) = 4$, then x, y are together on six blocks of $\mathcal{D}_n^2$. For let $x = (x_1, x_2, x_3, x_4, x_5, \ldots, x_n)$ and $y = (x_1+1, x_2+1, x_3+1, x_4+1, x_5, \ldots, x_n)$. If $x, y \in \bar{z}_2$ then z can only differ from x, y in the first four coordinate positions, which gives $\binom{4}{2} = 6$ possibilities.

Thus two points are together on 0, six or $2(n-2)$ blocks and dually any two blocks meet in 0, six or $2(n-2)$ points. Blocks have size $\binom{n}{2}$ which is even if $n \equiv 0, 1 \pmod 4$. Thus in these cases $C \subseteq C^\perp$, and equality holds for $n \equiv 0 \pmod 4$ since the dimensions of C and $C^\perp$ are the same. ∎

Note: From Lemma 2, $(A_n + I)^2 = 0$ for n odd showing that the binary code from $A_n + I$ is self-orthogonal. We show in [5] that it is a $[2^n, 2^{n-1}, n+1]_2$ self dual code. Similarly $B_n^2 = 0$ for $n \equiv 0, 1 \pmod 4$, and $(B_n + I)^2 = 0$ for $n \equiv 2, 3 \pmod 4$, implies the codes are self-orthogonal. For $n \equiv 2 \pmod 4$, $B_n + I$ gives a self-dual code.

5 Binary codes for Γ_n^3

Now consider the graph Γ_n^3 and its design $\mathcal{D}_n^3$. For $n > 6$, the latter is a symmetric 1-$(2^n, \binom{n}{3}, \binom{n}{3})$ design. Using the natural ordering of the vectors in $V_n = \mathbb{F}_2^n$, as before, if we denote the adjacency matrix for Γ_n^3 by $D_n = M(n,3)$, we have, for $n \geq 2$,

$$D_n = \begin{bmatrix} D_{n-1} & B_{n-1} \\ B_{n-1} & D_{n-1} \end{bmatrix}. \tag{4}$$

With notation as used before for B_n and A_n we have the following lemma. All the matrices here are binary, i.e. over $\mathbb{F}_2$.

Lemma 4 *Over $\mathbb{F}_2$, for $n \geq 1$ odd, $B_n A_n = D_n$; for $n \geq 2$ even, $D_n = B_n A_n + A_n$. Further,*

$$D_n^2 = \begin{cases} I & \text{if } n \equiv 3 \pmod 4 \\ 0 & \text{if } n \equiv 0, 1, 2 \pmod 4 \end{cases}$$

Proof: For the first statement, consider the first row of the product $B_n A_n$ for n odd. This corresponds to the row given by $\bar{0}_2$ multiplied by the columns of A_n. For this one gets $n-1$ for the columns labelled by the e_i, 3 for the columns labelled by the $e_i + e_j + e_k$, and 0 for the rest. Thus if n is odd this row gives the first row of the adjacency matrix for the Γ_n^3 graph, and this clearly follows for the remaining rows, by transitivity. (This can also be proved by induction, using Equation (4).)

If n is even, then writing $B = B_{n-1}$ and $A = A_{n-1}$, we have, since $A^2 = I$,

$$B_n A_n = \begin{bmatrix} B & A \\ A & B \end{bmatrix} \begin{bmatrix} A & I \\ I & A \end{bmatrix} = \begin{bmatrix} AB + A & B + A^2 \\ B + A^2 & AB + A \end{bmatrix} = D_n + A_n.$$

For D_n^2, note that for n even, $D_n^2 = B_n^2 A_n^2 + A_n^2 = 0$ since $A_n^2 = 0$. If $n \equiv 1 \pmod 4$ then $B_n^2 = 0$, so $D_n^2 = 0$. If $n \equiv 3 \pmod 4$ then $D_n^2 = B_n^2 A_n^2 = I$. ∎

Recall that the matrices A_n, B_n and D_n all commute, by Lemma 1.

Proposition 2 *For $n \geq 2$,*

$$\mathrm{rank}_2(D_n) = \begin{cases} 2^{n-1} & \text{for } n \equiv 0 \pmod 4 \text{ and } D_n \sim A_n \\ 2^{n-1} - 2^{\frac{n-1}{2}} & \text{for } n \equiv 1 \pmod 4 \text{ and } D_n \sim B_n \\ 2^{n-2} - 2^{\frac{n-2}{2}} & \text{for } n \equiv 2 \pmod 4 \\ 2^n & \text{for } n \equiv 3 \pmod 4 \end{cases}$$

Proof: For $n \equiv 3 \pmod 4$, D_n is invertible by the lemma.

For $n \equiv 0 \pmod 4$, write $B = B_{n-1}$, $A = A_{n-1}$ and $D = D_{n-1}$. Then $n-1 \equiv 3 \pmod 4$ so $B^2 = A^2 = D^2 = I$ and $D = AB$. Thus

$$D_n = \begin{bmatrix} D & B \\ B & D \end{bmatrix} \sim \begin{bmatrix} I & BD \\ B & D \end{bmatrix} \sim \begin{bmatrix} I & A \\ 0 & 0 \end{bmatrix} \sim A_n.$$

For $n \equiv 2 \pmod 4$, $n-1 \equiv 1 \pmod 4$, so, with the same notation as above, $A^2 = I$ and $D = AB$. So

$$D_n = \begin{bmatrix} D & B \\ B & D \end{bmatrix} = \begin{bmatrix} AB & B \\ B & AB \end{bmatrix} \sim \begin{bmatrix} B & AB \\ 0 & 0 \end{bmatrix},$$

so that $\mathrm{rank}_2(D_n) = \mathrm{rank}_2(B_{n-1}) = 2^{n-2} - 2^{\frac{n-2}{2}}$.

If $n \equiv 1 \pmod 4$, then $n-1 \equiv 0 \pmod 4$, take $B = B_{n-2}$, $A = A_{n-2}$, $D = D_{n-2}$, where $n-2 \equiv 3 \pmod 4$. So $B^2 = A^2 = D^2 = I$, $D = AB$, $DA = B$, and $DB = A$. Then

$$D_n = \begin{bmatrix} D & B & B & A \\ B & D & A & B \\ B & A & D & B \\ A & B & B & D \end{bmatrix} \sim \begin{bmatrix} I & A & A & B \\ 0 & 0 & A+AB & B+I \\ 0 & A+AB & 0 & B+I \\ 0 & B+I & B+I & 0 \end{bmatrix} \sim \begin{bmatrix} I & A & A & B \\ 0 & B+I & 0 & A+AB \\ 0 & 0 & B+I & A+AB \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

which is row equivalent to B_n, from the proof of Proposition 1. ■

Thus the only new binary codes we have from D_n are when $n \equiv 2 \pmod 4$. These are self-orthogonal (as are those from $n \equiv 0, 1 \pmod 4$, as noticed earlier).

Lemma 5 *Let $n \geq 6$. For $x, y \in V_n$, if $\mathrm{wt}(x+y) = 2$, x and y are together in $(n-2)(n-3)$ blocks of $\mathcal{D}_n^3$; if $\mathrm{wt}(x+y) = 4$, x and y are together in $6(n-4)$ blocks of $\mathcal{D}_n^3$; if $\mathrm{wt}(x+y) = 6$, x and y are together in 20 blocks of $\mathcal{D}_n^3$; otherwise they are not together in any block of $\mathcal{D}_n^3$. Further, distinct blocks of $\mathcal{D}_n^3$ meet in $0, 20, 6(n-4)$ or $(n-2)(n-3)$ points.*

For $n \equiv 2 \pmod 4$, $n \geq 6$, $C_2(\Gamma_n^3)$ is self-orthogonal, doubly-even, $C_2(\Gamma_n^3) \subset C_2(\Gamma_n^1)$, and the minimum weight of $C_2(\Gamma_n^3)$ is at least $n+2$.

Proof: As in the Γ_n^2 case, it is easier to count the number of blocks through two points. For $x, y \in \bar{z}_3$, $x \neq y$, $\mathrm{wt}(x+y) = 2, 4, 6$. A simple count shows that if $\mathrm{wt}(x+y) = 6$ then they are together on 20 blocks; if $\mathrm{wt}(x+y) = 4$ they are together on $6(n-4)$ blocks; if $\mathrm{wt}(x+y) = 2$, they are together on $(n-2)(n-3)$ blocks, which gives the result about block intersections.

If $n \equiv 2 \pmod 4$, $D_n^2 = 0$ so the code is self-orthogonal. Further, $\binom{n}{3}$ is even, divisible by 4, so the code is doubly-even. Since $D_n = A_n B_n + A_n$, $D_n A_n = 0$ so $C_2(\Gamma_n^3) \subseteq C_2(\Gamma_n^1)^\perp = C_2(\Gamma_n^1)$. Since the minimum weight of $C_2(\Gamma_n^1)$ for n even is n and $n \equiv 2 \pmod 4$, the minimum weight of $C_2(\Gamma_n^3)$ is at least $n+2$, since it is doubly-even. ■

6 Automorphism groups

We look here at the automorphism groups of the graphs, designs and codes. It is clear that the group of the graph is a subgroup of that of the design which is a subgroup of that of the code. We have not, in general, identified the full automorphism groups of the codes. For any n, we write T for the translation group of order 2^n on V_n, and S_n for the symmetric group acting on the n coordinate positions of the points $v \in V_n$. For each $w \in V_n$, write $T(w)$ for the translation on V_n given by w, i.e. $T(w) : v \mapsto v + w$ for each $v \in \mathbb{F}_2^n$. The identity map will be denoted by $\iota = T(0)$. Then $T = \{T(w) \mid w \in V_n\}$. The group $TS_n = T \rtimes S_n$ acts imprimitively on V_n for $n \geq 4$ with $\{v, v_c\}$, for each $v \in V_n$, a block of imprimitivity (see [12]). It is the automorphism group of the graph $Q_n = \Gamma_n^1$ (see [3, 9, 17]). It is clear that, for all k such that $1 \leq k \leq n$, the group TS_n is a subgroup of $\mathrm{Aut}(\Gamma_n^k)$ and $\mathrm{Aut}(\mathcal{D}_n^k)$, since, for $u \in V_n$, $T(u)$ has the property that if $x, y \in \bar{z}_k$, then $\mathrm{wt}(x + z) = \mathrm{wt}(y + z) = k$, so $\mathrm{wt}(xT(u) + zT(u)) = \mathrm{wt}(x + u + z + u) = \mathrm{wt}(y + u + z + u) = k$, so that $xT(u), yT(u) \in \overline{(z + u)}_k$. Clearly any element in S_n also preserves $\mathrm{wt}(x + y)$. Furthermore, we clearly always have $\mathrm{Aut}(\Gamma_n^k) \leq \mathrm{Aut}(\mathcal{D}_n^k)$.

Proposition 3 *For $n \geq 6$,*

$$\mathrm{Aut}(\mathcal{D}_n^1) = \mathrm{Aut}(\mathcal{D}_n^2) = \mathrm{Aut}(\Gamma_n^2) = (T^* \rtimes S_n) \wr S_2$$

where $T^* = \{T(u) \mid u \in V_n, \mathrm{wt}(u)$ is even$\}$.

Proof: We first show that $\mathrm{Aut}(\mathcal{D}_n^1) = \mathrm{Aut}(\Gamma_n^2)$. Two points x, y are together on a block of $\mathcal{D}_n^1$ if and only if $\mathrm{wt}(x + y) = 2$, and any two points are on exactly two blocks or no blocks of $\mathcal{D}_n^1$. Thus if blocks of $\mathcal{D}_n^1$ are preserved then so are edges of Γ_n^2, and conversely, giving the assertion.

Next we show that if $\sigma \in \mathrm{Aut}(\mathcal{D}_n^2)$ and $n \geq 6$, then $\sigma \in \mathrm{Aut}(\Gamma_n^2)$. For if x and y are on an edge of Γ_n^2 then $\mathrm{wt}(x + y) = 2$, so x, y are together on $2(n - 2)$ blocks of $\mathcal{D}_n^2$, by Lemma 3. Thus $x\sigma, y\sigma$ are together on $2(n - 2)$ blocks of $\mathcal{D}_n^2$. So $\mathrm{wt}(x\sigma + y\sigma)$ is 2 or 4. If $\mathrm{wt}(x\sigma + y\sigma) = 4$ then $x\sigma, y\sigma$ are together on six blocks, by Lemma 3. Now $6 < 2(n - 2)$ for $n \geq 6$, so this is impossible, i.e. $\mathrm{wt}(x\sigma + y\sigma) = 2$ and hence they are on an edge of Γ_n^2.

Finally, to complete the proof, equality of the first three groups follows from the preceding statements, since clearly $\mathrm{Aut}(\Gamma_n^2) \leq \mathrm{Aut}(\mathcal{D}_n^2)$. To prove the final equality, note that Γ_n^2 consists of two connected components, i.e. the vectors of even weight and those of odd weight. The group $T^* \rtimes S_n$ preserves each of these components, and since they can be mapped to one another, the wreath product with S_2 will also act. Equality follows from a result to be found in [7]. ■

Note: The group $(T^* \rtimes S_n) \wr S_2$ also acts imprimitively on the points of the graphs and designs, with the same blocks of imprimitivity as the smaller group $T \rtimes S_n$.

Proposition 4 *For $n \geq 8$,*
(1) $\mathrm{Aut}(\mathcal{D}_n^3) = \mathrm{Aut}(\mathcal{D}_n^1)$; *(2)* $\mathrm{Aut}(\Gamma_n^3) = \mathrm{Aut}(\Gamma_n^1)$.

Proof: We first prove (1). For $n \geq 6$, $\mathrm{Aut}(\mathcal{D}_n^1) = \mathrm{Aut}(\mathcal{D}_n^2) = \mathrm{Aut}(\Gamma_n^2)$, from Proposition 3.

Suppose that $\sigma \in \mathrm{Aut}(\mathcal{D}_n^1)$. Then σ permutes the points of $\mathcal{D}_n^3$. If x, y are distinct points on a block of $\mathcal{D}_n^3$, then $\mathrm{wt}(x + y) = 2, 4, 6$, and conversely, any two points whose sum has weight $2, 4, 6$ are on a block of $\mathcal{D}_n^3$. If $\mathrm{wt}(x + y) = 2$ then x, y are on a block of $\mathcal{D}_n^1$ and hence so are $x\sigma, y\sigma$, and so $\mathrm{wt}(x\sigma + y\sigma) = 2$ and hence they are on a block of $\mathcal{D}_n^3$. If $\mathrm{wt}(x + y) = 4$, then x, y are on a block of $\mathcal{D}_n^2$ and hence so are $x\sigma, y\sigma$, and so $\mathrm{wt}(x\sigma + y\sigma) = 2, 4$, and so they are on a block of $\mathcal{D}_n^3$. If $\mathrm{wt}(x + y) = 6$, then without loss of generality we can take $x = e_1 + e_2 + e_3$, $y = e_4 + e_5 + e_6$. The point $z = e_4$ has $\mathrm{wt}(x + z) = 4$, $\mathrm{wt}(y + z) = 2$. So x and z are on a block of $\mathcal{D}_n^2$, y and z are on a block of $\mathcal{D}_n^1$. Thus $\mathrm{wt}(x\sigma + z\sigma) = 2, 4$ and $\mathrm{wt}(y\sigma + z\sigma) = 2$. This implies that

$$0 < \mathrm{wt}(x\sigma + y\sigma) = \mathrm{wt}(x\sigma + z\sigma) + \mathrm{wt}(y\sigma + z\sigma) - 2i \leq 6,$$

and is even, so $x\sigma, y\sigma$ are on a block of $\mathcal{D}_n^3$. Thus $\sigma \in \mathrm{Aut}(\mathcal{D}_n^3)$.

Now suppose $\sigma \in \mathrm{Aut}(\mathcal{D}_n^3)$. If x, y are in a block of $\mathcal{D}_n^1$, then $\mathrm{wt}(x + y) = 2$ and so they are on a block of $\mathcal{D}_n^3$, and hence so are $x\sigma, y\sigma$. Thus $\mathrm{wt}(x\sigma + y\sigma) = 2, 4, 6$. Now x and y are in $(n-2)(n-3)$ blocks of $\mathcal{D}_n^3$, by Lemma 5, and so $x\sigma$ and $y\sigma$ are together in $(n-2)(n-3)$ blocks of $\mathcal{D}_n^3$. If $\mathrm{wt}(x\sigma + y\sigma) = 2$ then $x\sigma, y\sigma$ are in a block of $\mathcal{D}_n^1$, as required. If $\mathrm{wt}(x\sigma + y\sigma) = 4$ then we must have $6(n-4) = (n-2)(n-3)$, i.e. $n = 5, 6$ which is impossible since $n \geq 8$. If $\mathrm{wt}(x\sigma + y\sigma) = 6$ then $20 = (n-2)(n-3)$ and $n = 7$, again impossible. Thus $\sigma \in \mathrm{Aut}(\mathcal{D}_n^1)$.

Now we prove (2). Let $G = \mathrm{Aut}(\Gamma_n^3)$, $A = \mathrm{Aut}(\Gamma_n^1)$. Then we have already established that $G \geq A$, and, since $G \leq \mathrm{Aut}(\mathcal{D}_n^3)$, that G acts imprimitively on V_n with $\{v, v_c\}$ forming blocks of imprimitivity, for $v \in V_n$. Let $H = G_0$, the stabilizer of 0, the zero vector of V_n, in G. Since $A_0 \cong S_n$, we need to show that H does not contain any non-identity element that fixes $e_1, \ldots, e_n$. Let $\sigma \in H$. We first introduce some notation: for $0 \leq i \leq n$ let

$$\mathcal{W}_i = \{x \mid x \in V_n, \mathrm{wt}(x) = i\}.$$

Further, let $d(x)$, for $x \in V_n$, denote the distance in Γ_n^3 of x from 0. Then $d(x) = d(x\sigma)$ for all x. Since $H \geq S_n$, each $x \in \mathcal{W}_i$ is at the same distance from 0 in the graph Γ_n^3, and we denote this distance by d_i. Thus $d_0 = 0$, $d_3 = 1$, $d_2 = d_4 = d_6 = 2$, and $d_1 = 3$, for example, and $d_i = \frac{1}{3}(i + 2(i \bmod 3))$ in general for $i \neq 1$. For $i \geq 2$, write $i = 3t - j$ where $j = 0, 2, 4$; then $d_i = t$. If

$$\mathcal{S}_t = \{x \mid x \in V_n, d(x) = t\}$$

then $\mathcal{S}_0 = 0$, $\mathcal{S}_1 = \mathcal{W}_3$,

$$\mathcal{S}_t = \mathcal{W}_{3t-4} \cup \mathcal{W}_{3t-2} \cup \mathcal{W}_{3t}$$

for $t \geq 2$, $t \neq 3$ (where some of the $\mathcal{W}_i$ may be empty), and

$$\mathcal{S}_3 = \mathcal{W}_1 \cup \mathcal{W}_5 \cup \mathcal{W}_7 \cup \mathcal{W}_9.$$

So σ fixes the classes $\mathcal{S}_t$, for all t. Before commencing the proof of the proposition, we note that $x \in \mathcal{W}_i$ for $i \geq 3$ has neighbours in $\mathcal{W}_j$ for $j = i+3, i+1, i-1, i-3$ (where some of these sets may be empty, for example if $i > n-3$). For $i = 1$, $x \in \mathcal{W}_1$ has neighbours in $\mathcal{W}_j$ for $j = 2, 4$, i.e. only in the one class $\mathcal{S}_2$, and for $i = 2$, $x \in \mathcal{W}_2$ has neighbours in $\mathcal{W}_j$ for $j = 1, 3, 5$.

We now show that for $n > 7$ all the $\mathcal{W}_i$ are fixed by $H = G_0$. We first show that all the weight classes in $\mathcal{S}_2$ must be fixed and then follow with induction on t for the classes in $\mathcal{S}_t$. We know that $\mathcal{W}_3$ is fixed. The number of weight-3 neighbours of $x \in \mathcal{W}_2$ is $(n-2)(n-3)$, that of $x \in \mathcal{W}_4$ is $6(n-4)$, and that of $x \in \mathcal{W}_6$ is 20. No two of these numbers can be equal for $n \geq 8$, and it follows that these weight classes cannot be interchanged for $n \geq 8$ and so $\mathcal{W}_2, \mathcal{W}_4$ and $\mathcal{W}_6$ are fixed. It then follows that $\mathcal{W}_1$ is fixed, since none of the other $\mathcal{W}_i$ in $\mathcal{S}_3$ have neighbours in only the two weight classes $\mathcal{W}_2$ and $\mathcal{W}_4$. Thus the sets $\mathcal{W}_i$ for $i = 0, 1, 2, 3, 4, 6$ are all fixed. We show that all the $\mathcal{W}_i$ are fixed, using induction and the fact that if $\mathcal{W}_i$ is fixed then its set of neighbouring weight classes is fixed. The fact that each member of $\mathcal{S}_2$ is fixed immediately gives that $\mathcal{W}_i$ is fixed for $i = 5, 7, 9$, i.e. that all members of $\mathcal{S}_3$ are fixed. Suppose that all members of $\mathcal{S}_t$ are fixed, where $t \geq 3$. We use induction on $t \geq 3$. To consider $\mathcal{S}_{t+1}$, we look at the members of $\mathcal{S}_t$ and their neighbours. The neighbours of vectors in $\mathcal{W}_{3t-4}$ are in $\mathcal{W}_i$ where $i = 3(t+1)-4, 3(t-1), 3(t-1)-2, 3(t-1)-4$, which tells us that $\mathcal{W}_{3(t+1)-4}$ is fixed, by induction. The neighbours of vectors in $\mathcal{W}_{3t-2}$ are in $\mathcal{W}_i$ where $i = 3(t+1)-2, 3(t+1)-4, 3(t-1), 3(t-1)-2$, which tells us that $\mathcal{W}_{3(t+1)-2}$ is fixed, by induction. The neighbours of vectors in $\mathcal{W}_{3t}$ are in $\mathcal{W}_i$ where $i = 3(t+1), 3(t+1)-2, 3(t+1)-4, 3(t-1)$, which tells us that $\mathcal{W}_{3(t+1)}$ is fixed, by induction. This covers $\mathcal{S}_{t+1}$, so all the $\mathcal{W}_i$ are fixed.

Let $\sigma \in G_0$. Then σ fixes $\mathcal{W}_1$, so there is an element $\tau \in A_0$ such that $\sigma\tau \in G_{[0,e_1,\ldots,e_n]}$, the pointwise stabilizer. Since $G_0 \geq A_0$, $\tau \in G_0$, so we can take $\sigma \in G_{[0,e_1,\ldots,e_n]}$ and show it must be the identity. Then it will follow that $G_0 = A_0$ and the proof is complete. Suppose then that $\sigma \in G_{[0,e_1,\ldots,e_n]}$. We first show that σ also fixes every weight-2 vector. Let $x = e_1 + e_2$. Then x is a neighbour in Γ_n^3 of e_i for $i = 3, \ldots, n$. We want to show that it is the only common neighbour of this set of points. Suppose w is a neighbour to all these points. Then $\mathrm{wt}(w + e_i) = 3$ for $i = 3, \ldots, n$. So, for $i = 3, \ldots, n$, we have $3 = \mathrm{wt}(w) + 1 - 2\mathrm{wt}(w \cap e_i)$, so $\mathrm{wt}(w) = 2 + 2\mathrm{wt}(w \cap e_i)$. Now $\mathrm{wt}(w \cap e_i)$ is 0 or 1. Suppose $\mathrm{wt}(w \cap e_i) = 1$ for some $i \geq 3$. Then $\mathrm{wt}(w) = 4$, and thus $\mathrm{wt}(w \cap e_i) = 1$ for all $i \geq 3$, so that $\mathrm{wt}(w) \geq n - 2 > 4$, giving a contradiction. So $\mathrm{wt}(w \cap e_i) = 0$ for all $i \geq 3$ and so $w = x$. Since each of the e_i are fixed, this unique common neighbour is also fixed. Thus any weight-2 vector is fixed.

Finally we show that every vector is fixed by σ. We do this by induction on i for $\mathcal{W}_i$. It is true for $i = 1, 2$. If $x \in \mathcal{W}_3$ then it is neighbour to precisely $3(n-3)$ weight-2 vectors, all of which are fixed, and no other weight-3 can be neighbour to this set. Thus every weight-3 vector is fixed. Suppose the result is true for $i = j - 1 \geq 3$, and let $x \in \mathcal{W}_j$. Then x is neighbour to $\binom{j}{3}$ vectors of weight $j - 3$, and no other weight-j can be a neighbour to this set, so by the same argument, x is fixed. Thus σ is the identity and $G = A$. ■

Note: It seems that this argument can be adapted to hold for Γ_n^k for any odd k. It clearly will not work for k even.

7 Permutation decoding for the self-dual $C_2(\Gamma_n^2)$

We will show that the same 2-PD-sets as found in [6] and 3-PD-sets as found in [12] for $C_2(\Gamma_n^1)$ for n even will work for $C_2(\Gamma_n^2)$ for $n \equiv 0 \pmod 4$, $n \geq 8$, although a different information set needs to be chosen. We do not have a formula for the minimum weight of $C_2(\Gamma_n^2)$, although we know it is 2 for $n = 4$, 8 for $n = 8$, and at least 12 for $n = 12$.[1] For $n \geq 16$, using Equation (3) and Lemma 4, we have $B_n \sim \left[\begin{array}{cc} I & D_{n-1} \end{array}\right] \sim \left[\begin{array}{cc} D_{n-1} & I \end{array}\right]$ for $n \equiv 0 \pmod 4$, since $D_{n-1}^2 = I$. Supposing the minimum weight is less than 8, it must be 2,4 or 6. We need only look at sums of one, two or three rows of $\left[\begin{array}{cc} I & D_{n-1} \end{array}\right]$. From Lemma 5 we see that the sum of two blocks of $\mathcal{D}_{n-1}^3$ has weight at least $2(\binom{n-1}{3} - (n-3)(n-4))$ and the sum of three blocks has weight at least $3(\binom{n-1}{3} - 2(n-3)(n-4))$. For $n \geq 12$ the sum of two or three rows of the the equivalent matrices for B_n thus has weight greater than 6, which shows that the minimum weight of $C_2(\Gamma_n^2)$ is at least 8 for $n \geq 12$ and thus the code will always correct three errors for $n \geq 8$.

Lemma 6 *For $n \equiv 0 \pmod 4$, an information set can be obtained for the binary code $C_2(\Gamma_n^2)$ by making the following interchanges between the information and check sets from the natural ordering of the vectors: move $e_1 + e_2 + e_3 + \boldsymbol{\jmath}_n = (0, 0, 0, 1, \ldots, 1)$ and $e_2 + e_3 + \boldsymbol{\jmath}_n = (1, 0, 0, 1, \ldots, 1)$ into the information set, and move $\sum_{i=2}^{n-1} e_i = (0, 1, \ldots, 1, 0)$ and $\sum_{i=1}^{n-1} e_i = (1, \ldots, 1, 0)$ into the check positions.*

[1] We thank John Cannon for computing this lower bound for us.

Proof: In this case, $[B_{n-1} \mid A_{n-1}]$ is a generator matrix for the code, and this is equivalent to $[I \mid B_{n-1}A_{n-1}]$ since $B_{n-1}^2 = I$ by Lemma 2. From Lemma 4 $B_{n-1}A_{n-1}$ is an adjacency matrix for Γ_{n-1}^3. Thus the last two rows of the column for $e_1 + e_2 + e_3 + \boldsymbol{\jmath}_n = (0,0,0,1,\ldots,1) = \mathbf{2^n - 8}$ have entries 0 and 1 respectively, while the last two rows of the column for $e_2+e_3+\boldsymbol{\jmath}_n = (1,0,0,1,\ldots,1) = \mathbf{2^n - 7}$ have entries 1 and 0. Thus the last two columns of I, representing the points $\mathbf{2^{n-1} - 2} = (0,1,\ldots,1,0) = \sum_{i=2}^{n-1} e_i$ and $\mathbf{2^{n-1} - 1} = (1,\ldots,1,0) = \sum_{i=1}^{n-1} e_i$, can be replaced by these columns, preserving the rank, and giving an isomorphic code. ■

For each i such that $1 \le i < n$ let $t_i = (i,n) \in S_n$, i.e. the automorphism of $C_2(\Gamma_n^2)$ defined by the transposition of the coordinate positions. For $n \ge 4$ let

$$\begin{aligned} P_n &= \{t_i \mid 1 \le i \le n-1\} \cup \{\iota\} \\ T_n &= TP_n. \end{aligned}$$

Since the translation group T is normalized by S_n, elements of the form $T(w)t_iT(u)$ are all in T_n, i.e. $\sigma^{-1}T(u)\sigma = T(u\sigma^{-1})$, so that for transpositions t, $tT(u) = T(ut)t$. Let $P_n^* = \{t_{n-1}, \iota\}$ and

$$T_n^* = TP_n^* = T\{t_{n-1}, \iota\}.$$

We will write

$$\begin{aligned} \mathcal{I}_1 &= \{\mathbf{r} \mid 0 \le r \le 2^{n-1} - 3\} = \{(r_1,\ldots,r_{n-1},0) \mid r_i \in \mathbb{F}_2\} \setminus \{(0,1,\ldots,1,0),(1,\ldots,1,0)\} \\ \mathcal{C}_1 &= \{\mathbf{r} \mid 2^{n-1} \le r \le 2^n - 1\} \setminus \{\mathbf{2^n - 8}, \mathbf{2^n - 7}\} \\ &= \{(r_1,\ldots,r_{n-1},1) \mid r_i \in \mathbb{F}_2\} \setminus \{(0,0,0,1,\ldots,1),(1,0,0,1,\ldots,1)\} \\ \mathcal{I}_2 &= \{\mathbf{2^n - 8}, \mathbf{2^n - 7}\} = \{(0,0,0,1,\ldots,1),(1,0,0,1,\ldots,1)\} \\ \mathcal{C}_2 &= \{\mathbf{2^{n-1} - 2}, \mathbf{2^{n-1} - 1}\} = \{(0,1,\ldots,1,0),(1,\ldots,1,0)\}, \end{aligned}$$

and $\mathcal{I} = \mathcal{I}_1 \cup \mathcal{I}_2$, $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$. Write

$$a = \mathbf{2^n - 8} = (0,0,0,1,\ldots,1),\ b = a + 1 = \mathbf{2^n - 7} = (1,0,0,1,\ldots,1),$$

$$\alpha = \mathbf{2^{n-1} - 2} = (0,1,\ldots,1,0),\ \beta = \alpha + 1 = \mathbf{2^{n-1} - 1} = (1,\ldots,1,0).$$

Proposition 5 *With $\mathcal{I}$ as information set, for $n \equiv 0 \pmod 4$, $n \ge 8$, T_n^* is a 2-PD-set of size 2^{n+1} for $C_2(\Gamma_n^2)$, and T_n is a 3-PD-set of size $n2^n$ for $C_2(\Gamma_n^2)$.*

Proof: First consider the case of 2-PD-sets. Let $\mathcal{T} = \{x, y\}$ be a set of two points in V_n. We need to show that there is an element in T_n^* that maps $\mathcal{T}$ into $\mathcal{C}$. We consider the various possibilities for the points in $\mathcal{T}$. If $\mathcal{T} \subseteq \mathcal{C}$ then use ι. Thus suppose at least one of the points is in $\mathcal{I}$ and, by using a translation, suppose that one of the points, say y, is $\mathbf{0}$.

If $x \in \mathcal{I}$, then suppose first that $x \in \mathcal{I}_1$. Then $T((0,\ldots,0,1))$ will work unless $x = (0,0,0,1,\ldots,1,0)$ or $(1,0,0,1,\ldots,1,0)$, in which case $T((0,\ldots,0,1,1))$ will work. If $x \in \mathcal{I}_2$, then $T((1,1,1,0,\ldots,0,1))$ will map y into $\mathcal{C}_1$ and x into $\mathcal{C}_2$.

If $x \in \mathcal{C}$, then suppose first that $x \in \mathcal{C}_1$. Then $x = (x_1,\ldots,x_{n-1},1)$ and $(x_1,\ldots,x_{n-1}) \ne (0,0,0,1,\ldots,1),(1,0,0,1,\ldots,1)$. Then $T((1,\ldots,1,0))$ will map y into $\mathcal{C}_2$ and x to $(x_1+1,\ldots,x_{n-1}+1,1) \in \mathcal{C}_1$ unless $x = (1,1,1,0,\ldots,0,1)$ or $(0,1,1,0,\ldots,0,1)$, in which case $t_{n-1}T((0,\ldots,0,1))$ will work. If $x \in \mathcal{C}_2$, then $T((0,\ldots,0,1))$ will work. This completes the case of the 2-PD-set.

Now let $\mathcal{T} = \{x, y, z\}$ be a set of three points in V_n. We need to show that there is an element in T_n that maps $\mathcal{T}$ into $\mathcal{C}$. We consider the various possibilities for the points in $\mathcal{T}$. If $\mathcal{T} \subseteq \mathcal{C}$ then use ι. Thus suppose at least one of the points is in $\mathcal{I}$ and, by using a translation, suppose that one of the points, say z, is $\mathbf{0}$.

If $\mathcal{T} \subseteq \mathcal{I}$, then suppose first that $x, y \in \mathcal{I}_1$. Then $T((0,\ldots,0,1)$ will work unless x or y is $(0,0,0,1,\ldots,1,0)$ or $(1,0,0,1,\ldots,1,0)$. If x and y are these two points then $T((0,\ldots,0,1,1))$ will work. If x is one of these points and y is not, then $T((0,\ldots,0,1,1)$ will work unless y is $(0,0,0,1,\ldots,1,0,0)$ or $(1,0,0,1,\ldots,1,0,0)$, in which case $T((0,\ldots,0,1,0,1)$ will work.

If $x, y \in \mathcal{I}_2$, then $T((0,1,1,0\ldots,0,1))$ will work. Now suppose $x \in \mathcal{I}_2$, $y \in \mathcal{I}_1$, and suppose $x = (0,0,0,1\ldots 1), y = (y_1,\ldots,y_{n-1},0)$. Then $T((1,1,1,0,\ldots,0,1))$ will work; similarly if $x = (1,0,0,1,\ldots,1)$, then $T((0,1,1,0,\ldots,0,1))$ will work, since in the first case $yT = ((y_1)_c,(y_2)_c,(y_3)_c,y_4\ldots,y_{n-1},1) \notin \mathcal{C}$ only if $yT = a,b$, i.e. $y = \alpha,\beta$, which is impossible.

The other cases for $\mathcal{T}$ involve one or two points in $\mathcal{C}$.

Case (i) $x \in \mathcal{I}_1$ and $y \in \mathcal{C}_1$. Then $x = (x_1,\ldots,x_{n-1},0)$, $y = (y_1,\ldots,y_{n-1},1)$, $x \neq \alpha,\beta$, $y \neq a,b$.

1. Suppose $x = y_c$. Then $\tau = T((x_1,\ldots,x_{n-1},1))$ will have $z\tau = (x_1,\ldots,x_{n-1},1)$, $x\tau = (0,\ldots,0,1)$, $y\tau = (1,\ldots,1,0)$ which will work unless $z\tau = a,b$, i.e. $x = (0,0,0,1,\ldots,1,0)$ or $(1,0,0,1,\ldots 1,0)$. In this case $\sigma = t_{n-1}T((0,1,1,0,\ldots,0,1,1))$ will work.

2. Suppose $x_i = y_i$ for $1 \leq i \leq n-1$. Then $x = (x_1,\ldots,x_{n-1},0)$ and $y = (x_1,\ldots,x_{n-1},1)$. Then if $\tau = T(x_c)$, $z\tau = x_c$, $x\tau = (1,\ldots,1)$, $y\tau = (1,\ldots,1,0)$ are all in $\mathcal{C}$ unless $x_c = a,b$, i.e. $x = (1,1,1,0,\ldots,0)$ or $(0,1,1,0\ldots 0)$. In this case $\sigma = t_{n-1}T((0,\ldots,0,1))$ will work.

3. Suppose there exists i such that $x_i = y_i = 0$, and $x_j \neq y_j$ for some j. Then $\sigma = T((1,\ldots,1))t_i$ will work as long as $x\sigma, y\sigma \neq a$ or b. In this case $t_iT((0,\ldots,0,1))$ or $t_iT((0,1,0\ldots,0,1))$ will work.

4. Suppose there is no i for which $x_i = y_i = 0$, and $x \neq y_c$. If $y = (1,\ldots,1)$ then $T((1,0,\ldots,0,1))$ will do unless $x = (0,0,0,1,\ldots,1,0)$ or $(1,0,0,1,\ldots,1,0)$, in which case $t_{n-1}T((1,\ldots,1,0))$ will work. Otherwise $y_j = 0$ for some j, $1 \leq j \leq n-1$. The possibility $y = (0,\ldots,0,1)$ cannot arise, so $x_i = y_i = 1$ for some $i \leq n-1$ and then $\sigma = t_iT((1,\ldots,1,0))$ will do, unless $x\sigma$ or $y\sigma$ is a,b. If $x\sigma = a$, then $i \geq 4$ and $x = (1,1,1,0,\ldots,0) + \mathbf{2^{i-1}}$, $y = (y_1,y_2,y_3,1,\ldots,1)$, where y_j for $j = 1,2,3$ are not all 0 and not all 1. The translation $T(((y_1)_c,(y_2)_c,(y_3)_c,0,\ldots,0,1))$ will work. If $x\sigma = b$ then $i = 1$ or $i \geq 4$, $x = (1,1,1,0,\ldots,0)$ if $i = 1$, or $x = (0,1,1,0,\ldots,0) + \mathbf{2^{i-1}}$ if $i \geq 4$, and $y = (1,y_2,y_3,1,\ldots,1)$ in either case. Then $T((0,(y_2)_c,(y_3)_c,0,\ldots,0,1))$ will work. Similarly, if $y\sigma = a$ or b, then $y = (1,1,1,0,\ldots,0,1)$ or $(0,1,1,0,\ldots,0,1)$, respectively and $t_{n-1}T(((x_1)_c,(x_2)_c,(x_3)_c,0,\ldots,0,1,1))$ will work.

Case (ii) $x \in \mathcal{I}_1$ and $y \in \mathcal{C}_2$. Then $x = (x_1,\ldots,x_{n-1},0)$ and $y = \alpha$ or β. Then in either case for y, $T((0,\ldots,0,1))$ will work unless $x = (0,0,0,1,\ldots,1,0)$ or $(1,0,0,1,\ldots,1,0)$. In this case, $T((1,\ldots,1))$ will do.

Case (iii) $x \in \mathcal{I}_2$ and $y \in \mathcal{C}_2$. In all the four cases the map $t_{n-1}T(\beta)$ will work.

Case (iv) $x \in \mathcal{I}_2$ and $y \in \mathcal{C}_1$. Then $x = a,b$ and $y = (y_1,\ldots,y_{n-1},1)$. If $x = a$, then $T(\beta)$ will work unless $y = (1,1,1,0,\ldots,0,1)$ or $(0,1,1,0,\ldots,0,1)$, in which case $t_{n-1}T((1,1,1,0,\ldots,0,1))$ will work. Similarly if $x = b$.

Case (v) $x \in \mathcal{C}_2$ and $y \in \mathcal{C}_2$. Then $T((0,\ldots,0,1))$ will do.

Case (vi) $x \in \mathcal{C}_1$ and $y \in \mathcal{C}_2$. Then if $x = (x_1,\ldots,x_{n-1},1)$ and $y = \beta$, $\sigma = T(((x_1)_c,\ldots,(x_{n-1})_c,1))$ will work unless $z\sigma = ((x_1)_c,\ldots,(x_{n-1})_c,1) = a,b$. If it is a, then $x = (1,1,1,0,\ldots,0,1)$, and if b, then $x = (0,1,1,0,\ldots,0,1)$. In either case, $t_{n-1}T((0,\ldots,0,1,1))$ will work. If $y = \alpha$, then, as above, $T((x_1,(x_2)_c,\ldots,(x_{n-1})_c,1))$ will work unless $(x_1,(x_2)_c\ldots,(x_{n-1})_c,1) = a,b$, i.e. $x = (0,1,1,0,\ldots,0,1)$ or $(1,1,1,0,\ldots,0,1)$. The same map $t_{n-1}T((0,\ldots,0,1,1))$ will work.

Case (vii) $x, y \in \mathcal{C}_1$. Then $x = (x_1, \ldots, x_{n-1}, 1)$, $y = (y_1, \ldots, y_{n-1}, 1)$, $\neq a, b$. Then $T(\beta)$ will work unless one or both of x, y are either $u = (1,1,1,0,\ldots,0,1)$ or $v = (0,1,1,0,\ldots,0,1)$. If $x = u$ and $y = v$ then $t_{n-1}T((1,\ldots,1))$ will work. If $x = u$ or v and $y = (1,\ldots,1)$ then $t_{n-1}T((0,\ldots,0,1))$ will work. Thus suppose $x = u$ or v and $y_i = 0$ for some i, but $y \neq u, v$. If there is no $j \geq 4$ for which $x_j = y_j = 0$ then $y = (y_1, y_2, y_3, 1, \ldots, 1)$ where $y_i = 0$ for some $1 \leq i \leq 3$. In this case $t_{n-1}T((y_1)_c, (y_2)_c, (y_3)_c, 0\ldots,0,1)$ will work. Otherwise $y_i = 0$ for some $4 \leq i \leq n-1$. Then $t_iT((0,\ldots,0,1))$ will work unless $y = (0,0,0,1,\ldots,1,0,1,\ldots,1)$ or $(1,0,0,1,\ldots,1,0,1,\ldots,1)$ where the 0 is in the i^{th} position. In this case, $t_iT((1,\ldots,1))$ will work.

This completes all the cases. ■

Note: The combinatorial lower bound for the size of an s-PD-set from Result 1 is 14 for $s = 3$, and 6 for $s = 2$.

8 Ternary codes for Γ_n^1

We now look at the ternary codes from the graph Γ_n^1, i.e. from the design $\mathcal{D}_n^1$. All the spans are now over $\mathbb{F}_3$. We first establish a general result for all the Γ_n^k, $k \geq 1$. Using the notation of Section 3:

Lemma 7 *Over $\mathbb{F}_3$, if $k \geq 0$, $n \geq 1$, then $M^3(n,k) = M(n,k)$, $(M^2(n,k) + I)^2 = I$, and* $\text{rank}_3(M(n,k)) = \text{rank}_3(M^2(n,k))$.

Proof: We prove this by induction on n and $k \leq n$. It is true for $n = 1$ and $k = 0, 1$ since $M(1,1) = A_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $M(1,0) = I$. Suppose by induction that it is true for n and all $0 \leq k \leq n$. Then, writing $M(n+1,k) = M$, $M(n,k) = N$, $M(n,k-1) = L$,

$$M^3 = \begin{bmatrix} N^2 + L^2 & 2NL \\ 2NL & N^2 + L^2 \end{bmatrix} \begin{bmatrix} N & L \\ L & N \end{bmatrix} = \begin{bmatrix} N^3 & L^3 \\ L^3 & N^3 \end{bmatrix} = M,$$

by induction if $k \leq n$. If $k = n+1$, then $M(n+1, n+1)$ is the reverse diagonal matrix, which does have this property.

For the other statements, just notice that $(M^2 + I)^2 = I$, and $\text{rank}_3(M) \geq \text{rank}_3(M^2) \geq \text{rank}_3(M^3) = \text{rank}_3(M)$. ■

We now return to the ternary codes of Γ_n^1, i.e. we take $A_n = M(n,1)$ over $\mathbb{F}_3$.

Lemma 8 *For $n \geq 3$,* $\text{rank}_3(A_n) = 2^{n-1} + \text{rank}_3(A_{n-2})$.

Proof: Writing $A = A_{n-2}$, using $A^3 = A$ and elementary row operations over $\mathbb{F}_3$, we have

$$A_n = \begin{bmatrix} A & I & I & 0 \\ I & A & 0 & I \\ I & 0 & A & I \\ 0 & I & I & A \end{bmatrix} \sim \begin{bmatrix} I & 0 & A & I \\ 0 & I & I & A \\ 0 & I & I+2A^2 & 2A \\ 0 & A & 2A & 0 \end{bmatrix} \sim \begin{bmatrix} I & 0 & 0 & A^2+I \\ 0 & I & A^2+I & 0 \\ 0 & 0 & A & 2A^2 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

This gives the result. ■

Proposition 6 *For $n \geq 1$,*

$$\text{rank}_3(A_n) = \begin{cases} \frac{2}{3}(2^n - 1) & \text{if } n \text{ is even} \\ \frac{2}{3}(2^n + 1) & \text{if } n \text{ is odd} \end{cases}$$

Proof: We can verify directly that the result is true for $n = 1, 2$. Let $n \geq 3$ and write $\text{rank}_3(A_n) = a_n$. Then by Lemma 8 $a_n = 2^{n-1} + a_{n-2}$. Solving this recurrence with $a_1 = a_2 = 2$, gives $a_n = \frac{2}{3}(2^n - 1)$ for n even, $a_n = \frac{2}{3}(2^n + 1)$ for n odd, proving the assertion. ■

Note: 1. Since $\sum_{x \in V_n} v^{\bar{x}} = n\jmath$, it follows that $\jmath \in C_3(\Gamma_n^1)$ for $n \equiv 1, 2 \pmod 3$. Clearly $\jmath \in C_3(\Gamma_n^1)^\perp$ for $n \equiv 0 \pmod 3$.
2. Peeters [16] obtains the p-rank for graphs that include the class of Hamming graphs in a different, more general, way.

9 Ternary codes for Γ_n^2

Now we consider the codes generated by the adjacency matrices B_n of Γ_n^2 over $\mathbb{F}_3$. All spans will now be over $\mathbb{F}_3$ with notation as before. Recall that $A_n^3 = A_n$ and $B_n^3 = B_n$, by Lemma 7.

Lemma 9 *For all $n \geq 1$, $A_n^2 = nI + 2B_n$, $A_nB_n = (n-1)A_n$, and* $B_n^2 = \begin{cases} 2B_n & \text{if } n \equiv 0 \pmod 3 \\ B_n & \text{if } n \equiv 1 \pmod 3 \\ I & \text{if } n \equiv 2 \pmod 3 \end{cases}$

Proof: The proof of the first statement is by induction. It is true for $n = 1$ since $A_1^2 = I$ and $B_1 = 0$. Suppose it is true for all $k < n$. Then

$$A_n^2 = \begin{bmatrix} A_{n-1}^2 + I & 2A_{n-1} \\ 2A_{n-1} & A_{n-1}^2 + I \end{bmatrix} = \begin{bmatrix} 2B_{n-1} + nI & 2A_{n-1} \\ 2A_{n-1} & 2B_{n-1} + nI \end{bmatrix} = 2B_n + nI,$$

as required. The other statements follow from the first. ■

Writing now $B = B_{n-2}$, $A = A_{n-2}$, we have

$$B_n = \begin{bmatrix} B & A & A & I \\ A & B & I & A \\ A & I & B & A \\ I & A & A & B \end{bmatrix} \sim \begin{bmatrix} I & A & A & B \\ 0 & I + 2A^2 & B + 2A^2 & A + 2AB \\ 0 & B + 2A^2 & I + 2A^2 & A + 2AB \\ 0 & A + 2AB & A + 2AB & I + 2B^2 \end{bmatrix}. \tag{5}$$

Proposition 7 *For $n \geq 1$,*

$$\text{rank}_3(B_n) = \begin{cases} \frac{2}{3}(2^n - 1) & \text{for } n \equiv 0 \pmod 6 \text{ and } B_n \sim A_n \\ \frac{2}{3}(2^n + 1) & \text{for } n \equiv 3 \pmod 6 \text{ and } B_n \sim A_n \\ \frac{2}{3}(2^{n-1} - 1) & \text{for } n \equiv 1 \pmod 6 \\ \frac{2}{3}(2^{n-1} + 1) & \text{for } n \equiv 4 \pmod 6 \\ 2^n & \text{for } n \equiv 2 \pmod 3 \end{cases}.$$

Proof: First take $n \equiv 0 \pmod 3$. Then $n - 2 \equiv 1 \pmod 3$, and $B^2 = B$, $AB = 0$, and $A^2 = I + 2B$. By Equation (5), using elementary row operations,

$$B_n \sim \begin{bmatrix} I & A & A & B \\ 0 & B & 2I + 2B & A \\ 0 & 2I + 2B & B & A \\ 0 & A & A & I + 2B \end{bmatrix} \sim \begin{bmatrix} I & 0 & 0 & A^2 + I \\ 0 & I & A^2 + I & 0 \\ 0 & 0 & A & 2A^2 \\ 0 & 0 & 0 & 0 \end{bmatrix} \sim A_n,$$

by the proof of Lemma 8.

For $n \equiv 1 \pmod 3$, $n-2 \equiv 2 \pmod 3$, $n-1 \equiv 0 \pmod 3$, so $B^2 = I$, $A^2 = 2I+2B$, and $AB = A$. By Equation (5),

$$B_n \sim \begin{bmatrix} I & A & A & B \\ 0 & 2I+B & I+2B & 0 \\ 0 & I+2B & 2I+B & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} I & A & A & B \\ 0 & 2I+B & 2B+I & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

and so $\text{rank}_3(B_n) = 2^{n-2} + \text{rank}_3(B_{n-2}+2I)$ for $n \equiv 1 \pmod 3$. Now $B_{n-2}+2I = I + 2A_{n-2}^2$ and

$$A_{n-2}^2 - I = \begin{bmatrix} A_{n-3} & I \\ I & A_{n-3} \end{bmatrix}^2 - \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix} = \begin{bmatrix} A_{n-3}^2 & 2A_{n-3} \\ 2A_{n-3} & A_{n-3}^2 \end{bmatrix} \sim \begin{bmatrix} A_{n-3}^2 & 2A_{n-3} \\ 0 & 0 \end{bmatrix}.$$

So $\text{rank}_3(I + 2A_{n-2}^2) = \text{rank}_3(A_{n-3})$ and this is given by the formula in Proposition 6, giving the stated result.

For $n \equiv 2 \pmod 3$, $B_n^2 = I$ by Lemma 9, so B_n is invertible and hence of full rank. ■

10 The self-dual binary codes

For $n \equiv 0 \pmod 4$, both the codes $C_2(\Gamma_n^1)$ and $C_2(\Gamma_n^2)$ are self-dual, from [12, 6] for the first case, and from Lemma 3, for the second. The graph Γ_n^3 only yields new codes when $n \equiv 2 \pmod 4$, in which case $C_2(\Gamma_n^3)^\perp \supset C_2(\Gamma_n^1)$ by Result 2 and Lemma 5.

Lemma 10 *For $n \geq 4$, $n \equiv 0 \pmod 4$, $C_2(\Gamma_n^1) \neq C_2(\Gamma_n^2)$.*

Proof: Since these are self-dual, we need only show that there are blocks of the designs that do not meet evenly. Thus consider $u = e_1 = (1, 0, \ldots, 0)$ and $w = 0 = (0, 0, \ldots, 0)$ in V_n. Then $|\bar{u}_1 \cap \bar{w}_2)| = n - 1$, which is odd, so $v^{\bar{u}_1} \notin C_2(\Gamma_n^2)$ and so the codes are distinct. ■

Note: For $n = 4$, $C_2(\Gamma_n^2)$ has minimum weight 2; for $n = 8$ it has minimum weight 8 and two types of minimum words: if $\mathcal{P}_1 = \{0, e_1+e_2, e_3+e_4, e_1+e_2+e_3+e_4\}$, $\mathcal{P}_2 = \{0, e_1+e_2+e_7+e_8, e_3+e_4+e_7+e_8, e_1+e_2+e_3+e_4\}$ and if $\mathcal{P}_i^c = \{x_c \mid x \in \mathcal{P}_i\}$, and $\mathcal{S}_i = \mathcal{P}_i \cup \mathcal{P}_i^c$, then $w = v^{\mathcal{S}_i} \in C_2(\Gamma_n^2)$, and $v^{\mathcal{S}_i} \notin C_2(\Gamma_n^1)$, for $i = 1, 2$. This was discovered computationally (using Magma [2, 4]) but can easily be verified by checking that w meets every block of $\mathcal{D}_n^2$ evenly, but for $v = (0, 0, 0, 0, 1, 0, 0, 0)$, $|\mathcal{S}_1 \cap \bar{v}_1| = 1$, and similarly for $\mathcal{S}_2$. Computational results showed that the number of minimum weight words of $C_2(\Gamma_n^1)$ for $n = 8$ is 256, i.e. the incidence vectors of the blocks of the design, and that the minimum weight of $C_2(\Gamma_n^2)$ is 8, and that there are 10080 minimum words, 6720 of the first type, and 3360 of the second, as counting will verify. The intersection of these codes has dimension 72, minimum weight 16, and 1680 minimum words.

Proposition 8 *For $n \geq 4$, $n \equiv 0 \pmod 4$, $\dim(C_2(\Gamma_n^1) \cap C_2(\Gamma_n^2)) = 2^{n-2} + 2^{\frac{n}{2}-1}$.*

Proof: Since $(C_2(\Gamma_n^1) \cap C_2(\Gamma_n^2))^\perp = C_2(\Gamma_n^1)^\perp + C_2(\Gamma_n^2)^\perp = C_2(\Gamma_n^1) + C_2(\Gamma_n^2)$, we consider the row span of the matrices A_n and B_n. Thus, with $A = A_{n-1}$ and $B = B_{n-1}$, $n \equiv 0 \pmod 4$ implies $n - 1 \equiv 3 \pmod 4$ so $A^2 = B^2 = I$ by Lemma 2, and

$$\begin{bmatrix} A_n \\ B_n \end{bmatrix} = \begin{bmatrix} A & I \\ I & A \\ B & A \\ A & B \end{bmatrix} \sim \begin{bmatrix} I & A \\ 0 & B+I \\ 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

By the proof of Proposition 1, $\mathrm{rank}_2(B+I) = 2^{n-3}+2(2^{n-4}-2^{\frac{n-4}{2}}) = 2^{n-2}-2^{\frac{n-2}{2}}$, thus $\dim(C_2(\Gamma_n^1)+C_2(\Gamma_n^2)) = 2^{n-1}+2^{n-2}-2^{\frac{n-2}{2}}$, and it follows that $\dim(C_2(\Gamma_n^1)\cap C_2(\Gamma_n^2)) = 2^{n-2}+2^{\frac{n-2}{2}}$. ■

We can identify some words in $C_2(\Gamma_n^2)$ and in $C_2(\Gamma_n^1)\cap C_2(\Gamma_n^2)$, for $n \equiv 0 \pmod 4$, $n \geq 4$, although we have not yet found the minimum weight of these codes for $n \geq 12$. Similarly, we have found some words in $C_2(\Gamma_n^2)^\perp$ when $n \equiv 1 \pmod 4$, $n \geq 5$, that are of minimum weight in the smallest case. The constructions of these words are similar.

Our words will be constructed as follows: write $\Omega_n = \{1,\ldots,n\}$. For $n \equiv 0 \pmod 4$ let $\{\mathcal{N}_i \mid 1 \leq i \leq \frac{n}{2}\}$ be the partition of Ω_n into 2-subsets given by $\mathcal{N}_i = \{2i-1, 2i\}$ for $1 \leq i \leq \frac{n}{2}$, and let $f_i = e_{2i-1}+e_{2i}$. Let $g = f_1+f_2$. Thus the f_i are weight-2 vectors in V_n and g has weight 4. Let

$$\begin{aligned} U_n &= \langle f_i \mid 1 \leq i \leq \frac{n}{2}\rangle \\ W_n &= \langle \{f_k \mid 3 \leq k \leq \frac{n}{2}\} \cup \{g\}\rangle, \end{aligned}$$

i.e. subspaces of dimension $\frac{n}{2}$ and $\frac{n}{2}-1$, respectively.

For $n \equiv 1 \pmod 4$ we partition up to $n-1$ and define

$$Y_n = \langle f_i \mid 1 \leq i \leq \frac{n-1}{2}\rangle.$$

Thus Y_n is a subspace of V_n of dimension $\frac{n-1}{2}$. With this notation we get:

Proposition 9 *For $n \equiv 0 \pmod 4$, $n \geq 4$, the code $C_2(\Gamma_n^1)\cap C_2(\Gamma_n^2)$ has a word of weight $2^{\frac{n}{2}}$ given by the incidence vector v^{U_n} of the subspace U_n. Further, $C_2(\Gamma_n^2)$ has a word of weight $2^{\frac{n}{2}-1}$ given by the incidence vector v^{W_n} of the subspace W_n.*

For $n \equiv 1 \pmod 4$, $n \geq 5$, $C_2(\Gamma_n^2)^\perp$ has a word of weight $2^{\frac{n-1}{2}}$ given by v^{Y_n}.

Proof: First we deal with the $n \equiv 0 \pmod 4$ case. Notice that U_n is the union of the subspace W_n and the coset f_1+W_n. Thus if we can show that the incidence vector of W_n is in the code $C_2(\Gamma_n^2)$ then its translate by f_1 will also be in $C_2(\Gamma_n^2)$ and hence the incidence vector of U_n will be in $C_2(\Gamma_n^2)$.

For $x \in V_n$ let

$$\begin{aligned} S_x^1 &= \{y \mid y \in U_n, \mathrm{wt}(x+y) = 1\}; \\ S_x^2 &= \{y \mid y \in W_n, wt(x+y) = 2\}. \end{aligned}$$

Then for $z \in U_n$, $S_{(x+z)}^1 = S_x^1 + z$ and for $z \in W_n$, $S_{(x+z)}^2 = S_x^2 + z$. Proving the first of these,

$$S_{(x+z)}^1 = \{y \mid y \in U_n, \mathrm{wt}(x+z+y) = 1\} = \{(r+z) \mid r \in U_n, \mathrm{wt}(x+r) = 1\} = S_x^1 + z.$$

The other follows similarly.

First we show that $v^{U_n} \in C_2(\Gamma_n^1)$, and that U_n is in fact an arc for $\mathcal{D}_n^1$, i.e. blocks of the design meet it in 0 or 2 points. If $x \in V_n$ has even weight then $\bar{x}_1 \cap U_n = \emptyset$. If $x \in V_n$ has odd weight, we can reduce it by adding suitable elements of U_n so that the entries at the coordinate pairs in $\mathcal{N}_i$ are $1,0$ or $0,0$. Thus, without loss of generality, suppose x has this form. Suppose there are i of the first type where $0 \leq i \leq \frac{n}{2}$, and i is odd, since $\mathrm{wt}(x) = i$. For any $y \in U_n$, $\mathrm{wt}(x+y) \geq i$, so if $i \geq 2$, $\bar{x}_1 \cap U_n = \emptyset$. If $i = 1$ then $x = e_j$ for some j, and $\bar{x}_1$ meets U_n in precisely two points. This shows that $v^{U_n} \in C_2(\Gamma_n^1)$, and that U_n is an arc for $\mathcal{D}_n^1$.

Now we prove $v^{W_n} \in C_2(\Gamma_n^2)$. If $x \in V_n$ has odd weight then $\bar{x}_2 \cap U_n = \emptyset$. If $x \in V_n$ has even weight, we can reduce it by adding suitable elements of W_n so that the entries at the coordinate pairs in $\mathcal{N}_i$ for $i \geq 3$ are $1,0$ or $0,0$, and such that the first four entries have r 1's where $0 \leq r \leq 2$. Suppose there are i of the type $1,0$, where $0 \leq i \leq \frac{n}{2} - 2$. Then for $y \in W_n$, $\mathrm{wt}(x+y) \geq i + r$. Thus if $i \geq 3$, $\bar{x}_2 \cap W_n = \emptyset$. If $i = 2$ then we need $r = 0$ for a non-trivial intersection, and we get $|S_x^2| = 4$. If $i = 1$ then $r = 1$ and $|S_x^2| = 2$. If $i = 0$ then $r = 0$ or $r = 2$. In the first case $|S_x^2| = \frac{n}{2} - 2$, which is even, and in the second, $|S_x^2| = 2$. Thus $v^{W_n} \in C_2(\Gamma_n^2)$.

For $n \equiv 1 \pmod 4$, we show that $v^{Y_n} \in C_2(\Gamma_n^2)^\perp$. For $x \in V_n$ we write $T_x = \{y \mid y \in Y_n, \mathrm{wt}(x + y) = 2\}$, and note that as before, for $z \in Y_n$, $T_{(x+z)} = T_x + z$. Thus we can employ the same method of proof as in the previous cases. If $\mathrm{wt}(x)$ is odd, then $\bar{x}_2 \cap Y_n = \emptyset$. If $x \in V_n$ has even weight, we can reduce it by adding suitable elements of Y_n so that the entries at the coordinate pairs in $\mathcal{N}_i$ for $1 \leq i \leq \frac{n-1}{2}$ are $1,0$ or $0,0$. The entry at n is x_n. Suppose x now has i pairs with entries $1,0$, where $0 \leq i \leq \frac{n-1}{2}$. Then for $y \in Y_n$, $\mathrm{wt}(x + y) \geq i$. Thus if $i \geq 3$, $\bar{x}_2 \cap Y_n = \emptyset$. If $i = 2$ then $x_n = 0$ and $|T_x| = 4$. If $i = 1$ then $x_n = 1$ and again $|T_x| = 2$. If $i = 0$ then $x = 0$ and $|T_0| = \frac{n-1}{2}$ which is even for $n \equiv 1 \pmod 4$. Thus $v^{Y_n} \in C_2(\Gamma_n^2)^\perp$. ■

11 The dual codes when $p = 3$

Proposition 10 *Let $C = C_3(\Gamma_n^1)$ or $C_3(\Gamma_n^2)$ for $n \geq 4$. Then $C \cap C^\perp = \{0\}$.*

Further, for $n \equiv 1 \pmod 3$, $C_3(\Gamma_n^1)^\perp = C_3(\Gamma_n^2)$; for $n \equiv 0, 2 \pmod 3$, the minimum weight of $C_3(\Gamma_n^1)^\perp$ is at most $\binom{n}{2} + 1$.

Proof: Recall that $C_3(\Gamma_n^1) = C_3(\Gamma_n^2)$ for $n \equiv 0 \pmod 3$ by Proposition 7.

In both cases we show that $\mathbb{F}_3^{V_n} = C + C^\perp$ by showing that the incidence vector of any point can be written as $u + w$ where $u \in C$ and $w \in C^\perp$, which will prove the assertion.

First let $C = C_3(\Gamma_n^1)$. For brevity, write $0 = (0, \ldots, 0)$ and $\bar{z}$ for $\bar{z}_1$ in this part of the proof. We show that $w = v^0 - \sum_{0 \in \bar{z}} v^{\bar{z}}$ is in $C^\perp$. Since the automorphism group is transitive on points, this will show that all the weight-1 vectors are in $C + C^\perp$.

The blocks containing 0 are the blocks $\bar{e}_i$, so $w = v^0 - \sum_{i=1}^n v^{\bar{e}_i}$. We show that the inner product $(w, v^{\bar{x}}) = 0$ for all blocks $\bar{x}$.

First suppose $0 \in \bar{x}$. Then $\mathrm{wt}(x) = 1$, so $x = e_i$ for some i. Without loss of generality take $x = e_1$. Then

$$(w, v^{\bar{e}_1}) = (v^0, v^{\bar{e}_1}) - \sum_{i=1}^n (v^{\bar{e}_i}, v^{\bar{e}_1}) = 1 - \sum_{i=1}^n (v^{\bar{e}_i}, v^{\bar{e}_1}).$$

Now $(v^{\bar{e}_1}, v^{\bar{e}_1}) = n$ and $(v^{\bar{e}_i}, v^{\bar{e}_1}) = 2$ for $i \neq 1$, since, for each i, $\bar{e}_i = \{0, e_i + e_j \mid j \neq i\}$. So $(w, v^{\bar{e}_1}) = 1 - n - 2(n-1) = 0$.

Now suppose $0 \notin \bar{x}$. For $y \in \bar{x}$, $\mathrm{wt}(x + y) = 1$ and since

$$\mathrm{wt}(x + y) = \mathrm{wt}(x) + \mathrm{wt}(y) - 2\mathrm{wt}(x \cap y) = 1,$$

if $\bar{x}$ meets $\bar{e}_i$ then $y \in \bar{x} \cap \bar{e}_i$ has $\mathrm{wt}(y) = 2$, so $\mathrm{wt}(x) = 2\mathrm{wt}(x \cap y) - 1 \leq 3$ (since $\mathrm{wt}(x \cap y) \leq 2$), and $wt(x)$ is odd. Since $0 \notin \bar{x}$, if $\bar{x}$ meets any of the $\bar{e}_i$ then $\mathrm{wt}(x) = 3$ and $x = e_i + e_j + e_k$ for some distinct i, j, k. Then $\bar{e}_l \cap \bar{x} = \emptyset$ unless $l = i, j, k$, so

$$\sum_{l=1}^n (v^{\bar{e}_l}, v^{\bar{x}}) = (v^{\bar{e}_i}, v^{\bar{x}}) + (v^{\bar{e}_j}, v^{\bar{x}}) + (v^{\bar{e}_k}, v^{\bar{x}}) = 6 = 0.$$

This covers all blocks, so $w \in C^\perp$ for $C = C_3(\Gamma_n^1)$.

Now let $C = C_3(\Gamma_n^2)$. From Proposition 7 we need only consider $n \equiv 1 \pmod 3$. Now $\bar{z}$ will denote $\bar{z}_2$.

Using a similar argument as in the case of Γ_n^1, the blocks containing 0 are the blocks $\overline{e_i + e_j}$, so let

$$w = v^0 - \sum_{0 \in \bar{z}} v^{\bar{z}} = v^0 - \sum_{i \neq j} v^{\overline{e_i+e_j}},$$

where $\bar{z}$ denotes the neighbourhood block of $z \in V_n$ in Γ_n^2, i.e. $\bar{z}_2$. We show that the inner product $(w, v^{\bar{x}}) = 0$ for all blocks $\bar{x}$. Recall that $\overline{e_i + e_j} = \{0, e_i + e_k, e_j + e_k, e_i + e_j + e_k + e_l \mid k, l \neq i, j, k \neq \ell\}$.

As before, let us first suppose that $0 \in \bar{x}$ so that $\mathrm{wt}(x) = 2$, and $x = e_i + e_j$ for some $i \neq j$. Without loss of generality take $x = e_1 + e_2$. Notice that

$$\overline{e_1 + e_2} = \{0, e_1 + e_i, e_2 + e_i, e_1 + e_2 + e_i + e_j \mid i, j \neq 1, 2, i \neq j\}.$$

Then $(v^{\bar{x}}, v^{\bar{x}}) = \binom{n}{2} = 0$ since $n \equiv 1 \pmod 3$.

$$\overline{e_1 + e_2} \cap \overline{e_1 + e_3} = \{0, e_1 + e_i, e_2 + e_3, e_1 + e_2 + e_3 + e_i \mid i \neq 1, 2, 3\},$$

of size $2(n-2)$. There are $2(n-2)$ blocks of the form $\overline{e_1 + e_i}$ or $\overline{e_2 + e_i}$, $i \neq 1, 2$, so $4(n-2)^2 = 1$ is the contribution to the inner product from these blocks.

$$\overline{e_1 + e_2} \cap \overline{e_3 + e_4} = \{0, e_1 + e_3, e_1 + e_4, e_2 + e_3, e_2 + e_4, e_1 + e_2 + e_3 + e_4\}$$

of size 6, so these blocks do not contribute to the inner product. Thus we have, for $0 \in \bar{x}$, $(w, v^{\bar{x}}) = 1 - 1 = 0$, as required.

If $0 \notin \bar{x}$ then $\mathrm{wt}(x) \neq 2$. Every y in Support(w) has weight 0,2 or 4. If y is also in $\bar{x}$ then $\mathrm{wt}(x+y) = 2 = \mathrm{wt}(x) + \mathrm{wt}(y) - 2\mathrm{wt}(x \cap y)$, and taking $\mathrm{wt}(y)$ to be 2 or 4 gives $\mathrm{wt}(x) = 2 + 2\mathrm{wt}(x \cap y) - \mathrm{wt}(y)$. Thus $\mathrm{wt}(x)$ is even and at most 6. If $x = 0$ then $\bar{x} \cap \overline{e_i + e_j} = 2(n-2)$ for each pair i, j, and each occurs $\binom{n}{2}$ times, thus giving $(w, v^{\bar{x}}) = 0$.

If $\mathrm{wt}(x) = 4$, then taking $x = \sum_{i=1}^4 e_i$, we have $\bar{x} \cap \overline{e_i + e_j} = \emptyset$ if i or $j \neq 1, 2, 3, 4$. Also

$$\bar{x} \cap \overline{e_1 + e_5} = \{e_1 + e_2, e_1 + e_3, e_1 + e_4, e_1 + e_5 + e_2 + e_3, e_1 + e_5 + e_2 + e_4, e_1 + e_5 + e_3 + e_4\}$$

of size 6, so these blocks make no contribution, and

$$\bar{x} \cap \overline{e_1 + e_2} = \{e_1 + e_3, e_1 + e_4, e_2 + e_3, e_2 + e_4, e_1 + e_2 + e_3 + e_i, e_1 + e_2 + e_4 + e_i \mid i \neq 1, 2, 3, 4\},$$

of size $4 + 2(n-4) = 2(n-2)$. There are $\binom{4}{2} = 6$ choices of these so they also cancel in the inner product, giving $(w, v^{\bar{x}}) = 0$.

If $\mathrm{wt}(x) = 6$, taking $x = \sum_{i=1}^6 e_i$ say, then only blocks of the form $\overline{e_i + e_j}$ for $1 \leq i, j \leq 6$ intersect $\bar{x}$; for example,

$$\bar{x} \cap \overline{e_1 + e_2} = \{e_1 + e_2 + e_i + e_j \mid 3 \leq i, j \leq 6\}$$

has size $\binom{4}{2} = 6$, and thus does not contribute to the inner product. This completes the proof that $w \in C^\perp$ for $C = C_3(\Gamma_n^2)$. Thus $C \cap C^\perp = \{0\}$ for $C = C_3(\Gamma_n^k)$, $k = 1, 2$.

For the remaining assertions, notice that, from Lemma 9, $A_n B_n = 0$ for $n \equiv 1 \pmod 3$, so $C_3(\Gamma_n^1)^\perp \supseteq C_3(\Gamma_n^2)$. Since they have the same dimensions, they are equal. For the final assertion, we have, for $n \equiv 0, 2 \pmod 3$, $w = v^0 - \sum_{z \in \bar{0}_1} v^{\bar{z}_1} \in C_3(\Gamma_n^1)^\perp$ has weight $\binom{n}{2} + 1$. ■

Table 1 shows the minimum weight of $C_3(\Gamma_n^1)$ for small values of n that were computable easily with Magma. The supports of words in the dual were of the form a subspace of V_n (with coordinate

n	Dim(C)	Dim(Dual(C))	MW(C)	MW(Dual(C))
3	6	2	2	4
4	10	6	2	4
5	22	10	4	8
6	42	22	4	8
7	86	42	7	16

Table 1: Minimum weight for $C_3(\Gamma_n^1)$, small n

value 1) and a translate of the subspace (with coordinate value -1). From Proposition 10 we get the results also for the codes of Γ_n^2. That proposition also gives an upper bound for the minimum weight that, for n large, will be better than a bound given by a subspace of V_n and a translate. Thus we have not pursued the construction of such words, although we have found them to exist in this form for values of n up to $n = 11$.

12 Conclusion

The minimum weight of the codes has not been established in general. This seems to be a hard problem. Similarly, the ternary codes for Γ_n^3 are certainly interesting but as yet we have no general method of finding out more about them.

Acknowledgement

J. D. Key thanks the Department of Mathematics and Applied Mathematics at the University of the Western Cape for their hospitality.

All the authors thank the reviewers for careful reading and constructive suggestions.

References

[1] E. F. Assmus, Jr and J. D. Key. *Designs and their Codes.* Cambridge: Cambridge University Press, 1992. Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).

[2] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symb. Comp.*, 24, 3/4:235–265, 1997.

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

[4] J. Cannon, A. Steel, and G. White. Linear codes over finite fields. In J. Cannon and W. Bosma, editors, *Handbook of Magma Functions*, pages 3951–4023. Computational Algebra Group, Department of Mathematics, University of Sydney, 2006. V2.13, http://magma.maths.usyd.edu.au/magma.

[5] W. Fish, J. D. Key, and E. Mwambene. Binary codes of line graphs from the n-cube. In preparation.

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

[7] Robert Frucht. On the groups of repeated graphs. *Bull. Amer. Math. Soc.*, 55:418–420, 1949.

[8] D. M. Gordon. Minimal permutation sets for decoding the binary Golay codes. *IEEE Trans. Inform. Theory*, 28:541–543, 1982.

[9] Frank Harary. The automorphism group of the hypercube. *J.UCS*, 6:136–138, 2000.

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

[11] J. D. Key, T. P. McDonough, and V. C. Mavron. Partial permutation decoding of codes from finite planes. *European J. Combin.*, 26:665–682, 2005.

[12] 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, and V. Ustimenko, editors, *Advances in Coding Theory and Cryptology*, pages 152–159. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2007. Series on Coding Theory and Cryptology, 2.

[13] Hans-Joachim Kroll and Rita Vincenti. PD-sets related to the codes of some classical varieties. *Discrete Math.*, 301:89–105, 2005.

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

[15] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* Amsterdam: North-Holland, 1983.

[16] René Peeters. On the p-ranks of the adjacency matrices of distance-regular graphs. *J. Algebraic Combin.*, 15:127–149, 2002.

[17] Gordon F. Royle. Colouring the cube. Preprint.

[18] J. Schönheim. On coverings. *Pacific J. Math.*, 14:1405–1411, 1964.