Binary codes from the line graph of 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

Abstract

We examine designs and binary codes associated with the line graph of the n-cube Q_n, i.e. the Hamming graph $H(n, 2)$. We find the automorphism groups and the parameters of the codes. We find a regular subgroup of the automorphism group that can be used for permutation decoding, or partial permutation decoding, for any information set.

Key words: Line graph, n-cube, permutation decoding

1. Introduction

Linear codes associated with the Hamming graphs $H(n, m)$ and related graphs were examined, with a view to employing permutation decoding, in (7; 14; 6; 5). They are good candidates for this decoding method since the combinatorial properties of the graphs and related designs can be used to determine the main parameters of the codes, including automorphism groups and information sets. Further, line graphs of various regular graphs were shown to be particularly suitable for permutation decoding: see (15; 13; 22).

We examine here the binary codes from the line graph of the n-cube, Q_n. This is the Hamming graph $H(n, 2)$, where the Hamming graph $H(n, m)$, for n, m integers, has for vertices the m^n n-tuples of R^n, where R is a set of size m, and adjacency is defined by two n-tuples being adjacent if they differ in one coordinate position. The n-cube, Q_n, is $H(n, 2)$ with $R = \mathbb{F}_2$. The line graph of Q_n, denoted by $L(Q_n)$, has for vertices the $2^{n-1}n$ edges of Q_n and adjacency defined by two distinct vertices $[x, y]$ and $[u, w]$ being adjacent, where $x, y, u, w \in V_n = \mathbb{F}_2^n$, if x or y is equal to u or w. The binary code from

Email address: wfish@uwc.ac.za,keyj@clemson.edu,emwambene@uwc.ac.za (W. Fish, J.D. Key and E. Mwambene).

URL: www.math.clemson.edu/~keyj (W. Fish, J.D. Key and E. Mwambene).

Article published in J. Symbolic Comput. 45 (2010) 800–812

the row span over $\mathbb{F}_2$ of an incidence matrix (see Section 2 for the definition of this) for Q_n contains the binary code from the row span of an adjacency matrix of the line graph, and needs to be studied in conjunction with it.

Our main results regarding the binary code from $L(Q_n)$ can be summarized in the following theorem:

Theorem 1. *For $n \geq 2$ let C_1 be the binary code obtained from the span over $\mathbb{F}_2$ of an adjacency matrix for the line graph $L(Q_n)$ of the n-cube, Q_n, and C_2 the binary code spanned by an incidence matrix for Q_n. Then $C_1 \subset C_2$, C_1 is a $[2^{n-1}n, 2^n-2, 2(n-1)]_2$ code, and C_2 is a $[2^{n-1}n, 2^n-1, n]_2$ code. For $n \geq 4$, the minimum words of C_1 and C_2 are the rows of an adjacency, respectively incidence, matrix and the automorphism group of either code is $T \rtimes S_n$, where T is the translation group on $V_n = \mathbb{F}_2^n$, and S_n the symmetric group of degree n acting on the n coordinate positions.*

Further, $C_1^\perp$ and $C_2^\perp$ have minimum weight 4, $C_1 \cap C_1^\perp \supset C_2 \cap C_2^\perp$, and $C_1 \cap C_1^\perp$, respectively $C_2 \cap C_2^\perp$, has dimension 2^{n-1}, respectively $2^{n-1}-1$, and minimum weight at most n^2 for n even, or $n(n-1)$ for n odd.

If E denotes the subgroup of T of translations by even-weight vectors, and g is an n-cycle in S_n, then $E\langle g\rangle$, regular of order $2^{n-1}n$, is a $\lfloor \frac{n}{2} \rfloor$-PD-set for C_1, a PD-set for C_2, and an $(n-1)$-PD-set for $C_i \cap C_i^\perp$, for $i = 1, 2$, for any information set. $\square$

The proof of the theorem will follow from propositions and lemmas in the following sections. Information sets for C_1 and C_2 of Theorem 1 are obtained in Corollary 4, and for the hulls in Corollary 17.

2. Background and terminology

The notation for designs and codes follows (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. An **incidence matrix** $M = [m_{i,j}]$ of $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{J})$ with $|\mathcal{B}| = b$ is a $b \times v$ matrix with rows labelled by the blocks, columns by the points and $m_{i,j} = 1$ if the i^{th} block is incident with the j^{th} point, and $m_{i,j} = 0$ otherwise. A design is **symmetric** if $v = b$. 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. Equivalently, it is the row span of an incidence matrix for the design over F. If $\mathcal{Q} \subseteq \mathcal{P}$, then we denote the **incidence vector** of $\mathcal{Q}$ by $v^{\mathcal{Q}}$, writing v^P if $\mathcal{Q} = \{P\}$ where $P \in \mathcal{P}$. Thus $C_F(\mathcal{D}) = \langle v^B \mid B \in \mathcal{B}\rangle$, and is a subspace of $F^{\mathcal{P}}$. If $F = \mathbb{F}_p$ we write $C_F(\mathcal{D}) = C_p(\mathcal{D})$. The **$p$-rank** of $\mathcal{D}$, written $\text{rank}_p(\mathcal{D})$, is the dimension of $C_p(\mathcal{D})$, i.e. the rank over $\mathbb{F}_p$ of an incidence matrix for $\mathcal{D}$. The **hull** of a design with code C over $\mathbb{F}_p$ is $C \cap C^\perp$, written $\text{Hull}_p(\mathcal{D})$ or simply $\text{Hull}(\mathcal{D})$. A set of points of a design is an **arc** if blocks of the design meet it in at most two points.

We consider only **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** $\text{wt}(v)$ of a vector v (n-tuple) is the number of non-zero coordinate entries. The **distance** $\text{d}(u, v)$ (Hamming distance) between two vectors or n-tuples u, v is the number of coordinate positions in which they differ, i.e. $\text{wt}(u - v)$. If c is a codeword then the **support** of c, $\text{Supp}(c)$, is the set of non-zero coordinate positions of c. 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 **check matrix** for C is a generator matrix for $C^\perp$. A code C is **self-orthogonal** if $C \subseteq C^\perp$ and **self-dual** if $C = C^\perp$. The **all-one vector** will be denoted by $\boldsymbol{\jmath}$, and is the vector with all entries equal to 1. We say that 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. 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 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 $\Gamma = (V, E)$ where $|V| = n$ is an $n \times n$ matrix with entries $a_{i,j}$ such that $a_{i,j} = 1$ if vertices v_i and v_j are adjacent, and $a_{ij} = 0$ otherwise. An **incidence matrix** of Γ is an $n \times |E|$ matrix B with $b_{i,j} = 1$ if the vertex labelled by i is on the edge labelled by j, and $b_{i,j} = 0$ otherwise. The **neighbourhood design**, $\mathcal{D}(\Gamma)$, of a regular graph Γ 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 was introduced by MacWilliams (17) and Prange (19). It involves finding a set of automorphisms of a code, called a PD-set and the method is described fully in standard coding-theory texts: see, for example, MacWilliams and Sloane (18, Chapter 16, p. 513) and Huffman (10, Section 8). In (11) and (16) the definition of PD-sets was extended to that of s-PD-sets for s-error-correction:

Definition 2. 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 $s \leq t$ 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 $\mathcal{C}$. $\square$

The algorithm for permutation decoding is given in (10) and requires that the generator matrix is in standard form. There is a combinatorial bound on the minimum size of $\mathcal{S}$ (see (8),(21), or (10)).

3. The line graph of the n-cube

We write $L(Q_n) = L(H(n,2))$ for the line graph of $H(n,2) = Q_n$. For $x, y \in V_n = \mathbb{F}_2^n$, if x and y are adjacent in $H(n,2)$ (i.e. $\text{wt}(x+y) = 1$), then $[x, y]$ will denote the edge between them, i.e. the 2-set $\{x, y\}$. In $L(Q_n)$, two distinct vertices $[x, y]$ and $[u, w]$ are adjacent if x or y is u or w. As usual, e_i is the i^{th} vector of the canonical basis for V_n. The neighbourhood design $\mathcal{D}(L(Q_n))$ of $L(Q_n)$ has for points the vertices of $L(Q_n)$, i.e. the set $\mathcal{P}_n$ of edges of Q_n, and a block $\overline{[x, y]}$ defined for each point $[x, y] \in \mathcal{P}_n$ by

$$\overline{[x, y]} = \{[x, u] \mid \text{wt}(x+u) = 1, u \neq y\} \cup \{[y, w] \mid \text{wt}(y+w) = 1, w \neq x\}. \qquad (1)$$

This gives a 1-$(2^{n-1}n, 2(n-1), 2(n-1))$ symmetric design $\mathcal{D}(L(Q_n))$ with point set $\mathcal{P}_n$ and block set $\{\overline{[x,y]} \mid [x,y] \in \mathcal{P}_n\}$, which we will denote by $\mathcal{D}_n$.

Let G_n denote the $2^n \times 2^{n-1}n$ vertex by edge incidence matrix of the graph Q_n with the vertices (rows) ordered in the usual standard way by the binary representation of the numbers 0 to $2^n - 1$, writing $m = \sum_{i=0}^{n-1} a_i 2^i = (a_0, a_1, \ldots, a_{n-1})$, where $a_i \in \mathbb{F}_2$ for $0 \leq i \leq n-1$. The columns of G_n, representing the edges of Q_n, are ordered in the following manner: first take $G_1 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$. Now suppose that G_{n-1} has been defined. For G_n we order the rows in the standard way as described. For the columns, the first $2^{n-2}(n-1)$ columns will represent the edges of the graph Q_{n-1}; the next 2^{n-1} columns will represent the edges $[x, x+e_n]$ of Q_n between the first 2^{n-1} vertices and the second 2^{n-1}, starting with the edge $[0, e_n]$, $[e_1, e_1 + e_n]$, $[e_2, e_2 + e_n]$, and so on, i.e. ordered according to the vertices in the first 2^{n-1} set; the final $2^{n-2}(n-1)$ columns will represent the edges between vertices in the second set of vertices, i.e. those with n^{th} coordinate 1.

Example 1. For $n = 3$, the ordering of the rows is

$$0, e_1, e_2, e_1 + e_2, e_3, e_1 + e_3, e_2 + e_3, e_1 + e_2 + e_3,$$

and the ordering of the edges is

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

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

Thus

$$G_3 = \left[\begin{array}{cccc|cccc|cccc} 1&1&0&0&1&0&0&0&0&0&0&0 \\ 1&0&1&0&0&1&0&0&0&0&0&0 \\ 0&1&0&1&0&0&1&0&0&0&0&0 \\ 0&0&1&1&0&0&0&1&0&0&0&0 \\ \hline 0&0&0&0&1&0&0&0&1&1&0&0 \\ 0&0&0&0&0&1&0&0&1&0&1&0 \\ 0&0&0&0&0&0&1&0&0&1&0&1 \\ 0&0&0&0&0&0&0&1&0&0&1&1 \end{array}\right].$$

With this ordering, we see that

$$G_n = \begin{bmatrix} G_{n-1} & I_{2^{n-1}} & 0 \\ 0 & I_{2^{n-1}} & G_{n-1} \end{bmatrix}. \tag{2}$$

If M_n denotes the adjacency matrix of $L(Q_n)$ for $n \geq 2$ with this ordering of edges, and writing $I = I_{2^{n-1}n}$,

$$M_n = G_n^T G_n - 2I = \begin{bmatrix} G_{n-1}^T G_{n-1} & G_{n-1}^T & 0 \\ G_{n-1} & 2I_{2^{n-1}} & G_{n-1} \\ 0 & G_{n-1}^T & G_{n-1}^T G_{n-1} \end{bmatrix} - 2I = \begin{bmatrix} M_{n-1} & G_{n-1}^T & 0 \\ G_{n-1} & 0 & G_{n-1} \\ 0 & G_{n-1}^T & M_{n-1} \end{bmatrix} \tag{3}$$

where

$$G_n^T = \begin{bmatrix} G_{n-1}^T & 0 \\ I_{2^{n-1}} & I_{2^{n-1}} \\ 0 & G_{n-1}^T \end{bmatrix}. \tag{4}$$

Taking G_n as an incidence matrix of a design we get a 1-$(2^{n-1}n, n, 2)$ design which we will denote by $\mathcal{G}_n$. The point set is that of $\mathcal{D}_n$, i.e. $\mathcal{P}_n$, and the block defined by $x \in V_n$ is given by

$$\bar{\bar{x}} = \{[x, x + e_i] \mid 1 \leq i \leq n\}. \tag{5}$$

It is well-known that $\mathrm{Aut}(Q_n) = T \rtimes S_n$ (see (3; 9; 20)), where T is the translation group on $V_n = \mathbb{F}_2^n$ and S_n is the symmetric group acting by permuting the coordinates of vectors in V_n. Thus by Whitney (23), $\mathrm{Aut}(L(Q_n)) = T \rtimes S_n$. The translation by $u \in V_n$ will be denoted by T_u and will act on $L(Q_n)$ by

$$[x, y]T_u = [x + u, y + u]. \tag{6}$$

Clearly $T \rtimes S_n$ acts on all these graphs, designs and codes. Furthermore, it acts transitively on the points, since the point $[0, e_1]$ can be mapped to $[x, x + e_j]$, for arbitrary $x \in V_n$ and $1 \leq j \leq n$, by the transposition $(1, j) \in S_n$ followed by the translation $T_x \in T$.

4. The binary codes

We now consider the binary codes that arise from the graphs and designs described in Section 3. Thus Equation (3) becomes $M_n = G_n^T G_n$. Using the notation from Sections 2 and 3, note that $C_2(L(Q_n)) = C_2(\mathcal{D}_n) = C_2(M_n)$ and $C_2(G_n) = C_2(\mathcal{G}_n)$. In the statement of the theorem in Section 1, we have used $C_1 = C_2(\mathcal{D}_n)$ and $C_2 = C_2(\mathcal{G}_n)$. Notice that, for any $x \in V_n$, $1 \leq i \leq n$,

$$v^{\overline{[x,x+e_i]}} = v^{\bar{\bar{x}}} + v^{\overline{\overline{x+e_i}}}, \tag{7}$$

using the notation of Equations (1) and (5) for blocks of $\mathcal{D}_n$ and $\mathcal{G}_n$, since

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

i.e. the symmetric difference of the two blocks of $\mathcal{G}_n$.

For any n, let $W = C_2(G_n^T)$ and define the linear transformation $\tau_n : W \mapsto C_2(M_n)$ defined by $v\tau = vG_n$ for $v \in W$. With this notation we have the following:

Lemma 3. *For $n \geq 1$, $\mathrm{rank}_2(G_n) = 2^n - 1$ and for $n \geq 2$, $\mathrm{rank}_2(M_n) = 2^n - 2$ and the kernel of τ_n is $\langle \boldsymbol{\jmath} \rangle$.* $\square$

Proof. We prove the first part of this by induction, and using Equation (2), noting that $\mathrm{rank}_2(G_1) = 1 = 2 - 1$. Suppose it is true for $n-1$; then from Equation (2) we see that $\mathrm{rank}_2(G_n) = 2^{n-1} - 1 + 2^{n-1} = 2^n - 1$. Notice that if $\jmath$ denotes the all-one vector of length 2^n, then $\jmath G_n = 0$.

Notice that $C_2(M_n) \subseteq C_2(G_n)$, so $\mathrm{rank}_2(M_n) \leq 2^n - 1$. Then since we see from Equation (4) that the sum of the middle block of rows of G_n^T is the vector $\jmath$, we have that $\jmath \in W$ and the kernel of τ_n is $\langle \jmath \rangle$, and so $\dim(C_2(M_n)) = 2^n - 2$. ■

Note 1. In fact it also follows that $C_2(M_n)$ is the code spanned by the differences of the rows of G_n.

Corollary 4. *For $n \geq 3$, using the ordering described above for the columns of the matrix G_n, if the columns in the set of positions*

$$\mathcal{T}_n = \bigcup_{i=2}^{n-1} \{2^{i-2}(i+1) + t \mid 1 \leq t \leq 2^{i-2}(i-1)\},$$

are placed at the end of the matrix G_n, then the first $2^n - 1$ columns will be an information set for $C_2(G_n)$. Furthermore, if the columns in the set of positions $\mathcal{T}_n$ are placed at the end of the matrix M_n, then the first $2^n - 2$ columns will be an information set for $C_2(M_n)$.

The check set $\mathcal{C}_n$ for $C_2(G_n)$ for $n \geq 2$ is thus

$$\mathcal{C}_n = \bigcup_{i=2}^{n} \{[x + e_i, x + e_i + e] \mid [x, x + e] \in \mathcal{P}_{i-1}\} = \bigcup_{i=2}^{n} \mathcal{P}_{i-1} T_{e_i}, \tag{8}$$

where $\mathcal{P}_i$ is the set of vertices of the design $\mathcal{G}_i$. □

Proof. Notice that $\mathcal{T}_n = \mathcal{T}_{n-1} \cup \{2^{n-3}n + t \mid 1 \leq t \leq 2^{n-3}(n-2)\}$, and $\mathcal{T}_3 = \{4\}$, $\mathcal{T}_4 = \{4, 9, 10, 11, 12\}$, and so on.

The proof for $C_2(G_n)$ follows easily from the inductive description of the matrices G_n. Then this is used for $C_2(M_n)$, using Equation (3), by observing that the first $2^{n-1} - 1$ positions will follow from the result for $C_2(G_{n-1})$. The next $2^{n-1} - 1$ are taken from G_{n-1}^T, since this has rank $2^{n-1} - 1$, and any $2^{n-1} - 1$ columns can be chosen. ■

Proposition 5. *For $n \geq 1$, the minimum weight of $C_2(G_n)$ is n and $C_2(G_n)$ is a $[2^{n-1}n, 2^n - 1, n]_2$ code. For $n \geq 3$ the minimum words are the rows of G_n.* □

Proof. The dimension we already have from Lemma 3. We prove the assertion about the minimum weight by induction. The rows of G_n have weight n, so the minimum weight is at most this value. For $n = 1, 2$ the minimum weight is n. For $n = 3$, the minimum weight is 3 and the minimum words are the rows of G_3. So we start our induction at $n = 3$. Suppose both assertions are true for $n-1$. The matrix G_n is partitioned according to Equation (2).

Let w be a non-zero sum of k rows from the first set of 2^{n-1} rows (blocks). Then w is a concatenation of three vectors, w_1, w_2, w_3 from the three block matrices, where $w_1 = \sum_{i \in I} s_i$ for I a set of size k, and s_i is the i^{th} row of G_{n-1}, and $w_2 = v^I$ is a vector of weight $k \geq 1$, and $w_3 = 0$. If $w_1 \neq 0$ then by induction it has weight at least $n-1$, and so $\mathrm{wt}(w) \geq n-1+k > n$ unless $k=1$ and w is a row of G_n . If $w_1 = 0$ then $v^I = \jmath$, of weight $2^{n-1} > n$ for $n \geq 3$. If we take a sum of vectors from the second set of 2^{n-1} rows, we can use the same argument.

Now take k from the first set and ℓ from the second. Then $w_1 = \sum_{i \in I} s_i$, $w_2 = v^I + v^J$, $w_3 = \sum_{j \in J} s_i$, where $|I| = k$, $|J| = \ell$. If $w_1, w_3 \neq 0$ then $\mathrm{wt}(w) \geq 2(n-1) > n$ for $n \geq 3$. Suppose $w_1 = 0$; then $v^I = \jmath$. If $w_3 = 0$ then $v^J = \jmath$ and $w = 0$. If $w_3 \neq 0$ then $\mathrm{wt}(w_3) \geq n-1$. If $w_2 = 0$ then $v^J = v^I = \jmath$, $J = \{1, \ldots, 2^{n-1}\}$, and w_3 is the sum of all the rows of G_{n-1}, and hence $w_3 = 0$. So $w_2 \neq 0$, so that $\mathrm{wt}(w_2) \geq 1$ and $\mathrm{wt}(w) \geq n-1+1 = n$. If $\mathrm{wt}(w) = n$ then $\mathrm{wt}(w_3) = n-1$ and so $w_3 = s_m = \sum_{j \in J} s_i$ for some m, by the induction hypothesis. Thus $v^J + v^m = \jmath$ or 0. Since $w_2 = \jmath + v^J$ has weight 1, we must have $v^J = \jmath + v^m$, and $w_2 = v^m$, so that w is a row of G_n. The case $w_3 = 0, w_1 \neq 0$ is handled similarly. ■

Proposition 6. *For $n \geq 2$, the minimum weight of $C_2(M_n)$ is $2(n-1)$, so $C_2(M_n) = C_2(L(Q_n)) = C_2(\mathcal{D}_n)$ is a $[2^{n-1}n, 2^n - 2, 2(n-1)]_2$ code for $n \geq 2$.*

For $n \geq 4$ the minimum words of $C_2(M_n)$ are the incidence vectors of the blocks of the design, i.e. the rows of M_n. □

Proof. Again we prove this by induction, using Equation (3), and starting at $n = 4$, since we verified the assertions with Magma (2; 4) for $n \leq 4$. The rows of M_n have weight $2(n-1)$, so the minimum weight is at most this value. Suppose it is true for $n-1$ and that the minimum words are the rows of M_{n-1}. A word w in the row-span over $\mathbb{F}_2$ of the matrix M_n will be a concatenation of three parts, corresponding to the block matrices, and we will write these parts as w_1, w_2, w_3. Label the rows corresponding to the matrix blocks as R_i, $i = 1, 2, 3$. Again we consider cases.
(i) $k \geq 1$ rows from R_1.
Here $w_1 = \sum_{i \in I} r_i$, where r_i is the i^{th} row of M_{n-1} and $|I| = k$. Then if g_i is the i^{th} row of G^T_{n-1}, $w_2 = \sum_{i \in I} g_i$ and $r_i = g_i G_{n-1}$. Also $w_3 = 0$. So $w_1 = w_2 G_{n-1}$. So $w_2 \neq 0$ and hence has weight at least 2, since $C_2(G^T_{n-1})$ is an even weight code. If $w_1 \neq 0$ then $\mathrm{wt}(w_1) \geq 2(n-2)$ by the induction hypothesis, and so $\mathrm{wt}(w) \geq 2(n-2) + 2 = 2(n-1)$. If $\mathrm{wt}(w) = 2(n-1)$ then $\mathrm{wt}(w_1) = 2(n-2)$, so that $w_1 = r_m = \sum_{i \in I} r_i$, by the induction hypothesis, and $\mathrm{wt}(w_2) = 2$. So $r_m = g_m G_{n-1} = w_2 G_{n-1}$, and thus $g_m + w_2 = \jmath$ or 0. Both g_m and w_2 have weight 2, so we must have $g_m = w_2$, which means that w is a row of G_n. If $w_1 = 0$ then $w_2 G_{n-1} = 0$ so $w_2 = \jmath$ (by Lemma 3), and $\mathrm{wt}(w) = 2^{n-1} > 2(n-1)$ for $n \geq 4$.
(ii) $k \geq 1$ rows from R_2.
Then $w_1 = w_3 = \sum_{i \in I} s_i \neq 0$, where s_i is the i^{th} row of G_{n-1}, i.e. $s_i = g_i^T$. So $\mathrm{wt}(w) \geq 2(n-1)$ by Proposition 5, with equality only if $w_1 = w_3 = s_m$, i.e. a row of M_n.
(iii) $k \geq 1$ rows from R_3.
This is the same as Case (i).
(iv) $k \geq 1$ rows from R_1 and $j \geq 1$ rows from R_2.
Here $w_1 = \sum_{i \in I} g_i G_{n-1} + \sum_{j \in J} s_j = u + v$, $w_2 = \sum_{i \in I} g_i$, $w_3 = \sum_{j \in J} s_j = v \neq 0$ (since if $v = 0$ we have Case (i)). If $w_2 = 0$ then $u = 0$ and we have Case (ii). So $\mathrm{wt}(w_2) \geq 2$. If $w_1 \neq 0$ then $\mathrm{wt}(w) \geq n-1+2+n-1 > 2(n-1)$ (since $u \in C_2(M_{n-1}) \subset C_2(G_{n-1})$). If $w_1 = 0$ then $u = v \in C_2(M_{n-1})$. Thus $u \neq 0$ and $\mathrm{wt}(w) \geq 2 + 2(n-2) = 2(n-1)$. If $\mathrm{wt}(w) = 2(n-1)$ then $u = v = r_m$, for some m, by induction, so $w_2 = g_m G_{n-1}$ and w

is a row of M_n. The case of k rows from R_2 and ℓ rows from R_3 is handled similarly.
(v) $k \geq 1$ rows from R_1 and $j \geq 1$ rows from R_3.
Here $w_1 = \sum_{i \in I} g_i G_{n-1}$, $w_2 = \sum_{i \in I} g_i + \sum_{j \in J} g_j$, $w_3 = \sum_{j \in J} g_j G_{n-1}$. If $w_1, w_3 \neq 0$ then $\mathrm{wt}(w) \geq 2(n-2) + 2(n-2) > 2(n-1)$ for $n \geq 4$. If $w_1 = 0$ then $\sum_{i \in I} g_i = \boldsymbol{\jmath}$. If $w_2 = 0$ then $\sum_{j \in J} g_j = \boldsymbol{\jmath}$ and hence $w_3 = 0$. Thus $w_2 \neq 0$. Since $w_3 \neq 0$ (otherwise $w = 0$), we have $\mathrm{wt}(w) \geq 2 + 2(n-2) = 2(n-1)$, with equality if and only if $w_3 = g_m G_{n-1}$ for some m, by induction. Then, as before, $\sum_{j \in J} g_j + g_m = \boldsymbol{\jmath}$ or 0. If the former then $w_2 = g_m$, and we get a row of M_n; if 0 then we get $\mathrm{wt}(w_2) > 2$, and hence $\mathrm{wt}(w) > 2(n-1)$, a contradiction. Similarly if $w_3 = 0$.
(vi) $k \geq 1$ rows from R_1, $j \geq 1$ rows from R_2, $\ell \geq 1$ rows from R_3.
Then $w_1 = \sum_{i \in I} g_i G_{n-1} + \sum_{j \in J} s_j = u + v$, $w_2 = \sum_{i \in I} g_i + \sum_{t \in K} g_t$, where $|K| = \ell$, and $w_3 = \sum_{t \in K} g_t G_{n-1} + \sum_{j \in J} s_t = y + v$.

If $w_1, w_3 \neq 0$ then $\mathrm{wt}(w) \geq 2(n-1)$ with equality only if $w_1 = s_m$, $w_3 = s_r$, $w_2 = 0$, for some m, r. Since $w_2 = 0$ we have $\sum_{i \in I} g_i = \sum_{t \in K} g_t$, and so $\sum_{i \in I} g_i G_{n-1} = \sum_{t \in K} g_t G_{n-1}$, i.e. $u = y$ and so $s_m = s_r$ and we have a row of M_n.

If $w_1 = 0$ then $u = v$, so $w_3 = \sum_{t \in K} g_t G_{n-1} + \sum_{i \in I} g_i G_{n-1} = w_2 G_{n-1}$. If $w_3 = 0$ then $w_2 = 0$ or $\boldsymbol{\jmath}$, so for $w \neq 0$, $\mathrm{wt}(w) = 2^{n-1} > 2(n-1)$ for $n \geq 4$. If $w_3 \neq 0$ then $w_2 \neq 0$, so $\mathrm{wt}(w) \geq 2 + 2(n-2)$, with equality if $w_3 = r_m$, for some m, and so $w_3 = r_m = g_m G_{n-1} = w_w G_{n-1}$, so that $w_2 + g_m = \boldsymbol{\jmath}, 0$. Since $\mathrm{wt}(w_2) = 2$, we must have $w_2 = g_m$, and again we have a row of M_n. A similar argument works for $w_3 = 0$.

This completes all the cases and the induction. ■

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

$$u(x, y, z) = v^{[x,y]} + v^{[x,z]} + v^{[x+y+z,y]} + v^{[x+y+z,z]}, \tag{9}$$

where $x \in V_n$, $y = x + e_i$, $z = x + e_j$, $1 \leq i, j \leq n$, $i \neq j$. Further, for $n \geq 3$ $C^\perp$ has minimum weight 4 . □

Proof. Let $S(u(x,y,z)) = \mathrm{Supp}(u(x,y,z)) = \{[x,y], [x,z], [x+y+z,y], [x+y+z,z]\}$. Since $C_2(\mathcal{D}_n) \subseteq C_2(\mathcal{G}_n)$, $C_2(\mathcal{D}_n)^\perp \supseteq C_2(\mathcal{G}_n)^\perp$, so we need only show that every $u(x,y,z) \in C_2(\mathcal{G}_n)^\perp$ and that the minimum weight of $C_2(\mathcal{D}_n)^\perp$ is at least 4 for $n \geq 3$.

Clearly $|\overline{\overline{a}} \cap S(u(x,y,z))|$ is 0 or 2 for any block $\overline{\overline{a}}$ of $\mathcal{G}_n$, proving the first statement. To show that 4 is the minimum weight for $n \geq 3$, note that from Lemma 11 $\boldsymbol{\jmath} \in C$, in both cases for C, so the minimum weight of $C^\perp$ is either 2 or 4. Suppose $C_2(\mathcal{D}_n)^\perp$ has a vector w of weight 2. Since $\mathrm{Aut}(\mathcal{D}_n)$ is transitive on points (see Section 3), we can suppose the support of w is $\{\underline{[0,e_1]}, \overline{[x, x+e]}\}$. Now we just show that for every choice of $\overline{[x, x+e]}$ there is a block $\underline{\overline{[u,v]}}$ that meets $\mathrm{Supp}(w)$ just once. If $\overline{[x, x+e]} = \underline{[0, e_i]}$ or $\underline{\overline{[e_1, e_1+e_i]}}$ where $i \neq 1$, then $\overline{[0, e_1]}$ will do; if $x, x+e \neq 0, e_1$ then $\overline{[x, x+f]}$ or $\overline{[x+e, x+e+f]}$, where f has weight 1, $f \neq e, e_1$, will do. This covers all possibilities. ■

Note 2. The minimum weight of $C_2(\mathcal{G}_2)^\perp$ is also 4, but that of $C_2(\mathcal{D}_2)^\perp$ is 2.

We will need the following lemma concerning intersections of blocks in $\mathcal{D}_n$ in the following section.

Lemma 8. *Blocks of the design $\mathcal{D}_n$ meet in* $0, 1, 2,$ *or* $(n-2)$ *points.* □

Proof. We first solve the dual problem, i.e. we count the number of blocks through two points. Suppose the two points are on a block. Since we have transitivity on blocks, consider the block $\overline{[0, e_1]}$. Then

- $[0, e_i]$ and $[0, e_j]$, where $1, i, j$ are distinct, are on the $(n-2)$ blocks $\overline{[0, e_k]}$ for $k \neq i, j$; similarly, $[e_1, e_1 + e_i]$ and $[e_1, e_1 + e_j]$, where $1, i, j$ are distinct, are on the $(n-2)$ blocks $\overline{[e_1, e_1 + e_k]}$ for $k \neq i, j$; there are $(n-1)(n-2)$ such pairs of points;
- $[0, e_i]$ and $[e_1, e_1 + e_i]$, $i \neq 1$, are on the two blocks $\overline{[0, e_1]}$ and $\overline{[e_1 + e_i, e_i]}$; there are $(n-1)$ such pairs of points;
- $[0, e_i]$ and $[e_1, e_1 + e_j]$, where $1, i, j$ are distinct, are only together on the one block $\overline{[0, e_1]}$; there are $(n-1)(n-2)$ such pairs of points.

Now count the number of blocks that meet $\overline{[0, e_1]}$:

- it meets $\overline{[e_i, e_i + e_j]}$ and $\overline{[e_i + e_1, e_i + e_j + e_i]}$ for $1, i, j$ all distinct, in exactly one point; there are $2(n-1)(n-2)$ of these;
- it meets $\overline{[e_i, e_i + e_1]}$ in two points; there are $(n-1)$ of these;
- it meets $\overline{[0, e_i]}$ and $\overline{[e_1, e_i + e_1]}$, for $i \neq 1$, in $n-2$ points; there are $2(n-1)$ of these.

Thus, in all, it is disjoint from $2^{n-1}n - 1 - (n-1)(2n-1)$ blocks. ■

5. The automorphism groups

As noted in Section 3, $\mathrm{Aut}(L(Q_n)) = T \rtimes S_n$. We now identify the automorphism groups of the designs and codes.

Proposition 9. *For $n \geq 4$, $\mathrm{Aut}(L(Q_n)) = \mathrm{Aut}(\mathcal{D}_n) = \mathrm{Aut}(\mathcal{G}_n) \cong \mathrm{Aut}(Q_n) = T \rtimes S_n$, acting imprimitively of degree $2^{n-1}n$.* □

Proof. We need only prove that $\mathrm{Aut}(L(Q_n)) = \mathrm{Aut}(\mathcal{D}_n)$, by the comment above and since the statement is clear for $\mathrm{Aut}(\mathcal{G}_n)$.

Let $A = \mathrm{Aut}(L(Q_n))$ and $B = \mathrm{Aut}(\mathcal{D}_n)$. We need only show that $\sigma \in B$ implies that $\sigma \in A$. Thus suppose $[x, y]$ and $[z, w]$ are on an edge of $L(Q_n)$. Then we can take $z = x$, and thus $[x, y]$ and $[x, w]$ are together on $n-2$ blocks, from the proof of Lemma 8. Thus $[x, y]\sigma$ and $[x, w]\sigma$ are on $n-2$ blocks. For $n-2 > 2$, i.e. $n \geq 5$, this means that $[x, y]\sigma = [X, Y]$ and $[x, w]\sigma = [X, W]$ and hence that they are on an edge of the line graph. Thus $\sigma \in A$. If $n = 4$ we verified the result using Magma.

Now let $G = \mathrm{Aut}(\mathcal{D}_n)$. We noted that G is transitive in Section 3. To show that the action is imprimitive, let $H = G_{[0,e_1]} \cong \langle T_{e_1} \rangle S_{n-1}$. Then if $S = \langle T_{e_1}, T_{\boldsymbol{\jmath}} \rangle$, we have $G > SS_{n-1} > H$, so H is not maximal. Blocks of imprimitivity are $\{[x, x+e], [x+\boldsymbol{\jmath}, x+e+\boldsymbol{\jmath}]\}$ for $x \in V_n$. ■

Corollary 10. *For $n \geq 4$, $\mathrm{Aut}(C_2(\mathcal{D}_n)) = T \rtimes S_n$; for $n \geq 3$, $\mathrm{Aut}(C_2(\mathcal{G}_n)) = T \rtimes S_n$.* □

Proof. By Proposition 6, for $n \geq 4$ the words of weight $2(n-1)$ of $C_2(\mathcal{D}_n)$ are the incidence vectors of the blocks of $\mathcal{D}_n$. Since an automorphism of the code must preserve the weight classes, it follows that it preserves the blocks, and hence the design.

The same holds for $C_2(\mathcal{G}_n)$ for $n \geq 3$ by Proposition 5. ■

6. The hulls

Recall that for any design $\mathcal{D}$, $\mathrm{Hull}_p(\mathcal{D}) = C_p(\mathcal{D}) \cap C_p(\mathcal{D})^\perp$, written simply $\mathrm{Hull}(\mathcal{D})$ if the prime p is clear from the context. Since $p = 2$ in our context, we will use this latter notation here. The hull is a self-orthogonal code, and it is advantageous to study the hull in conjunction with the code itself: see (1) for applications of this.

In this section we locate some words of low weight in the hulls of the two designs $\mathcal{D}_n$ and $\mathcal{G}_n$ and use these to determine their dimensions.

In the proof of the following lemma we label the vectors of V_n by the numbers $0, 1, \ldots 2^n - 1$ in the usual way, and as described in Section 3. We also use the notation:

$$E_i = \langle e_j \mid j \in \{1, \ldots, n\} \setminus \{i\} \rangle \tag{10}$$

for $1 \leq i \leq n$.

Lemma 11. *For $n \geq 2$, $1 \leq i \leq n$, let*

$$S_i = \{[u, u + e_i] \mid u \in E_i\} \tag{11}$$

$$T_i = \{[e_i + u, e_i + e_{i+1} + u] \mid u \in \langle e_j \mid j \in \{1, \ldots, n\} \setminus \{i, i+1\} \rangle \tag{12}$$

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

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

has weight 2^{n-1}, and is in $\mathrm{Hull}(\mathcal{D}_n)$. Each S_i is an arc in $\mathcal{D}_n$. Furthermore, $\jmath = \sum_{i=1}^n v^{S_i} \in \mathrm{Hull}(\mathcal{D}_n)$, and $v^{S_i} \notin C_2(G_n)^\perp$ for any $1 \leq i \leq n$. $\square$

Proof. We prove this for $i = 1$ where $S = S_1 = \{[2k, 2k+1] \mid 0 \leq k \leq 2^{n-1} - 1\}$ and $T = T_1 = \{[4i+1, 4i+3] \mid 0 \leq i \leq 2^{n-2} - 1\}$, written in terms of the numerals from 0 to $2^n - 1$. The proof will then follow for all i. Let $C = C_2(\mathcal{D}_n)$.

Let $w = \sum_{z \in T} v^{\bar{z}}$ and $W = \mathrm{Supp}(w)$. First show that $S \subseteq W$. Let $P = [2k, 2k+1] \in S$. If $k = 2l$ then $P = [4l, 4l+1] \in \overline{[4l+1, 4l+3]}$ and no other block from T; if $k = 2l+1$ then $P = [4l+2, 4l+3] \in \overline{[4l+1, 4l+3]}$ and no other block from T. Thus $P \in W$.

Notice that all points in $\overline{[4i+1, 4i+3]}$ are of the form $[4i+1, z]$, $[4i+3, u]$ where z and u are odd numbers in the range $[0 \ldots 2^n - 1]$, or either $[4i, 4i+1]$ or $[4i+2, 4i+3]$, i.e. points of S. Thus we need only consider points $[x, y]$ where both x, y are odd, and $y = x + e_j$ where $j \geq 2$. If $y = x + e_2$ then $[x, y]$ will not be in any of the $\overline{[4i+1, 4i+3]}$.

Writing the points in terms of vectors in $V_n = \mathbb{F}_2^n$, $4i + 1 = e_1 + \sum_{k=3}^n \alpha_k e_k$, $4i + 3 = e_1 + e_2 + \sum_{k=3}^n \alpha_k e_k$, and writing $u = \sum_{k=3}^n \alpha_k e_k$, then

$$\overline{[4i+1, 4i+3]} = \{[e_1 + u, e_1 + u + e_k] \mid 3 \leq k \leq n\} \cup \{[e_1 + u, u]\} \cup$$

$$\{[e_1 + e_2 + u, e_1 + +e_2 + u + e_k] \mid 3 \leq k \leq n\} \cup \{[e_1 + e_2 + u, e_2 + u]\}.$$

If $[x, y] \in \overline{[4i+1, 4i+3]}$, and $[x, y] \notin S$, then, with this notation, $[x, y] = [e_1 + u, e_1 + u + e_k]$ or $[x, y] = [e_1 + e_2 + u, e_1 + e_2 + u + e_k]$, for some $k \geq 3$. In either case, $[x, y] \in \overline{[e_1 + (u + e_k), e_1 + e_2 + (u + e_k)]}$, i.e. $[x, y]$ is in exactly one other block $\bar{z}$ for $z \in T$. Thus the points cancel out in the sum, and we have proved that $w = v^S$. Thus $v^s \in C$.

Now to show that $v^S = w \in C^\perp$, we show that every block of the design meets it in zero or two points. If $[u, u+e_1] \in S$ is in $\overline{[v, v+e_k]}$, then $[u, u+e_1] = [v, v+e_j]$ or $[u, u+e_1] = [v+e_k, v+e_k+e_j]$ for some $j \neq k$. If $u = v, u+e_1 = v+e_j$, so $j = 1$ and $k \neq 1$ and then $u+e_k = v+e_k, u+e_k+e_1 = v+e_k+e_1$, so $[u+e_k, u+e_k+e_1] \in \overline{[v, v+e_k]}$. If another point $[t, t+e_1] \in S$ is in $\overline{[v, v+e_k]}$ then the same reasoning shows it must be one of these points. Thus $v^S \in C^\perp$ and S is an arc.

To show that $v^S \notin C_2(G_n)^\perp$, consider the block $\overline{\overline{0}}$ of $\mathcal{G}_n$. Since $\overline{\overline{0}} = \{[0, e_i] \mid 1 \leq i \leq n\}$, the inner product of this row of G_n with v^S is 1, so $v^S \notin C_2(G_n)^\perp$. Finally, note that the S_i are disjoint, and there are n of them of size 2^{n-1}, so they sum to $\boldsymbol{\jmath}$ of weight $2^{n-1}n$. ■

We now find words of smaller weight in $\mathrm{Hull}(\mathcal{D}_n) \cap \mathrm{Hull}(\mathcal{G}_n)$. For $n \geq 7$ we believe, on computational evidence, that these are minimum words for the hulls, but have not been able to prove it.

Lemma 12. *For $n \geq 3$, if*

$$w_n = \sum_{i=1}^{n} v^{\overline{[0,e_i]}} = nv^{\overline{\overline{0}}} + \sum_{i=1}^{n} v^{\overline{\overline{e_i}}}, \tag{13}$$

then $w_n \in \mathrm{Hull}(\mathcal{D}_n) \cap \mathrm{Hull}(\mathcal{G}_n)$ and

$$\mathrm{Supp}(w_n) = S = \begin{cases} \{[e_i, e_i+e_j] \mid 1 \leq i, j \leq n\} & n \text{ even} \\ \{[e_i, e_i+e_j] \mid 1 \leq i, j \leq n, i \neq j\} & n \text{ odd.} \end{cases} \tag{14}$$

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

Proof. Clearly $w_n \in C = C_2(\mathcal{D}_n)$. To show that $w_n \in C^\perp$, consider the blocks $\overline{[u, u+e_i]}$. It is easy to see that if $\mathrm{wt}(u), \mathrm{wt}(u+e_i) \geq 3$ then there is no intersection with w_n at all, and it is easy to verify that if $u = 0, e_j, e_j+e_k, j, k \neq i$, then the inner product is 0.

Finally, it is easy to verify that $w_n \in C_2(\mathcal{G}_n)^\perp$. ■

In the following lemma, recall that E_i, for $1 \leq i \leq n$, is defined in Equation (10) and that T_u denotes the translation of elements of V_n by the vector $u \in V_n$. Since the hulls are invariant under the translation group T, it follows that $v^{ST_u} \in \mathrm{Hull}(\mathcal{D}_n) \cap \mathrm{Hull}(\mathcal{G}_n)$ for all $u \in V_n$, where S is as in Equation (14). In fact we will show that the v^{ST_u} for $u \in E_1$ will suffice to generate all the v^{ST_u} for $u \in V_n$.

Lemma 13. *For $n \geq 3$, if S is as in Equation (14), and*

$$\mathcal{S} = \{ST_w \mid w \in E_1\},$$

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

$$\begin{cases} 2, n, 2(n-1) & n \text{ even} \\ 2, n-1, 2(n-2) & n \text{ odd.} \end{cases}$$

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

Proof. This is a direct count on the number of possibilities. In the following, $\emptyset \subseteq I \subseteq \{2, \ldots, n\}$, and if $I = \emptyset$, then $\sum_{i \in I} e_i = 0$. Again we consider cases.
(i) If n is even, so that

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

For each type of point $P = [u, u+e_i]$, where $1 \leq i \leq n$, we will list and count the elements of $w \in E_1$ for which $PT_w \in S$.

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

(ii) If n is odd, so that

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

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

The last statement now follows. ■

Proposition 14. *For $n \geq 3$, with $\mathcal{S}$ as in Lemma* 13, $\dim\langle v^R \mid R \in \mathcal{S} \rangle = 2^{n-1} - 1$. *Further,* $\dim(\mathrm{Hull}(\mathcal{G}_n)) \geq 2^{n-1} - 1$ *and* $\dim(\mathrm{Hull}(\mathcal{D}_n)) \geq 2^{n-1}$. □

Proof. We use the count obtained in Lemma 13 and show that the set $\{v^R \mid R \in \mathcal{S} \backslash \{S\}\}$ is linearly independent.

Suppose n is even. For $u \in E_1$, let $S_u = ST_u$. Let $U \subset E_1$, $0 \notin U$ and $U \neq \emptyset$. Suppose $\sum_{u \in U} v^{S_u} = 0$. From the proof of (i)(1) of Lemma 13, with $I = \emptyset$, we see that $e_i \notin U$ for any i. Using this, we see now from (i)(1) that $e_i + e_j \notin U$ for any i, j. Now we can use (i)(1) inductively so show that U is empty, contrary to assumption. Thus the set is linearly independent. An identical argument works for the case n odd.

For the statement concerning the hulls, all the v^R for $R \in \mathcal{S}$ are in both the hulls, by Lemma 12 and the fact that the translation group preserves the codes. This implies the statement about $\mathrm{Hull}(\mathcal{G}_n)$ immediately; for the statement about $\mathrm{Hull}(\mathcal{D}_n)$, we have shown that the words S_i of weight 2^{n-1} of Equation (11) of Lemma 11 are in $\mathrm{Hull}(\mathcal{D}_n)$ but not in $\mathrm{Hull}(\mathcal{G}_n)$, so that the code spanned by the v^R together with one of these words will have dimension 2^{n-1}. ■

In fact it is not hard to verify that

$$\sum_{i=1}^{n} v^{ST_{e_i}} = \begin{cases} 0 & \text{for } n \text{ even} \\ v^S & \text{for } n \text{ odd.} \end{cases}$$

We now turn to the code spanned by the weight-4 vectors of Equation (9) in the dual codes $C^{\perp}$. In the notation $u(x, y, z)$ defined there, note that any three vectors of the set

$\{x, y, z, x+y+z\}$ can be used to uniquely define the vector. Notice that two points of $\mathcal{P}_n$ are together in the support of at most one of these weight-4 vectors.

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

Proof. We prove this inductively by showing that vectors $u(x, y, z)$ can be chosen so that the matrix formed by these words, using the ordering of the points of the designs as described in Section 3, can be written in echelon form with at least $2^{n-1}(n-2)+1$ leading terms. Since this is the dimension of $C_2(\mathcal{G}_n)^\perp$ and all the vectors are in $C_2(\mathcal{G}_n)^\perp$ by Lemma 7, they will thus span $C_2(\mathcal{G}_n)^\perp$. We will speak of the leading term of the word $u(x, y, z)$ as the left-most term with this ordering. Thus for example the leading term of $u(0, e_1, e_2)$ is $[0, e_1]$.

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

We start with $n = 3$. Here $l_3 = 12$, $f_3 = 5$, and we take $\mathcal{F}_3$ to consist of the five weight-4 vectors: $u(0, e_1, e_3)$ (leading term $[0, e_1]$ at position 1); $u(0, e_2, e_3)$ (leading term $[0, e_2]$ at position 2); $u(e_1, e_1+e_2, e_1+e_3)$ (leading term $[e_1, e_1+e_2]$ at position 3); $u(e_2, e_2+e_1, e_2+e_3)$ (leading term $[e_2, e_1+e_2]$ at position 4); $u(e_3, e_1+e_3, e_2+e_3)$ (leading term $[e_3, e_1+e_3]$ at position 9). Notice that we have no leading terms in the range $5 \leq k \leq 8$ of length $4 = 2^2 = 2^{n-1}$ corresponding to the middle section of G_3 as given in the matrix of Equation (2), or Example 1.

Now suppose $n > 3$ and we have constructed $\mathcal{F}_{n-1}$ of size f_{n-1} in this way, having the centre section of 2^{n-2} positions with no leading terms. We construct $\mathcal{F}_n$ as follows: the first l_{n-1} positions will all be leading terms by first taking all the elements of $\mathcal{F}_{n-1}$ apart from the last one $u(\sum_{i=3}^{n-1} e_i, e_1+\sum_{i=3}^{n-1} e_i, e_2+\sum_{i=3}^{n-1} e_i)$ with the right-most leading term $[\sum_{i=3}^{n-1} e_i, e_1+\sum_{i=3}^{n-1} e_i]$. Then, for each of the remaining columns in this first l_{n-1} set, for the edge $[x, x+e]$ where $x \in \langle e_i \mid 1 \leq i \leq n-1 \rangle$ and $e = e_i$, for $1 \leq i \leq n-1$, we adjoin to our set $\mathcal{F}_n$ the word $u(x, x+e, x+e_n)$ which will clearly have leading term $[x, x+e]$. Thus far we have l_{n-1} elements in $\mathcal{F}_n$. Now we skip the next 2^{n-1} column positions, and then adjoin f_{n-1} words formed from the words of $\mathcal{F}_{n-1}$ as follows: if $u(x, x+e, x+f) \in \mathcal{F}_{n-1}$ with leading term $[x, x+e]$ then $u(x+e_n, x+e+e_n, x+f+e_n) \in \mathcal{F}_n$ with leading term $[x+e_n, x+e+e_n]$. This gives the required $f_n = l_{n-1} + f_{n-1}$ words, and they are in echelon form, with the middle section of length 2^{n-1} excluded. This concludes the proof, but we will show below in Example 2 the 17 elements of $\mathcal{F}_4$ obtained in this way. ■

Example 2. For $n = 4$ note that $f_4 = 17 = 12 + 5 = l_3 + f_3$. We show the weight-4 vectors and the leading terms and their positions in Table 1, where L.T. denotes leading term. The $2^{n-1} = 2^3 = 8$ positions 13 to 20 are excluded.

Note 3. In fact a basis for $C_2(\mathcal{G}_n)^\perp$ of weight-4 vectors can be constructed rather easily by using the check-set $\mathcal{C}_n$ of Equation (8) and considering an echelon form using

Weight-4 vector	L.T.	Position
$u(0,e_1,e_3)$	$[0,e_1]$	1
$u(0,e_2,e_3)$	$[0,e_2]$	2
$u(e_1,e_1+e_2,e_1+e_3)$	$[e_1,e_1+e_2]$	3
$u(e_2,e_2+e_1,e_2+e_3)$	$[e_2,e_1+e_2]$	4
$u(0,e_3,e_4)$	$[0,e_3]$	5
$u(e_1,e_1+e_3,e_1+e_4)$	$[e_1,e_1+e_3]$	6
$u(e_2,e_2+e_3,e_2+e_4)$	$[e_2,e_2+e_2]$	7
$u(e_1+e_2,e_1+e_2+e_3,e_1+e_2+e_4)$	$[e_1+e_2,e_1+e_2+e_3]$	8
$u(e_3,e_1+e_3,e_3+e_4)$	$[e_3,e_1+e_3]$	9
$u(e_3,e_2+e_3,e_3+e_4)$	$[e_3,e_2+e_3]$	10
$u(e_1+e_3,e_1+e_2+e_3,e_1+e_3+e_4)$	$[e_1+e_3,e_1+e_2+e_3]$	11
$u(e_2+e_3,e_1+e_2+e_3,e_2+e_3+e_4)$	$[e_2+e_3,e_1+e_2+e_3]$	12
$u(e_4,e_1+e_4,e_3+e_4)$	$[e_4,e_1+e_4]$	21
$u(e_4,e_2+e_4,e_3+e_4)$	$[e_4,e_2+e_4]$	22
$u(e_1+e_4,e_1+e_2+e_4,e_1+e_3+e_4)$	$[e_1+e_4,e_1+e_2+e_4]$	23
$u(e_2+e_4,e_2+e_1+e_4,e_2+e_3+e_4)$	$[e_2+e_4,e_1+e_2+e_4]$	24
$u(e_3+e_4,e_1+e_3+e_4,e_2+e_3+e_4)$	$[e_3+e_4,e_1+e_3+e_4]$	29

Table 1. Example 2: Basis weight-4 vectors and leading terms for $C_2(\mathcal{G}_4)^\perp$

the right-most element of the weight-4 vector. In this way the set of weight-4 vectors

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

has precisely the vectors in $\mathcal{C}_n$ as the right-most terms, in echelon array, reading to the right, if the ordering is according to that of the columns of G_n. However, this set does not lend itself as readily to Lemma 16 below.

Lemma 16. *For* $n \geq 3$, $\dim(C_2(\mathcal{G}_n)+C_2(\mathcal{G}_n)^\perp) \geq 2^{n-1}(n-1)+1$ *and* $\dim(C_2(\mathcal{D}_n)+C_2(\mathcal{D}_n)^\perp) \geq 2^{n-1}(n-1)$. □

Proof. In our echelon form for the code $C_2(\mathcal{G}_n)^\perp$ obtained in Proposition 15, we showed that the first $2^{n-2}(n-1)$ positions are all leading terms and that the middle section of 2^{n-1} positions has no leading term. Thus, in a generating matrix for $C_2(\mathcal{G}_n)+C_2(\mathcal{G}_n)^\perp$, we can reduce the first $2^{n-2}(n-1)$ positions to 0, and obtain leading terms for all the next 2^{n-1} without disturbing the remaining leading terms for $C_2(\mathcal{G}_n)^\perp$. This then provides $2^{n-1}(n-2)+1+2^{n-1} = 2^{n-1}(n-1)+1$ leading terms for $C_2(\mathcal{G}_n)+C_2(\mathcal{G}_n)^\perp$.

For $C_2(\mathcal{D}_n)+C_2(\mathcal{D}_n)^\perp$, we use a similar argument, but look at the form of the matrix M_n in Equation (3). Again we have the first $2^{n-2}(n-1)$ leading terms from $C_2(\mathcal{D}_n)^\perp$, then the next 2^{n-1} points will provide $2^{n-1}-1$ leading terms, since this is the dimension of G_{n-1}^T. Thus we have $2^{n-1}(n-2)+1+2^{n-1}-1 = 2^{n-1}(n-1)$ leading terms. ■

Corollary 17. *For $n \geq 3$, $\dim(\mathrm{Hull}(\mathcal{G}_n)) = 2^{n-1}-1$, $\dim(\mathrm{Hull}(\mathcal{D}_n)) = 2^{n-1}$ and $\mathrm{Hull}(\mathcal{G}_n) \subset \mathrm{Hull}(\mathcal{D}_n)$. An information set for $\mathrm{Hull}(\mathcal{G}_n)$ is the set of positions*

$$\mathcal{I}_n = \bigcup_{i=3}^{n} \{2^{n-1}n - t \mid 2^{n-i}(n-i+1) \leq t \leq 2^{n-i}(n-i+3)-1\} \cup \{2^{n-1}n\},$$

and one for $\mathrm{Hull}(\mathcal{D}_n)$ is $\mathcal{I}_n \cup \{s\}$, where s is any number in the range $2^{n-2}(n-1)+1 \leq s \leq 2^{n-2}(n+1)$. □

Proof. By Lemma 16, $\dim(\mathrm{Hull}(\mathcal{G}_n)) \leq 2^{n-1}-1$ and $\dim(\mathrm{Hull}(\mathcal{D}_n)) \leq 2^{n-1}$. By Proposition 14 $\dim(\mathrm{Hull}(\mathcal{G}_n)) \geq 2^{n-1}-1$ and $\dim(\mathrm{Hull}(\mathcal{D}_n)) \geq 2^{n-1}$. Thus we have equality. Since the words v^R of Proposition 14 span $\mathrm{Hull}(\mathcal{G}_n)$ and are in $\mathrm{Hull}(\mathcal{D}_n)$, we have the inclusion stated. The assertion concerning the information sets follows from the echelon form in Proposition 15 and Lemma 16, by taking the columns that are not leading terms for the dual of the hull in each case.■

Corollary 18. *For $3 \leq n \leq 6$, $\mathrm{Hull}(\mathcal{D}_n)$ has minimum weight 2^{n-1}; for $3 \leq n \leq 5$, $\mathrm{Hull}(\mathcal{G}_n)$ has minimum weight $n(n-1)$ and for $n=6$ it has minimum weight $n^2 = 36$. For $n=7$ both hulls have minimum weight 42 and for $n=8$ both hulls have minimum weight 64. For $n \geq 9$, the minimum weight of both hulls is at least $2n$ and at most $n(n-1)$ for n odd, and at least $2n$ and at most n^2 for n even.* □

Proof. Use Magma up to $n=8$. After that we have words of weight $n(n-1)$ for n odd, n^2 for n even, and $2^{n-1} > n(n-1), n^2$ for $n \geq 8$, so the words of Lemma 12 are smaller than those of Lemma 11. That the minimum weight is at least $2n$ follows from the fact that any word of either hull is in $C_2(\mathcal{D}_n)$ which has minimum weight $2(n-1)$. For $n \geq 4$ the minimum words of $C_2(\mathcal{D}_n)$ are the incidence vectors of the blocks of $\mathcal{D}_n$ and these cannot be in either hull since they can meet blocks of either design in one point. Since the hulls are even-weight codes, the next possible weight is $2n$. For $n=7,8$ the minimum words found were of the type of Lemma 12. ■

7. Permutation decoding

In (12, Lemma 7) the following, which generalizes a comment in (17) regarding cyclic codes, was proved:

Result 1. *Let C be a code with minimum distance d, $\mathcal{I}$ an information set, $\mathcal{C}$ the corresponding check set and $\mathcal{P} = \mathcal{I} \cup \mathcal{C}$. Let G be an automorphism group of C, and n the maximum of $|\mathcal{O} \cap \mathcal{I}|/|\mathcal{O}|$, where $\mathcal{O}$ is a G-orbit. If $s = \min(\lceil \frac{1}{n} \rceil - 1, \lfloor \frac{d-1}{2} \rfloor)$, then G is an s-PD-set for C.* □

Note that this result is true for any information set. If the group G is transitive then $|\mathcal{O}|$ is the degree of the group and $|\mathcal{O} \cap \mathcal{I}|$ is the dimension of the code. In our case, if $E = \{T_u \mid u \in V_n, \mathrm{wt}(u) \text{ is even}\}$ and g is an n-cycle in S_n, then $K = E\langle g \rangle$ is regular on $\mathcal{P}_n$, of order $2^{n-1}n$. This is easy to see since $\langle g \rangle$ normalizes E. So for dimension k we have that K is an s-PD-set for $s = \min(\lceil \frac{2^{n-1}n}{k} \rceil - 1, \lfloor \frac{d-1}{2} \rfloor)$, where d is the minimum weight.

Proposition 19. *For $n \geq 3$ the group K defined above, of order $2^{n-1}n$, is an s-PD-set for the code C of length $2^{n-1}n$ for any information set in each of the following cases:*
- *$C = C_2(\mathcal{G}_n)$ for $s = \lfloor (n-1)/2 \rfloor$, full error-correction (PD-set);*
- *$C = C_2(\mathcal{D}_n)$ for $s = \lfloor n/2 \rfloor$;*
- *$C = \mathrm{Hull}(\mathcal{G}_n)$ for $s = n-1$ for $n = 3$, n for $4 \leq n \leq 8$, $n-1$ for $n \geq 9$;*
- *$C = \mathrm{Hull}(\mathcal{D}_n)$ for $s = n-1$ for $n \geq 4$.*

Proof. We use Result 1 and the propositions and lemmas we have obtained for the dimensions of the codes and the minimum weights. The assertions for $C_2(\mathcal{G}_n)$ and $C_2(\mathcal{D}_n)$ then follow directly.

For the hulls, we have specific vales for the minimum weight up to $n = 8$. For $n \geq 9$ we have not shown that the minimum weight is n^2 or $n(n-1)$ for n even, or odd, respectively, as expected from Magma computations. However, from Corollary 18, the minimum weight is at least $2n$. Using this for d for $n \geq 9$ in the formula gives the stated result. ■

Information sets for $C_2(\mathcal{G}_n)$ and $C_2(\mathcal{D}_n)$ are given in Corollary 4, and for the hulls in Corollary 17. Those of Corollary 4, taking only the first 2^n or $2^n - 1$, respectively, positions, are information sets for the hulls as well, according to computations with Magma up to $n = 10$.

The proof of Theorem 1 is now complete.

8. Conclusion

The incidence structure of $2^{n-1}n$ points $\mathcal{P}_n$ and 2^n blocks the sets ST where S is the set given in Equation (14) and T is the translation group, is a 1-$(2^{n-1}n, n^2, 2n)$ design for n even, and a 1-$(2^{n-1}n, n(n-1), 2(n-1))$ design for n odd, with binary code $\mathrm{Hull}(\mathcal{G}_n)$. Further codes that can be studied in conjunction with those examined here, and for which we now have some information, are those spanned by the vectors $v^b - v^c$, where b and c are blocks of the relevant design. Properties of such codes from incidence structures are deduced in (1, Section 2.4).

Smaller PD-sets were found computationally with Magma for most of the codes discussed in this paper for small n, using the information set as given in Corollary 4. However, we were unable to find a general result to give smaller PD-sets or s-PD-sets, as, for example, in (13), using these information sets.

Acknowledgements

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

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. Codes, designs and groups from the Hamming graphs. *J. Combin. Inform. System Sci.* (To appear).

[6] W. Fish, J. D. Key, and E. Mwambene. Graphs, designs and codes related to the n-cube. *Discrete Math.*, 309:3255–3269, 2009.

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

[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 for codes from finite planes. *European J. Combin.*, 26:665–682, 2005.

[12] J. D. Key, T. P. McDonough, and V. C. Mavron. Information sets and partial permutation decoding for codes from finite geometries. *Finite Fields Appl.*, 12:232–247, 2006.

[13] J. D. Key and P. Seneviratne. Binary codes from rectangular lattice graphs and permutation decoding. *European J. Combin.*, 28:121–126, 2006.

[14] 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.

[15] J. D. Key and P. Seneviratne. Permutation decoding of binary codes from lattice graphs. *Discrete Math.*, 308:2862–2867, 2008.

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

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

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

[19] E. Prange. The use of information sets in decoding cyclic codes. *IRE Trans.*, IT-8:5–9, 1962.

[20] Gordon F. Royle. Colouring the cube. Preprint.
[21] J. Schönheim. On coverings. *Pacific J. Math.*, 14:1405–1411, 1964.
[22] Padmapani Seneviratne. *Permutation decoding of codes from graphs and designs.* PhD thesis, Clemson University, 2007.
[23] Hassler Whitney. Congruent graphs and the connectivity of graphs. *Amer. J. Math.*, 54:154–168, 1932.