BINARY CODES FROM $m$-ARY $n$-CUBES $Q_m^n$

JENNIFER D. KEY
Department of Mathematics and Applied Mathematics
University of the Western Cape, 7535 Bellville, South Africa

BERNARDO G. RODRIGUES
Department of Mathematics and Applied Mathematics
University of Pretoria, Hatfield 0028, South Africa

(Communicated by Sihem Mesnager)

Abstract. We examine the binary codes from adjacency matrices of the graph with vertices the nodes of the $m$-ary $n$-cube $Q^m_n$ and with adjacency defined by the Lee metric. For $n=2$ and $m$ odd, we obtain the parameters of the code and its dual, and show the codes to be LCD. We also find $s$-PD-sets of size $s+1$ for $s < m/2$ for the dual codes, i.e. $[m^2, 2m-1, m]_2$ codes, when $n=2$ and $m \geq 5$ is odd.

1. Introduction

The graphs defined by the $m$-ary $n$-cube $Q^m_n$ and with adjacency defined by the Lee metric are defined in various places in the literature, but see [5] for example. They are also known as Lee graphs.

Definition 1.1. Let $m, n \geq 1$ be positive integers, and $R = \{0, 1, \ldots, m-1\}$ with addition and multiplication as in the ring of integers modulo $m$, or, if $m = q$ is a prime power, $R$ could be $\mathbb{F}_m$. The graph $\Gamma = (V, E)$ on $Q^m_n$, has $V = R^n$, the set of $n$-tuples with entries in $R$, with adjacency defined by $x = \langle x_0, x_1, \ldots, x_{n-1} \rangle$ adjacent to $y = \langle y_0, y_1, \ldots, y_{n-1} \rangle$ if there exists an $i$, $0 \leq i \leq n-1$, such that $x_i - y_i \equiv \pm 1 \pmod{m}$ and $x_j = y_j$ for all $j \neq i$. Thus $\Gamma$ is regular of degree $2n$.

We will examine the binary codes from the adjacency matrices of these graphs. Since for $m = 2, 3$ the graph is the Hamming graph, the codes of which have been extensively studied, we take $m \geq 4$.

Our best findings are for $n = 2$ and $m$ odd, and we summarize our main results for these codes in a single theorem:

Theorem 1.2. Let $\Gamma = Q^m_2 = (V, E)$ and $R = \{0, 1, \ldots, m-1\}$ where $m \geq 5$ is odd, and $C = C_2(\Gamma)$. Then $C$ is LCD, i.e. $C \cap C^\perp = \{0\}$, and $C$ is a $[m^2, (m-1)^2, 4]_2$ code, $C^\perp$ a $[m^2, 2m-1, m]_2$ code.

The set of points

$$I = \{<0, i> | i \in R\} \cup \{<1, i> | i \in R \setminus \{m-1\}\}$$

2010 Mathematics Subject Classification: Primary: 05C50, 94B05; Secondary: 05B05.

Key words and phrases: LCD codes, Lee graph, permutation decoding.

The second author is supported by the National Research Foundation of South Africa (Grant Numbers 95725 and 106071).

* Corresponding author: J. D. Key.
is an information set for $C^\perp$, and for $s < \frac{m-1}{2}$, the set of translations $S = \{\tau_{<a,b>} | 0 \leq i \leq s\}$ is an $s$-PD-set of minimal size $s + 1$ for the code $C^\perp$ with information set $I$. The group $T = \{\tau_X | X \in R^2\}$ of translations is a PD-set for full error correction, where the translations are defined by $\tau_{<a,b>} : <x, y> \mapsto <x + a, y + b>$.

The theorem combines results from Propositions 2 and 3 in Section 3 and Section 4, respectively. Since the binary code for $Q_2^n$ has minimum weight 4 for all $m$, the better codes are the duals, with minimum weight $m$, and these are the codes we use for decoding.

The paper is organized as follows: Section 2 concerns the background definitions, terminology, and earlier results needed in our propositions, and includes background subsections on the graphs $Q_n^m$, on LCD codes, and on permutation decoding. Section 3 concerns the codes $C_2(Q_n^m)$ and has our main results for $n = 2$ and $m$ odd. Section 4 has our results on permutation decoding of $C_2(Q_2^n)^\perp$ for $m$ odd. In Section 5 some computational results for other values of $n$ and $m$ are given.

2. Background concepts and terminology

The notation for codes and codes from graphs is as in [1]. For an incidence structure $D = (\mathcal{P}, \mathcal{B}, \mathcal{J})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{J}$, the code $C_F(D) = C_Q(D)$ of $D$ over the finite field $F = \mathbb{F}_q$ is the space spanned by the incidence vectors of the blocks over $F$. If $Q$ is any subset of $\mathcal{P}$, then we will denote the incidence vector of $Q$ by $v^Q$, and if $Q = \{x\}$ where $x \in \mathcal{P}$, then we will write $v^x$. For any $w \in F^\mathcal{P}$ and $P \in \mathcal{P}$, $w(P)$ denotes the value of $w$ at $P$.

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 $wt(v)$ of a vector $v$ is the number of non-zero coordinate entries. Vectors in a code are also called words. For two vectors $u, v$ the distance $d(u, v)$ between them is $wt(u - v)$. The support, $\text{Supp}(v)$, of a vector $v$ is the set of coordinate positions where the entry in $v$ is non-zero. So $|\text{Supp}(v)| = wt(v)$. 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 $\langle ., . \rangle$, i.e. $C^\perp = \{v \in F^n | \langle v, c \rangle = 0 \text{ for all } c \in C\}$. The hull, $\text{Hull}(C)$, of a code $C$ is the self-orthogonal code $\text{Hull}(C) = C \cap C^\perp$. A check matrix for $C$ is a generator matrix for $C^\perp$. The all-one vector will be denoted by $\mathbf{1}$, and is the vector with all entries equal to 1. If we need to specify the length $m$ of the all-one vector, we write $J_m$. A constant vector is a non-zero vector in which all the non-zero entries are the same. We call two linear codes isomorphic (or permutation 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 $\text{Aut}(C)$, also called the permutation group of $C$, and denoted by $\text{PAut}(C)$ in [11].

The graphs, $\Gamma = (V, E)$ with vertex set $V$ and edge set $E$, discussed here are undirected with no loops, apart from the case where all loops are included, in which case the graph is called the reflexive associate of $\Gamma$, denoted by $R\Gamma$. If $x, y \in V$ and $x$ and $y$ are adjacent, we write $x \sim y$, and $xy$ for the edge in $E$ that they define. The set of neighbours of $x \in V$ is denoted by $N(x)$, and the valency of $x$ is $|N(x)|$. $\Gamma$ is regular if all the vertices have the same valency.

An adjacency matrix $A = [a_{x,y}]$ for $\Gamma$ is a $|V| \times |V|$ matrix with rows and columns labelled by the vertices $x, y \in V$, and with $a_{x,y} = 1$ if $x \sim y$ in $\Gamma$, and $a_{x,y} = 0$ otherwise. Then $RA = A + I$ is an adjacency matrix for $R\Gamma$. The row corresponding
to \( x \in V \) in \( A \) will be denoted by \( r_x \), that in \( RA \) by \( s_x \). In the following, we may simply identify \( r_x \) and \( s_x \) with the support of the row, so \( r_x = \{ y \mid x \sim y \} \) and \( s_x = \{ x \} \cup \{ y \mid x \sim y \} \).

The **code** over a field \( F \) of \( \Gamma \) will be the row span of an adjacency matrix \( A \) for \( \Gamma \), and written as \( C_F(A), C_F(\Gamma) \), or \( C_p(A), C_p(\Gamma) \), respectively, if \( F = \mathbb{F}_p \).

### 2.1. The graphs \( Q^m_n \)

The graphs are defined in Definition 1.1. For any \( x \in R^n \), \( x_i \) will denote the \( i^{th} \) coordinate of \( x \), for \( 0 \leq i \leq n - 1 \).

For \( a \in R^n \), \( a = < a_0, a_1, \ldots, a_{n-1} > \), the translation \( \tau_a \) is the map defined on \( x = < x_0, x_1, \ldots, x_{n-1} > \) by

\[
\tau_a : x \mapsto < x_0 + a_0, x_1 + a_1, \ldots, x_{n-1} + a_{n-1} > .
\]

If \( \sigma_i \in S_n \) for \( 0 \leq i \leq n - 1 \), then the map \( \sigma \) is defined by

\[
\sigma^{-1} : x \mapsto < x_0 \sigma_0, x_1 \sigma_1, \ldots, x_{n-1} \sigma_{n-1} >
\]

where the symmetric group \( S_n \) is acting on the \( n \) symbols \( 0, 1, \ldots, n - 1 \).

For any \( i \) such that \( 0 \leq i \leq n - 1 \), the map \( \mu_i \) is defined by

\[
\mu_i : x = < x_0, x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_{n-1} > \mapsto < x_0, \ldots, x_{i-1}, -x_i, x_{i+1}, \ldots, x_{n-1} > ,
\]

where \( -x_i = m - x_i \).

It is easy to verify that the translations \( \tau_a \) for \( a \in R^n \) and the permutations \( \sigma \), for all \( \sigma_i \), and \( \mu_i \) for all \( i \), are automorphisms of \( \Gamma \), and that \( \text{Aut}(\Gamma) \) is both vertex and edge transitive.

\( Q^m_n \) is the cartesian product \( (Q^m_1)^\otimes n \) of \( n \) copies of \( Q^m_1 \). If \( A_{n,m} \) denotes the adjacency matrix for \( Q^m_n \) where the elements of \( R \) are labelled naturally, and the \( n \)-tuples likewise, we have \( A_{2,m} = A_{1,m} \otimes I_m + I_m \otimes A_{1,m} \) (Kronecker product) and \( A_{n,m} = A_{1,m} \otimes I_{m^{n-1}} + I_m \otimes A_{n-1,m} \). Since the matrix \( A_{1,m} \) will be \( m \times m \) of the form

\[
A_{1,m} = \begin{bmatrix}
0 & 1 & 0 & 0 & \cdots & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & \cdots & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & \cdots & 0 & 0 & 1 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & \cdots & 1 & 0 & 1
\end{bmatrix}
\]

the matrix for \( A_{n,m} \) has the form

\[
A_{n,m} = \begin{bmatrix}
A_{n-1,m} & I & 0 & 0 & \cdots & 0 & I \\
I & A_{n-1,m} & I & 0 & \cdots & 0 & 0 \\
0 & I & A_{n-1,m} & I & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \cdots & I & A_{n-1,m} & I \\
I & 0 & 0 & 0 & \cdots & I & A_{n-1,m} & I
\end{bmatrix}
\]

where \( I \) is the \( m^{n-1} \times m^{n-1} \) identity matrix.

From the form of \( A_{1,m} \), one sees that for \( Q^m_1 \),

\[
\text{rank}_2(A_{1,m}) = \begin{cases}
    m - 2 & \text{if } m \text{ is even} \\
    m - 1 & \text{if } m \text{ is odd}
\end{cases}
\]

and

\[
\text{rank}_2(A_{1,m} + I) = \begin{cases}
    m - 2 & \text{if } m \equiv 0 \pmod{3} \\
    m & \text{if } m \not\equiv 0 \pmod{3}
\end{cases}
\]
Note that $A_{1,m} + I$ is a circulant $m \times m$ matrix generated by $(1,1,1,0,\ldots,0)$. If $m$ is divisible by 3, one sees that the 2-rank is $m - 2$. Otherwise it is $m$: see, for example, [17].

For $m$ odd, $C_2(Q_m)$ clearly has zero hull.

2.2. LCD codes. The background on LCD codes from [21] is described below.

**Definition 2.1.** A linear code $C$ over any field is a linear code with complementary dual (LCD) code if $\text{Hull}(C) = C \cap C^\perp = \{0\}$.

If $C$ is an LCD code of length $n$ over a field $F$, then $F^n = C \oplus C^\perp$. Thus the orthogonal projector map $\Pi_C$ from $F^n$ to $C$ can be defined as follows: for $v \in F^n$,

$$v \Pi_C = \begin{cases} v & \text{if } v \in C, \\ 0 & \text{if } v \in C^\perp \end{cases},$$

and $\Pi_C$ is defined to be linear.\(^1\) This map is only defined if $C$ (and hence also $C^\perp$) is an LCD code. Similarly then $\Pi_{C^\perp}$ is defined.

Note that for all $v \in F^n$,

$$v = v \Pi_C + v \Pi_{C^\perp}. \quad (3)$$

We will use [21, Proposition 4]:

**Result 1 (Massey).** Let $C$ be an LCD code of length $n$ over the field $F$ and let $\varphi$ be a map $\varphi : C^\perp \mapsto C$ such that $u \in C^\perp$ maps to one of the closest codewords $v$ to it in $C$. Then the map $\hat{\varphi} : F^n \mapsto C$ such that

$$\hat{\varphi}(r) = r \Pi_C + \varphi(r \Pi_{C^\perp})$$

maps each $r \in F^n$ to one of its closest neighbours in $C$.\(^2\)

We make the following observation which will be of use in the next section:

**Lemma 2.2.** If $C$ is a q-ary code of length $n$ such that $C + C^\perp = F_q^n$ then $C$ is LCD.

**Proof.** Since $(C + C^\perp)^\perp = C^\perp \cap C = (F_q^n)^\perp = \{0\} = \text{Hull}(C)$, $C$ (and $C^\perp$) are LCD. \(\square\)

From [15, 16]:

**Definition 2.3.** Let $\Gamma = (V,E)$ be a graph with adjacency matrix $A$. Let $p$ be any prime, $C = C_p(A)$, $RC = C_p(RA)$ (for the reflexive graph), where $RA = A + I$. Then if $C = RC^\perp$ we call $C$ a reflexive LCD code, and write $RLCD$ for such a code.

We will also use the following from [21, Proposition 1]:

**Result 2 (Massey).** If $G$ is a generator matrix for the $(n,k)$ linear code $C$ over the field $F$, then $C$ is LCD if and only if the $k \times k$ matrix $GG^T$ is nonsingular. Moreover, if $C$ is LCD then $\Pi_C = G^T(GG^T)^{-1}G$ is the orthogonal projector from $F^n$ onto $C$.

\(^1\)Note typographical error on p.338, l.-11, in [21]
\(^2\)Note typographical error on p.341, l.-7, in [21]
2.3. **Permutation decoding.** **Permutation decoding** was first developed by MacWilliams [19] and involves finding a set of automorphisms of a code called a PD-set. The method is described fully in MacWilliams and Sloane [20, Chapter 16, p. 513] and Huffman [11, Section 8]. In [12] and [18] the definition of PD-sets was extended to that of s-PD-sets for s-error-correction:

**Definition 2.4.** If C is a t-error-correcting code with information set \( \mathcal{I} \) and check set \( C \), then a **PD-set** for \( C \) for \( C \) is a set \( S \) of automorphisms of \( C \) which is such that every \( t \)-set of coordinate positions is moved by at least one member of \( S \) into the check positions \( C \).

For \( s \leq t \) an **s-PD-set** is a set \( S \) of automorphisms of \( C \) which is such that every \( s \)-set of coordinate positions is moved by at least one member of \( S \) into \( C \).

The algorithm for permutation decoding is as follows: we have a \( t \)-error-correcting \([n, k, d]_q\) code \( C \) with check matrix \( H \) in standard form. Thus the generator matrix \( G = [I_k | A] \) and \( H = [-A^T | I_{n-k}] \), for some \( A \), and the first \( k \) coordinate positions correspond to the information symbols. Any vector \( v \) of length \( k \) is encoded as \( vG \).

Suppose \( x \) is sent and \( y \) is received and at most \( t \) errors occur. Let \( S = \{g_1, \ldots, g_s\} \) be the PD-set. Compute the syndromes \( H(yg_i)^T \) for \( i = 1, \ldots, s \) until an \( i \) is found such that the weight of this vector is \( t \) or less. Compute the codeword \( c \) that has the same information symbols as \( yg_i \) and decode \( y \) as \( cg_i^{-1} \).

Notice that this algorithm actually uses the PD-set as a sequence. Thus it is expedient to index the elements of the set \( S \) by the set \( \{1, 2, \ldots, |S|\} \) so that elements that will correct a small number of errors occur first. Thus if **nested s-PD-sets** are found for all \( 1 < s \leq t \) then we can order \( S \) as follows: find an s-PD-set \( S_s \) for each \( 0 \leq s \leq t \) such that \( S_0 \subset S_1 \subset \ldots \subset S_t \) and arrange the PD-set \( S \) as a sequence in this order:

\[
S = [S_0, (S_1 - S_0), (S_2 - S_1), \ldots, (S_t - S_{t-1})].
\]

(Usually one takes \( S_0 = \{id\} \).)

There is a bound on the minimum size that a PD-set \( S \) may have, due to Gordon [10], from a formula due to Schönheim [22], and quoted and proved in [11]:

**Result 3.** If \( S \) is a PD-set for a \( t \)-error-correcting \([n, k, d]_q\) code \( C \), and \( r = n - k \), then

\[
|S| \geq \left\lfloor \frac{n - 1}{r - 1} \left\lfloor \frac{n - t + 1}{r - t + 1} \right\rfloor \cdots \right\rfloor = G(t).
\]

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

We note the following result from [14, Lemma 1]:

**Result 4.** If \( C \) is a \( t \)-error-correcting \([n, k, d]_q\) code, \( 1 \leq s \leq t \), and \( S \) is an s-PD-set of size \( G(s) \) then \( G(s) \geq s + 1 \). If \( G(s) = s + 1 \) then \( s \leq \lfloor \frac{n}{k} \rfloor - 1 \).

In [13, Lemma 7] the following was proved:

**Result 5.** Let \( C \) be a linear code with minimum weight \( d \), \( \mathcal{I} \) 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 value of \( |\mathcal{O} \cap \mathcal{I}|/|\mathcal{O}| \), over the \( G \)-orbits \( \mathcal{O} \). If \( s = \min(\lfloor \frac{1}{n} \rfloor - 1, \lfloor \frac{d-1}{2} \rfloor) \), then \( G \) is an s-PD-set for \( C \).

This result holds 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.
A simple argument yields that the worst-case time complexity for the decoding algorithm using an $s$-PD-set of size $z$ on a code of length $n$ and dimension $k$ is $O(nkz)$.

3. The codes $C_2(Q_n^m)$

We first note, referring to Definition 2.3:

**Lemma 3.1.** The codes $C_2(Q_n^m)$ are not RLCD for any $n,m \geq 4$.

**Proof.** Denoting the row of $A$ for the vertex $x$ as $r_x$ and that of $A+I$ for $x$ as $s_x$ it is easy to see that $s_{<0,\ldots,0>} \cap r_{<1,0,\ldots,0>} = \{<0,\ldots,0>\}$ and thus the inner product is not 0 modulo 2, so $C_2(Q_n^m)$ is not RLCD. \qed

**Proposition 1.** Let $\Gamma = Q_n^m = (V,E)$ and $R = \{0,1,\ldots,m-1\}$ where $m \geq 4$, and $C = C_2(\Gamma)$. Then if $\Lambda = \{<i,i> | i \in R\}$, it follows that the word $v^\Lambda \in C^\perp$.

Furthermore, there are $2m$ distinct words of weight $m$ obtained from $v^\Lambda$ by applying the automorphisms $\tau_{<1,0>}$ repeatedly and $\mu_0$ to each of these.

If $m$ is odd then the $2m$ words span a subspace $D$ of $C^\perp$ of dimension $2m-1$. Furthermore, $\text{Hull}(D) = \{0\}$. If $m \geq 4$ is even, the $2m$ words span a self-orthogonal subspace $D$ of $C^\perp$ of dimension $2m-2$.

**Proof.** For $<x,y> \in V$, $N(<x,y>) = \{<x, y+1>, <x, y-1>, <x+1, y>, <x-1, y>\}$. We need to show that $\Lambda$ meet every $N(<x,y>)$ evenly. Suppose $<a,a> \in N(<x,y>)$. Then $a = x$ or $a = y$ so without loss of generality we assume $a = x$, and $<a,a><x,y+1>$. Thus $a = y+1$, i.e. $y = a-1$, and so $<x-1,y><a-1,a-1> = \Lambda \cap N(<x,y>)$. Since $<a,a> \neq <a-1,a-1>$, $\Lambda$ meets $N(<x,y>)$ evenly.

Applying $\tau_{<1,0>}$ to $\Lambda$ gives $m$ distinct words (including $v^\Lambda$), and applying $\mu_0$ to each of these gives a further $m$ distinct words. We label these words as $u_i$ and $v_i$, for $i \in R$, where $u_i$ has support $\Lambda^{<i,i>}$ and $v_i$ has support $\Lambda^{<i,i>\mu_0}$, for $i \in R$, respectively. Thus $\text{Supp}(u_i) = \{<i+j,j> | j \in R\}$ and $\text{Supp}(v_i) = \{<-i-j,j> | j \in R\}$, where we are working modulo $m$.

To show that the set $\{u_i,v_i | i \in R\}$ spans a space of dimension $2m-1$ for $m$ odd, and $2m-2$ for $m$ even, we note first that every vertex $<a,b>$, where $a,b \in R$, occurs in the support of exactly two of these weight-$m$ words, viz., $u_{a-b}, v_{a-b}$. This follows since $<a,b> = <a,b> \cup <a-b,0> = (b,a) \cup (a,b)$. Clearly if we add all the $2m$ words we get the zero vector, and so the dimension is at most $2m-1$.

Suppose $w = \sum_{i=0}^{m-1} \alpha_i u_i + \sum_{i=0}^{m-1} \beta_i v_i = 0$. Then $w(<a,b>) = 0 = \alpha_{a-b} + \beta_{a-b}$ for all $a,b$, and taking $a = 0$ this shows that $\alpha_i = \beta_i$ for all $i$. So $\alpha_{a-b} = \alpha_{b-a}$ for all $a,b$, i.e. $\alpha_c = \alpha_{c-2b}$ for all $c,b$. For $m$ odd we deduce that $\alpha_i = \alpha$, a constant, and thus the only relation we get for $m$ odd is the sum of all the words being zero, and thus any $2m-1$ are linearly independent. For $m$ even, we divide the $u_i$ and $v_i$ into two sets each for $i$ and $j$ both even or both odd. Note that $a-b$ and $-a-b$ are both even or both odd, so that if we form the sum $w = \sum_{i \text{ even}} (u_i + v_i)$ we have $w = 0$, and similarly for $i$ odd, giving dimension $2m-2$ in the case where $m$ is even.

For the final statements, take first $m$ odd. For $w \in D$, we have $w = \sum_{i=0}^{m-1} \alpha_i u_i + \sum_{i=0}^{m-1} \beta_i v_i$. If $w \in D^\perp$, then $\langle w, u_j \rangle = \langle w, v_j \rangle = 0$ for all $j \in R$. Thus

$$\langle w, u_j \rangle = \sum_{i=0}^{m-1} \alpha_i (u_i, u_j) + \sum_{i=0}^{m-1} \beta_i (v_i, u_j) = m \alpha_j + \sum_{i=0}^{m-1} \beta_i = 0,$$
and so \( \alpha_j = \alpha = \sum_{i=0}^{m-1} \beta_i \) for \( j \in R \), i.e. a constant. Similarly, \((w, v_j) = m \beta_j + \sum_{i=0}^{m-1} \alpha_i = 0\), so \( \beta_j = \alpha \) for all \( j \in R \), and \( w = \alpha \sum_{i \in R} (w_i + v_i) = 0 \) as was shown above.

For \( m \) even, we show that \((u_i, u_j) = (u_i, v_j) = (v_j, v_j) = 0\) for all \( i, j \). Note first that it is clear that \((u_i, u_j) = (v_i, v_j) = 0\) since the \( m \) words \( u_i \) (respectively \( v_j \)) do not intersect, so we need only consider \((u_i, v_j)\). Here it is not difficult to see that \( \langle x, y \rangle = u_i \cap v_j \) implies that \( \langle x - \frac{m}{2}, y - \frac{m}{2} \rangle = u_i \cap v_j \), and since the points are distinct, the inner product is zero, as we require. \( \square \)

**Corollary 1.** For \( m \) odd \( \dim(C_2(Q_m^n)) \leq (m-1)^2 \), and for \( m \) even \( \dim(C_2(Q_m^n)) \leq (m-1)^2 + 1 \).

**Proof.** Follows from the proposition. \( \square \)

**Lemma 3.2.** If \( m \geq 4 \) is even and \( D, u_i, v_i \) are as in Proposition 1, \( \Gamma = Q_2^m \), then

1. If \( S = \{< 0, 0 >, < \frac{m}{2}, \frac{m}{2} >\} \), then \( u_S \in D^\perp \);
2. \( u_0 + u_2 = \sum_{i=0}^{m-1} r_{<2i+1,2i>} \) and \( \dim(C \cap D) \geq 2m - 4 \).

**Proof.** (1) \( < 0, 0 > \in u_0, v_0 \) and \( < \frac{m}{2}, \frac{m}{2} > \in u_0, v_0 \), and neither point is any other of the \( u_i, v_j \), so \( (v_S, u_i) = (v_S, v_j) = 0 \) for all \( i, j \).

(2) Using the fact that \( r_{<2i+1,2i>} = v^T \)\]

\[ T = \{< 2i + 1, 2i + 1 >, < 2i + 1, 2i >,< 2i + 1, 2i + 1 >, < 2i + 2, 2i + 1 >, < 2i + 2, 2i >, < 2i + 2, 2i + 1 >, \}

it is easy to verify the given identity.

Applying the translations to this gives \( u_i + u_j, v_i + v_j \in C \) for both \( i, j \) even or both odd, and hence gives \( C \cap D \) of index at most 2 in \( D \). \( \square \)

**Note:** According to Magma[3, 4], if \( 4 | m \) then \( D \subset C \) and for \( m = 8 \) we have

\[ u_7 = r_{<3,1>} + r_{<5,3>} + r_{<5,7>} + r_{<7,1>} + r_{<6,2>} + r_{<2,2>} + r_{<4,4>} + r_{<4,0>} \]

**Lemma 3.3.** Let \( \Gamma = Q_2^m \) and \( R = \{0, 1, \ldots, m-1\} \) where \( m \geq 4 \), and \( C = C_2(\Gamma) \).

For \( m \) odd, the minimum weight of \( C \) is 4. For \( m \geq 4 \) even, the code \( D^\perp \supset C \), where \( D \) is as in Proposition 1, has words of weight 2, but if \( m = 2m_1 \) where \( m_1 \geq 3 \) is odd, then \( C \) has minimum weight 4.

**Proof.** Clearly the rows of an adjacency matrix have weight 4, and \( C \) is an even weight code, so there are no words of weight 3. Suppose it has a word \( w \) of weight 2. Without loss of generality, we can assume \( w \) has support \{\( < 0, 0 >, < i, j > \)\}. Since \((w, w^A) = 0\), where \( A \) is as in Proposition 1, we must have \( i = j \neq 0 \). Since \( \mu_1 \in \mathrm{Aut}(\Gamma) \), \( w_{\mu_1} \) with support \{\( < 0, 0 >, < -i, i > \)\} is also in \( C \). But \( i \neq -i \) for \( i \neq 0 \) in \( R \) for \( m \) odd. Thus \( C \) cannot have weight-2 vectors.

If \( m \geq 4 \) is even, then the word with support \{\( < 0, 0 >, < \frac{m}{2}, \frac{m}{2} > \)\} is in \( D^\perp \) and so the argument for words from \( D \) does not rule out words of weight 2 in \( C \).

From Result 6, we can form words in \( C^\perp \) using words in \( C_2(Q_1^{m_1}) \). It is easy to see that words with support \( s_1 = \{0, 2, \ldots, m - 2\} \) and \( s_2 = \{1, 3, \ldots, m - 1\} \) are in \( C_2(Q_1^{m_1}) \). Thus from Result 6 the word with support \{\( < x, y > | x, y \in s_1 \)\} of weight \( \frac{m}{2}^2 \) will be in \( C_2(Q_2^{m_1}) \). If \( \frac{m}{2} \) is odd this word will meet the weight-2 with support \{\( < 0, 0 >, < \frac{m}{2}, \frac{m}{2} > \)\} only once, so we can deduce that \( C_2(2^{m_1}) \) has minimum weight 4 when \( m \equiv 2 \) (mod 4). \( \square \)

Note that the above argument does not give a contradiction for \( m \equiv 0 \) (mod 4) so one must find other words in \( C^\perp \) that cannot be orthogonal to weight-2 words in such cases, and in particular to the word with support \{\( < 0, 0 >, < \frac{m}{2}, \frac{m}{2} > \)\}.
In [7] the following result is proved:

**Result 6.** Let $\Gamma = \Gamma_1 \sqcup \Gamma_2$, where $\Gamma_i = (V_i, E_i)$ for $i = 1, 2$. Let $w_i \in C_2(\Gamma_i)^\perp$ be of weight $d_i$, with $S_1 = \text{Supp}(w_1) = \{a_1, \ldots, a_{d_1}\}$, $S_2 = \text{Supp}(w_2) = \{b_1, \ldots, b_{d_2}\}$, where $a_i \in V_1$, $b_j \in V_2$. Then the word with weight $d_1d_2$ and support

$$S = \{< a_i, b_j | i = 1, \ldots, d_1, j = 1, \ldots, d_2\},$$

is in $C_2(\Gamma^\square)^\perp$.

From Proposition 1 and Result 6 we may deduce the following:

**Lemma 3.4.** Let $\Gamma = Q^m_n = (Q^m_1)^\square \sqcup, n$ and $C = C_2(\Gamma)$. Then

1. if $m \geq 5$ is odd, then for $n \geq 2$, $C^\perp$ has words of weight $m^{n-1}$;
2. if $m \geq 4$ is even, then for $n \geq 2$, $C^\perp$ has words of weight $\frac{m^{n-1}}{2^{n-1}}$.

**Proof.** If $m$ is odd then $C_2(Q_n^m)^\perp = \{w\}$ with minimum weight $m$. By Proposition 1, $C_2(Q_n^m)^\perp$ has a word of weight $m$. Since $Q_3^m = Q_2^m \sqcup Q_1^m$, by Result 6, $C_2(Q_n^m)^\perp$ has words of weight $m^2$. By induction then $C_2(Q_n^m)^\perp$ has words of weight $m^{n-1}$.

If $m$ is even, then $C_2(Q_n^m)^\perp$ has dimension 2, and contains vectors of weight $\frac{m^2}{2}$. The same argument as for the odd case, but using $\frac{m^2}{2}$ instead of $m$, shows that $C_2(Q_n^m)^\perp$ has words of weight $\frac{m^{n-1}}{2^{n-1}}$. \qed

**Lemma 3.5.** For $4 \leq m$, the minimum weight of $C_2(Q_n^m)^\perp$ is $m$.

**Proof.** Let $w \in C_2(Q_n^m)^\perp$ have support $S$ and $|S| = s$. We can suppose $< 0, 0 \in S$. Every row $r_x$ of $A_{2,m}$ that contains $< 0, 0 \in S$ must meet $S$ again. Now $r_{<0,0>} = \{< 1, 0>, < 1, 1>, < 1, 0>, < 0, 1>, < 0, 0>, \}$, and

$$r_{<1,0>} = \{< 0, 0>, < 2, 0>, < 1, 1>, < 1, 1>, < 0, 1>, < 1, 0>, \}$$

$$r_{<1,0>} = \{< 0, 0>, < 2, 0>, < 1, 1>, < 1, 1>, < 0, 1>, < 1, 0>, \}$$

$$r_{<1,0>} = \{< 0, 0>, < 2, 0>, < 1, 1>, < 1, 1>, < 0, 1>, < 1, 0>, \}$$

Taking $S$ as small as it can be, all these blocks will meet $S$ again if we include the two points $< 1, 1>, < 1, 0>, < 1, 1>, < 1, 0>$. Since all blocks containing $< 1, 1, 0> \in S$ again, we consider $r_{<1,1>} = \{< 1, 0>, < 1, 2>, < 0, 1>, < 2, 1>, \}$. Then

$$r_{<1,2>} = \{< 1, 1>, < 1, 3>, < 0, 2>, < 2, 2>, \}$$

$$r_{<2,1>} = \{< 1, 1>, < 3, 1>, < 2, 0>, < 2, 2>, \}.$$

Thus a further point $< 2, 2 \in S$ must be included, so that $S$ contains the set $\{< 0, 0, 0>, < 1, 1>, < 0, 2>, < 2, 2>, \}$. If $m = 4$ this is the set $\Lambda$ of Proposition 1, so 4 is the minimum weight for $m = 4$. Otherwise we need to make sure that all the blocks through $< 1, 1, 1> \in S$ again. Now $r_{<1,1>} = \{< 1, 0>, < 1, 2>, < 0, 1>, < 0, 0>, < 2, 2>, \}$, and

$$r_{<1,2>} = \{< 1, 1>, < 1, 3>, < 0, 2>, < 2, 2>, \}$$

$$r_{<2,1>} = \{< 1, 1>, < 3, 1>, < 2, 0>, < 2, 2>, \}.$$

Thus including $< 2, 2 >$ will ensure that all blocks through $< 1, 1, 1> \in S$ again. For $m = 4$, $< 2, 2 >$ is needed but for $m = 4$ this is a new point. Thus the set $S$ contains at least the five points $T = \{< 0, 0>, < 1, 1>, < 0, 2>, < 2, 2>, \}$. For $m = 5$ this is precisely the set $\Lambda$ of Proposition 1.

We now proceed in this way by induction on $m$, knowing it is true for $m \leq 5$.

Suppose we have $S = \{< 0, 0>, < 1, 1>, < 1, 1>, < 1, 1>, \ldots, < k, k>, < -k, -k>, \}$,
of the Proposition 1. Writing $C = [N, n, d]_2$ code and $Q_{m}^{n}\parallel\perp$ is a $[8^n, 8^{n-1}6, 2n]_2$ code. 

For the next proposition we introduce a new notation for $n = 2$ to clarify the proof. For any $<x, y> \in V$, we write for its neighbours,

$$\text{(5)} \quad (x, y) = N(<x, y>) = \{<x, y \pm 1>, <x \pm 1, y>\} = r_{<x, y>}.$$ 

We sometimes refer to the $(x, y)$ as blocks, considering the neighbourhood design of the graph. The row $r_{<x, y>}$ would then be considered as the incidence vector of the block.

**Proposition 2.** For $m \geq 5$ odd, $C_2(Q_m^n)$ is LCD. Furthermore, $C_2(Q_m^n)$ is a $[m^2, (m - 1)^2, 4]_2$ code and $C_2(Q_m^n)^\perp$ is a $[m^2, 2m - 1, m]_2$ code.

**Proof.** We show that $w = v^{<0,0>} + u_0 + \sum_{i=1}^{m-1} v_i \in C_2(Q_m^n)$, using the notation of the Proposition 1. Writing $C = C_2(Q_m^n)$, this will show that $F D^2 = C \oplus D$, where the code $D$ is as in Proposition 1, and since $\text{dim}(D) = 2m - 1$, it implies that $\text{dim}(C) = m^2 - 2m + 1 = (m - 1)^2$. So $C\perp = D$ and $C$ is LCD.

It is easy to verify that if $S_m = \text{Supp}(w)$, then

$$S_m = \{<a + b, a >| a \in R, b \in R, b \neq 0\} \setminus \{<a, a>| a \in R\}.$$ 

Note that $<a, b> \in S_m$ if and only if $<b, a> \in S_m$, and $<a, a> \notin S_m$ for any $a \in R$. It follows that $|S_m| = \text{wt}(w) = (m - 1)^2$.

To show that $w \in C_2(Q_m^n)$ we find a set of rows of the adjacency matrix $A$ that sum up to $w$. The set taken will differ for $m \equiv 1 \pmod{4}$ and $m \equiv 3 \pmod{4}$. Thus, for $m \equiv 1 \pmod{4}$ let

$$\text{(6)} \quad B_m = \{(2i, 2i + 2 + 4r), (2i + 3 + 4r) | i, r \geq 0, 2i + 3 + 4r \leq \frac{m - 1}{2}\},$$ 

and for $m \equiv 3 \pmod{4}$ let

$$\text{(7)} \quad B_m = \{(2i, 2i), (2i, 2i + 3 + 4r), (2i + 4 + 4r) | i, r \geq 0, 2i + 4 + 4r \leq \frac{m - 1}{2}\}.$$ 

Then in either case we define our full set of rows by

$$B_m^* = B_m \cup \{(\pm x, \mp y), (y, x) | (x, y) \in B_m\}.$$
We will show that \( w = \sum_{(x,y) \in \mathcal{B}_m} r^{<x,y>} \).

Thus the members of \( \mathcal{B}_m \) produce one, four or eight blocks in \( \mathcal{B}_m^* \): (0, 0) gives just the one block, \((a, a)\) for \( a \neq 0 \) gives four, \(viz.\) \((a, a), (-a, a), (a, -a), (-a, -a)\). Likewise \((0, a)\) for \( a \neq 0 \) gives four, while for \( a \neq b \), and neither \(0, (a, b)\) gives eight:

\[(a, b), (-a, b), (a, -b), (-a, -b), (b, a), (b, -a), (-b, a), (-b, -a).\]

Below we will show that \(|\mathcal{B}_m^*| = (\frac{m-1}{2})^2\).

For example, Table 1 shows the blocks \((a, b)\) in \( \mathcal{B}_m \) for \( 5 \leq m \leq 19 \) odd. The parentheses have been omitted to save space.

| \( m \) | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
|-----|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|
| 5   | 0  | 2  |
| 7   | 0  | 0  | 0.3| 2  | 2  |
| 9   | 0  | 0.2| 0.3| 2  | 4  |
| 11  | 0  | 0.0| 0.3| 0.4| 2  | 2.2| 2.5| 4  | 4  |
| 13  | 0  | 0.2| 0.3| 0.6| 2.4| 2.5| 4  | 4  | 4.6|
| 15  | 0  | 0.0| 0.3| 0.4| 0.7| 2.2| 2.5| 2.6| 4  | 4  | 4.7| 6  | 6.6|
| 17  | 0  | 0.2| 0.3| 0.6| 0.7| 2.4| 2.5| 2.8| 4  | 4  | 4.7| 6  | 6.8|
| 19  | 0  | 0.0| 0.3| 0.4| 0.7| 0.8| 2.2| 2.5| 2.8| 4  | 4  | 4.7| 4.8| 6  | 0  | 0  | 8.8|

Table 1. Blocks in \( \mathcal{B}_m \)

The cases \( m \equiv 1 \quad (\mod 4) \) and \( m \equiv 3 \quad (\mod 4) \) need to be taken separately, and in fact each case breaks down again into two cases depending on \( m \) modulo 8.

To show that \(|\mathcal{B}_m^*| = (\frac{m-1}{2})^2\) it is simplest to exhibit the elements of \( \mathcal{B}_m \) in an array of rows \( \mathcal{B}_m(i) \) where for \( m \equiv 1 \quad (\mod 4) \)

\[ \mathcal{B}_m(i) = \{(2i, 2i + 2 + 4r), (2i + 3 + 4r) \mid r \geq 0, 2i + 3 + 4r \leq \frac{m-1}{2}\} \]

and for \( m \equiv 3 \quad (\mod 4) \)

\[ \mathcal{B}_m(i) = \{(2i, 2i), (2i, 2i + 3 + 4r), (2i + 4 + 4r) \mid r \geq 0, 2i + 4 + 4r \leq \frac{m-1}{2}\} \]

for \( i \geq 0 \). We need first to determine how many of these rows there are and this depends on \( m \) modulo 8. Recall that for \((a, b) \in \mathcal{B}_m, a, b \leq \frac{m-1}{2}\).

Case (1): \( m \equiv 1 \quad (\mod 4) \)

Thus here \( m = 1 + 4k \) and \( \frac{m-1}{2} \) is even, and \( m \equiv 1, 5 \quad (\mod 8) \). Recall that

\[ \mathcal{B}_m = \{(2i, 2i + 2 + 4r), (2i + 3 + 4r) \mid i \geq 0, 2i + 3 + 4r \leq \frac{m-1}{2}\} \]

Subcase 1(a) \( m \equiv 1 \quad (\mod 8) \).

Here \( m = 1 + 8l \) and \( \frac{m-1}{2} = 4l \). To find the last row, i.e. the highest value of \( i \), we cannot have \( 2i = \frac{m-1}{2} \) since then \( 2i + 2 + 4r > \frac{m-1}{2} \). If \( 2i = \frac{m-1}{2} - 2 = \frac{m-5}{2} \) then \( 2i + 2 + 4r = \frac{m-1}{2} \) for \( r = 0 \), and we have \( \mathcal{B}_m\left(\frac{m-5}{4}\right) = \{\left(\frac{m-5}{2}, \frac{m-5}{2}\right)\} \), i.e. just the one term. The number of rows in the array is thus \( \frac{m-5}{4} + 1 = \frac{m-1}{4} \).

For the row \( \mathcal{B}_m(0) \), the final term will be \((0, \frac{m-3}{2})\) with \( r = \frac{m-9}{8} \). Thus the number of terms in the row \( \mathcal{B}_m(0) \) is \( 2(r + 1) = \frac{m-1}{4} \). For \( \mathcal{B}_m(1) \) we have \( 2 + 2 + 4r = \frac{m-1}{2} \) for \( r = \frac{m-9}{8} \) and the last term is \( (2, \frac{m-3}{2}) \), and the number of entries in the row is \( 2r + 1 = \frac{m-1}{4} - 1 \), i.e. one less than the row above. Clearly each row will decrease by one as we go down with the last entries alternating from \((0, \frac{m-3}{2}), (2, \frac{m-3}{2}), (4, \frac{m-3}{2}), \ldots, (\frac{m-5}{2}, \frac{m-1}{2})\).
We can now count the number of elements of $B_m^*$. The first row of the array each give four entries, and the remainder each give eight. Thus the total is

$$4\left(\frac{m-1}{4}\right) + 8 \left(\frac{m-1}{4} - 1 + \frac{m-1}{4} - 2 + \ldots + \frac{m-1}{4} - 3 - \frac{m-5}{4}\right) = \left(\frac{m-1}{2}\right)^2.$$

We now show that every $x, y \in S_m$ is in an element of $B_m^*$. Since $|S_m| = (m-1)^2$ and there are four points on each $(a, b) \in B_m^*$, and $|B_m^*| = \left(\frac{m-1}{2}\right)^2$, this will show that the blocks $(a, b) \in B_m^*$ are mutually disjoint and that $w = \sum_{(x,y) \in B_m^*} r_{x,y}$.

First note that since $x, y \in S_m$ if and only if $-x, y \in (-a, b)$, we only need to show that each $x, y \in S_m$ for $x < y \leq \frac{m-1}{2}$.

(i) $x, y$ both even.

Then $x = 2i$ and $y \leq \frac{m-1}{2}$. If $y < \frac{m-1}{2}$ and $y = 2i + 2 + 4r$, then $x, y \in (2i, 2i + 3 + 4r) \in B_m$; if $y = 2i + 4r = 2i + 4 + 4(r - 1)$, then $x, y \in (2i, 2i + 3 + 4(r - 1)) \in B_m$.

If $y = \frac{m-1}{2}$ then $y = 2i + 2 + 4r$ or $y = 2i + 4r$. In the first case $(x, y) = (2i, 2i + 2 + 4r) \in B_m$, i.e. $(2i, \frac{m-1}{2}) \in B_m$. In this case $(2i, -\frac{m-1}{2}) \in B_m^*$, and $(2i, -\frac{m-1}{2}) = (2i, \frac{m+1}{2} + 1) \geq 2i, \frac{m+1}{2} + 1 > 2i, \frac{m+1}{2}$, so $x, y \notin B_m^*$. If $y = \frac{m-1}{2} = 2i + 4r = 2i + 4 + 4(r - 1)$, then $x, y \in (2i, 2i + 3 + 4(r - 1)) \in B_m$.

(ii) $x$ even, $y$ odd, $x < y$.

Then $x = 2i$ and $y = 2i + 1 + 4r$ or $2i + 3 + 4r$. In either case $x, y \in (2i, 2i + 2 + 4r) \in B_m$.

(iii) $x$ odd, $y$ even, $x < y$.

Then $x = 2i + 1, y = 2i + 2j$, i.e. $2i + 2 + 4r$ or $2i + 4r$. In the first case, $< 2i + 1, 2i + 2 + 4r \geq (2i, 2i + 2 + 4r) \in B_m$. If $y = 2i + 4r = 2i + 4 + 4(r - 1) = 2(i + 1) + 2 + 4(r - 1)$, then $x, y \in (2(i + 1), 2(i + 1) + 2 + 4(r - 1)) \in B_m$.

(iv) $x < y$ both odd.

Then $x = 2i + 1, y = 2i + 1 + 2j$, i.e. $2i + 1 + 2 + 4r = 2i + 3 + 4r$ or $2i + 1 + 4r$. If the former, then $< 2i + 1, 2i + 3 + 4r \geq (2i, 2i + 3 + 4r) \in B_m$, and if the latter, then $y = 2i + 1 + 4r = 2(i + 1) + 1 + 4r = 2(i + 1) + 3 + 4(r - 1)$, and $< 2i, 2i + 1 + 4r \geq (2(i + 1), 2(i + 1) + 3 + 4(r - 1)) \in B_m$ since $x \neq \frac{m-1}{2}$ because $y < \frac{m-1}{2}$. This completes all possibilities for $m \equiv 1 \pmod{8}$.

Subcase 1(b) $m \equiv 5 \pmod{8}$.

Here $m = 5 + 8l$ and $\frac{m-1}{2} = 1 + 2l$. As in (a), the last row is $B_m(\frac{m-5}{4}) = \{(\frac{m-3}{2}, \frac{m-1}{2})\}$. There are $\frac{m-1}{4}$ rows for $i = 0, 1, \ldots, \frac{m-1}{4}$, and the last term in the first row, $B_m(0)$, is $(0, \frac{m-1}{2})$ where $\frac{m-1}{2} = 2 + 4r$ and $r = \frac{m-5}{8}$. For $B_m(1)$ the last term is $(2, \frac{m-3}{2})$ where $\frac{m-3}{2} = 2 + 3 + 4r$ for $r = \frac{m-5}{8} - 1$.

The last rows decrease by one entry as we descend and the last entries alternate $(0, \frac{m-1}{2}), (2, \frac{m-3}{2}), (4, \frac{m-1}{2}), \ldots, (\frac{m-5}{2}, \frac{m-1}{2})$.

The count of the number of elements of $B_m^*$ follows exactly as in 1(a), and gives $\left(\frac{m-1}{2}\right)^2$. To check that every $x, y \in S_m$ for $x < y$ is in an element of $B_m^*$ follows exactly as in 1(a) since the set $B_m^*$ is given by the same formula, and the arguments as to when $\frac{m-1}{2}$ is $y$ depends only on congruence of $m$ modulo 4.

Case (2): $m \equiv 3 \pmod{4}$

Thus here $m = 3 + 4k$ and $\frac{m-1}{2}$ is odd, and $m \equiv 3, 7 \pmod{8}$. Recall that

$$B_m = \{(2i, 2i), (2i, 2i + 3 + 4r), (2i + 4 + 4r) | i, r \geq 0, 2i + 4 + 4r \leq \frac{m-1}{2}\}.$$
Since $m^{-1}$ is odd, the last row of the array for $B_m$ will have $i = m^{-3}/2$ and consist of $(m^{-3}/2, m^{-3}/2)$ for either congruence modulo 8.

**Subcase 2(a) $m \equiv 3 \pmod{8}$**

The last row is $B_m(m^{-3}/4) = \{(m^{-3}/2, m^{-3}/2)\}$. There are $m^{-3}/4 + 1 = m^{-1}/2$ and $m^{-1}/2$ terms in $B_m(0)$. The last term on $B_m(0)$ is not $(0, m^{-1}/2)$ since $m^{-1}/2$ is odd and if $m^{-1}/2$ is $3 + 4r$ we would have $r = m^{-7}/8$. For the last term to be $(0, m^{-3}/4)$ we would have $m^{-3}/2 = 4 + 4r$, so $r = m^{-3}/4$. The number of terms in $B_m(0)$ is then $1 + 2(m^{-11}/8 + 1) = m^{-1}/2$ as expected. For $B_m(1)$, $m^{-1}/2 = 2 + 3 + 4r$ for $r = m^{-11}/8$, so the number of terms in $B_m(1)$ is $1 + 2(m^{-11}/8 + 1) + m^{-3} = m^{-1}/2 - 1$, and the number of terms decrease as we descend, with the last entries the rows alternating $(0, m^{-3}/2), (2, m^{-3}/2), (4, m^{-3}/2), \ldots, (m^{-3}/2, m^{-3}/2)$.

To count the number of blocks in $B_m^n$, note first that, apart from the first entry $(0,0)$, the first row and first column only produce four blocks each in $B_m^n$, so for these we get $1 + 4.2(m^{-1}/4 - 1) = 2m - 5$. For the remaining elements in each row we get eight blocks each. For the array from $B_m(1)$ we get $m^{-3}/2 - 1$, for the next row $m^{-3}/2 - 2$, and so on for the last row $B_m(m^{-3}/4)$ we get zero. The number in $B_m$ in this count is thus $(m^{-3}/2)^2 - 1 = (m^{-3}/4)(m^{-1}/2) = (m^{-3}/8)(m - 3)(m - 7)$, and then counting for $B_m^n$ gives

$$2m - 5 + \frac{8}{32}(m - 3)(m - 7) = \left(\frac{m - 1}{2}\right)^2,$$

as expected.

We now show that every $x, y \in S_m$ is in an element of $B_m^n$, using similar arguments as in the case $m \equiv 1 \pmod{8}$. Thus we only need consider $x < y < m^{-1}/2$. Note that $m^{-1}/2$ is odd here.

(i) $x, y$ both even.

So $y < m^{-1}/2$. If $x = 2i$ and $y = 2i + 4 + 4r < m^{-1}/2$, then $< x, y > \in (2i, 2i+3+4r) \in B_m$. If $y = 2i + 2 + 4r$ then $< x, y > \in (2i, 2i + 3 + 4r)$ which is in $B_m$ as long as $2i + 3 + 4r < m^{-1}/2$. This is true since if $2i + 3 + 4r < m^{-1}/2$ then $2i + 2 + 4r > m^{-1}/2$ so $2i + 2 + 4r \geq m^{-3}/2 + 2 = m^{-1}/2$ contradicting our choices.

(ii) $x$ even, $y$ odd.

Then $x = 2i$, $y = 2i + t$ where $t$ is odd. First suppose $y = m^{-1}/2$. Then $< x, y > \in (x, y + 1) = (x, m^{-1}) = (x, m^{-3}/2)$. So if $(x, m^{-1}/2) \in B_m$ then $< x, y > \in (x, m^{-1}/2) + 1 = (x, m^{-1}/2) \in B_m,$ and if $(x, m^{-1}/2) \not\in B_m,$ then $< x, y > \in (x, m^{-1}/2) - 1 = (x, m^{-3}/2) \in B_m.$

If $y < m^{-1}/2$ then if $y = 2i + 1 + 4r$, and $r = 0$, $< x, y > \in (2i, 2i); if r > 0$ then $y = 2i + 5 + 4(r - 1)$ and $< x, y > \in (2i, 2i + 4 + 4(r - 1)) \in B_m.$ If $y = 2i + 3 + 4r < m^{-1}/2$ then $< x, y > \in (2i, 2i + 4 + 4r) \in B_m$ since $y < m^{-3}/2 - 2$ implies $y + 1 < m^{-3}/2$.

(iii) $x$ odd, $y$ even.

So $x = 2i + 1$, $y = 2i + 2j = 2i + 2 + 4r$ or $2i + 4 + 4r$. Since $x < y < m^{-1}/2$, clearly $x < m^{-1}/2$ and in fact $x < m^{-3}/2$. If $y = 2i + 4 + 4r$, then $< 2i + 1, 2i + 4 + 4r > \in (2i, 2i + 4 + 4r) \in B_m.$ If $y = 2i + 2 + 4r$, then if $r = 0, < x, y > = < 2i + 1, 2(i + 1) > \in (2i + 1, 2(i + 1)) \in B_m$ since $2(i + 1) \leq m^{-3}/2$. If $r \neq 0$ then $y = 2(i + 1) + 4 + 4(r - 1)$ and $< 2i + 1, 2(i + 1) + 4 + 4(r - 1) > \in (2i + 1, 2(i + 1) + 4 + 4(r - 1)) \in B_m.$

(iv) Both $x$ and $y$ odd.

Here $x = 2i + 1$, $y = 2i + 2j = 2i + 1 + 2 + 4r (r \geq 0)$ or $2i + 1 + 4r (r > 0).$ If $y = 2i + 1 + 4r = 2i + 1 + 2 + 4r$ then $< 2i + 1, 2i + 3 + 4r > \in (2i, 2i + 3 + 4r) \in B_m.$ If $y = 2i + 1 + 4r = 2(i + 1) + 3 + 4(r - 1)$, then $< 2i + 1, 2(i + 1) + 3 + 4(r - 1) > \in (2(i + 1), 2(i + 1) + 3 + 4(r - 1)) \in B_m$ since $2i + 2 \leq m^{-3}/2$. 

**Advances in Mathematics of Communications Volume X, No. X (200X), X–XX**
This completes the proof for \( m \equiv 3 \pmod{8} \).

**Subcase 2(b) \( m \equiv 7 \pmod{8} \).**

The proof here will mostly be as that in 2(a). The last row is again \( B_m(\frac{m-3}{2}, \frac{m-3}{2}) \), so again there are \( \frac{m+1}{2} \) rows. The last term in \( B_m(0) \) is \( (0, \frac{m-1}{2}) \) since \( \frac{m-1}{2} = 3 + 4r \) for \( r = \frac{m-7}{8} \). The number of terms in \( B_m(0) \) is \( 2(\frac{m-7}{8} + 1) = \frac{m+1}{2} \). The last term of \( B_m(2) \) is \( (2, \frac{m-3}{2}) \) and these last entries alternate as before, and the rows decrease in length by 1 as we descend. The count is thus the same as in (a), and \( |B^*_m| = (\frac{m-1}{2})^2 \). Likewise, to check that every \( x, y \in S_m \) for \( x < y \) is in an element of \( B^*_m \), follows exactly as in 2(a) since the set \( B^*_m \) is given by the same formula, and the arguments as to when \( \frac{m-1}{2} \) is \( y \) depends only on congruence of \( m \) modulo 4.

This completes the proof that the code is LCD. For the other code parameters, i.e. the minimum weights, refer to Lemmas 3.3 and 3.5.

**Note:** Proposition 2 holds also for \( m = 3 \), where the graph is a Hamming graph: see [8, Theorem 1].

**Examples of arrays for \( B_m \):**

\[
\begin{align*}
\text{m = 21:} & \quad \begin{bmatrix}
0,2 & 0,3 & 0,6 & 0,7 & 0,10 \\
2,4 & 2,5 & 2,8 & 2,9 \\
4,6 & 4,7 & 4,10 \\
6,8 & 6,9 \\
8,10
\end{bmatrix}, \\
\text{m = 23:} & \quad \begin{bmatrix}
0,0 & 0,3 & 0,4 & 0,7 & 0,8 & 0,11 \\
2,2 & 2,5 & 2,6 & 2,9 & 2,10 \\
4,4 & 4,7 & 4,8 & 4,11 \\
6,6 & 6,9 & 6,10 \\
8,8 & 8,11 \\
10,10
\end{bmatrix}.
\end{align*}
\]

**Examples of \( \langle x, y \rangle \in (a, b) \in B^*_m, x \neq \pm y \)**

1. \( m = 21: < 4,9 > = < 4,4+5 > = < 4,4+1+4 > \in (4,4+2+4) = (4,10) \in B_{21} \).
2. \( m = 21: < 5,8 > = < 5,5+3 > = < 5,6+2 > \in (6,8) \in B_{21} \).
3. \( m = 21: < 13,15 > = < 13,15 > \in (6,6+3) = (6,9) \in B_{21} \), so \( < 13,15 > \in (12,15) \in B^*_m \).
4. \( m = 19: < 7,5 > = < 4,1+4+3 > \in (4,7) \in B_{19} \), so \( < 7,5 > \in (7,4) \in B^*_m \).
5. \( m = 19: < 11,16 > = < 8,3 > = < 3,8 > > = < 3,3+1+4 > \in (4,8) \in B_{19} \), so \( < 11,16 > \in (8,4) \in (11,15) \in B^*_m \).

We can use Result 2 to get the orthogonal projector map for the code \( D = C_2(Q^m_2)^\perp \) for \( m \) odd.

**Corollary 2.** For \( m \geq 5 \) odd, let \( G \) be the generator matrix for \( D = C_2(Q^m_2)^\perp \) with rows given by the vectors \( u_0, \ldots, u_{m-1}, v_0, \ldots, v_{m-2} \) and columns in the natural order \( < 0,0 >, < 0,1 >, \ldots, < m-1,m-1 > \). Then if \( J_{r,t} \) denotes the all-one matrix of size \( r \times t \) over \( F_2 \), then

\[
M = GG^T = \begin{bmatrix}
I_m & J_{m,m-1} \\
J_{m-1,m} & I_{m-1}
\end{bmatrix},
M^{-1} = \begin{bmatrix}
I_m & J_{m,m-1} \\
J_{m-1,m} & I_{m-1} + J_{m-1,m-1}
\end{bmatrix}.
\]
Furthermore, \( v \Pi_D = vG^T M^{-1}G \) for any \( v \in \mathbb{F}_2^{m^2} \).

**Proof.** The proof follows immediately, since the distinct \( u_i \) meet in no points, and likewise the distinct \( v_i \), while each \( u_i \) meets each \( v_j \) exactly once. The inverse is simple to check. \( \square \)

**Lemma 3.6.** If \( \Gamma_i \), for \( i = 1, 2 \) are bipartite graphs, then so is \( \Gamma_1 \Box \Gamma_2 \), and hence also \( \Gamma_{i,m} \) if all the \( \Gamma_i \) are bipartite.

**Proof:** Let \( V_1, V_2 \) be the partition of vertices for \( \Gamma_1 \), and \( W_1, W_2 \) that for \( \Gamma_2 \). Then it is easy to see that bipartite sets for \( \Gamma_1 \Box \Gamma_2 \) are

\[
V_1 \times W_1 \cup V_2 \times W_2, \text{ and } V_1 \times W_2 \cup V_2 \times W_1.
\]

This extends obviously to the product of any number of bipartite graphs. \( \square \)

**Corollary 3.** If \( m \) is even then \( Q_m^n \) is bipartite.

**Proof:** This is clear since \( Q_1^m \) is clearly bipartite with the two classes of vertices being the even numbers and the odd numbers. \( \square \)

**Note:** That for \( m \) even, \( Q_m^n \) is bipartite is also mentioned in [2].

### 4. Permutation decoding for \( C_2(Q_2^n)\perp \) for \( m \) odd

We will show that \( s \)-PD-sets of smallest size \( s + 1 \) can be found for the codes \( C_2(Q_2^n)\perp \) for \( m \geq 5 \) odd.

**Lemma 4.1.** For \( \Gamma = Q_2^n \) where \( m \geq 5 \) is odd, \( R = \{0, \ldots, m-1\} \), the set

\[
\mathcal{I} = \{< 0, i > | i \in R \} \cup \{< 1, i > | i \in R \setminus \{m-1\}\}
\]

is an information set for \( C_2(\Gamma)\perp \).

**Proof.** Use the notation of Proposition 1. Consider the words that generate the code \( D = C_2(\Gamma)\perp \), viz. \( u_0, \ldots, u_{m-1}, v_0, \ldots, v_{m-1} \), and write them as rows of a \( 2m \times m^2 \) generating matrix for \( D \), but with the rows in the order

\[
u_0, u_{m-1}, u_{m-2}, \ldots, u_1, v_0, v_{m-1}, v_{m-2}, \ldots, v_1,
\]

and columns in the natural order \( (0,0), (0,1), \ldots, (m-1, m-1) \). We consider only the first \( 2m \) columns, from \( (0,0) \) to \( (1, m-1) \) as we know \( D \) has dimension \( 2m-1 \). Then the non-zero entries in these columns are: \( u_0 \ni < 0, 0 >, < 1, 1 >; u_{m-1} \ni < 0, 1 >, < 1, 2 >; u_{m-2} \ni < 0, 2 >, < 1, 3 >; \ldots; u_1 \ni < 0, m-1 >, < 1, 0 >; v_0 \ni < 0, 0 >, < 1, m-1 >; v_{m-1} \ni < 0, 1 >, < 1, 2 >; \ldots; v_1 \ni < 0, m-1 >, < 1, m-2 >.

Now use the first \( m \) rows, which have leading entries \( < 0, 0 >, \ldots, < 0, m-1 > \) to remove the similar leading entries in the second set of \( m \) rows, with the new ordered rows \( u_0, u_{m-1}, \ldots, u_1, v_0^* = v_0 + u_0, v_{m-1}^* = v_{m-1} + u_{m-1}, \ldots, v_1^* = v_1 + u_1 \).

Considering now the lower \( m \) rows starting with \( v_0^* \), and columns starting at \( < 1, 0 > \), we have \( v_0^* \ni < 1, 1 >, < 1, m-1 >; v_{m-2}^* \ni < 1, 1 >, < 1, 3 >; \ldots; v_1^* \ni < 1, m-2 >, < 1, 0 >. \) Reorder these rows as \( v_{m-1}^*, v_{m-2}^*, \ldots, v_1^*, v_0^* \). Now replace the row of \( v_1^* \) by \( v_1^{*\ast} = v_1^* + v_{m-3}^* + v_{m-1}^* \ni < 1, m-3 >, < 1, m-2 > \), and \( v_0^* \) by \( v_0^{*\ast} = v_0^* + v_{m-4}^* + v_{m-2}^* \ni < 1, m-3 >, < 1, m-2 > \). In the first \( 2m-1 \) columns the last three new rows corresponding to \( v_2^*, v_1^{*\ast}, v_0^{*\ast} \) have rank 2.

Thus \( \mathcal{I} \) is an information set of \( D \). \( \square \)
Recall that for $\Gamma = Q^m_2$, $\text{Aut}(\Gamma) \cong <T, Q>$, where $T$ is the translation group of order $m^2$ and $Q$ has order 8 and is the quaternion group of this order. This group is generated by the translations $\tau_{<a,b>}$, $\mu_0, \mu_1, \sigma$ where $<x, y> = <y, x>$. Then $\tau_{<a,b>} = \tau_{<-a,b>}$.

Proposition 3. Let $\Gamma = Q^m_2$ where $m \geq 5$ is odd, $R = \{0, ..., m-1\}$. Then for $s < \frac{m-1}{2}$, the set of automorphisms

$$S = \{\tau_{<2i,0>} | 0 \leq i \leq s\}$$

is an s-PD-set of minimal size $s+1$ for the code $C_2(\Gamma)^\bot$ with information set $\mathcal{I}$ as given in Equation (8).

The group $T = \{\tau_X | X \in R^2\}$ is a PD-set for full error correction.

Proof. By Proposition 2, $C = C_2(\Gamma)^\bot$ is an $[m^2, 2m-1, m]_2$ code for $m$ odd. Thus the code can correct $t = \frac{m-1}{2}$ errors. It is quite straightforward to show that the bound $G(t)$ in Equation (4) is $\frac{m+3}{2} = \frac{m-1}{2} + 2 = t + 2$. Result 4 tells us that if $G(s) = s + 1$ then $s \leq \left\lfloor \frac{m^2}{2m-1} \right\rfloor - 1$ which is $\frac{m-3}{2} = \frac{m-1}{2} - 1 = t - 1$ here. Thus we take $s \leq \frac{m-3}{2}$ and show that the set $S$ of Equation (9) of size $s + 1$ will correct $s$ errors for $m \geq 2s + 3$.

If all the $s$ errors are in $\mathcal{I}$ then any non-identity element of $S$ will take them all into $C$, and if all the $s$ errors are in $C$ then the identity $\tau_{<0,0>}$ will keep all the errors in $C$. Since any number of errors in $\mathcal{I}$ can be corrected by any non-identity element of $S$, we assume there are $s - 1$ errors in $\mathcal{C}$ and one in $\mathcal{I}$. If we prove our result for such a set it will follow for any smaller number.

Suppose the errors in $\mathcal{C}$ occur at $e_r = <i_r, j_r>$ for $1 \leq r \leq s - 1$, with $e_0 \in \mathcal{I}$ the error in $\mathcal{I}$. So $2 \leq i_r \leq m - 1$ for $1 \leq r \leq s - 1$. Since $\tau_{<2i,0>} = (\tau_{<2,0>})^i$, we see that the set of images of $i_r$ under the elements of $S$ are all distinct and all have the same parity until $m - 2$ or $m - 1$ is reached, (for odd or even respectively), after which 0 or 1 occurs and the parity changes. Thus any set of $s$ images $i_r + 2i$, for $1 \leq i \leq s$ can contain 0 or 1 only once, and never both, since $s \leq \frac{m-3}{2}$. There are $s - 1$ points $e_r$, so considering the $s$ sets of images of these points under non-identity elements of $S$, i.e. $\{e_{\tau_{<2i,0>}} | 1 \leq r \leq s - 1\}$ for $1 \leq i \leq s$, there must be a value of $i$ such that neither 0 nor 1 is in that image, i.e. the points are all in $C$. This $\tau_{<2i,0>}$ will move the full set of $s$ error positions to $C$.

Thus $S$ is an $s$-PD-set for $s \leq \frac{m-3}{2}$ of $s + 1$ elements.

For the last part of the statement we use Result 5. The group $T$ is transitive on vertices, and $\left\lfloor \frac{m^2}{2m-1} \right\rfloor$ is easily seen to be $\frac{m+1}{2}$, and thus the value of $s$ in that result is $t = \frac{m-1}{2}$, so $T$, of size $m^2$, will provide full error correction.

Note: 1. To use the maximal error-correction capacity of the code, $t = \frac{m-1}{2} + 2 = t + 2$ as mentioned above. Computationally with Magma we found that for $m = 5$, where $t = 2$, and $G(t) = 4$, 2-PD-sets of size 6 were found; for $m = 7$ where $t = 3$ and $G(t) = 5$, 3-PD-sets of size 10 were found; for $m = 9$, where $t = 4$ and $G(t) = 6$, 4-PD-sets of size 9 were found.

2. For $m = 5$, exhaustive searching with Magma yielded a 2-PD-set of size 5 to correct two errors, the error-correction capability of the code. The set obtained was

$$\{\text{Id}, \tau_{<1,3>}, \tau_{<2,3>}, \tau_{<3,0>}, \mu_0 \tau_{<2,3>}\}.$$
5. Magma observations for other $n$, and for $m$ even

1. For $n = 2$ and $m$ even we have not been able to obtain the basic parameters of $C_2(Q^m_2)$ as in the case of $m$ odd but computations with Magma yielded that $C_2(Q^m_2)$, for $m$ even, $4 \leq m \leq 16$, is a $[m^2, m(m-2), 4]_2$ code. The minimum weight of the dual was determined in Lemma 3.5. The codes are not LCD.

2. For $m \geq 5$ odd, Hull$(C) = \{0\}$ for $n = 3$ and $5 \leq m \leq 9$ odd, and also for $n = 4$, $m = 5, 7$.

3. • Indications from Magma suggest that the rows $x$ of an adjacency matrix $A$ for $Q^m_2$ where $m \geq 5$ is odd for $X$ in the check set of $C_2(Q^m_2)\perp$ corresponding to $x$ in Equation (8), i.e. for

$$X \in C = \{<1, m-1>, <2, 0>, <2, 1>, \ldots, <m-1, m-1>\},$$

form a basis for $C_2(Q^m_2)$.

- For an alternative basis set of rows of an adjacency matrix $A_{2,m}$ for $m$ odd we have the following conjecture

**Conjecture 1.** Let $\Gamma = Q^m_2 = (V, E)$ and $R = \{0, 1, \ldots, m-1\}$ where $m \geq 5$ is odd. Suppose that the elements of $R$ are ordered naturally and the vertices of $V = R \times R$ likewise. Suppose the adjacency matrix $A_{2,m}$ for $\Gamma$ has the form as shown in Equation (1), with the column blocks labelled $C_i$ for $0 \leq i \leq m-1$, and the row blocks as $R_i$ for $0 \leq i \leq m-1$, and $A_{1,m}$, the adjacency matrix for $Q^m_1$, on the diagonal. Let $S$ be the set of size $(m-1)^2$ of rows of $A_{2,m}$ consisting of

- the first $(m-1)$ rows of the first $(m-2)$ row blocks $R_i$, i.e. $0 \leq i \leq m-3$;
- the first $\frac{m-1}{2}$ rows of the last two row blocks $R_i$ for $i = m-2, m-1$.

Then $S$ is a linearly independent set.

Notice first that it is clear that the first $m-1$ rows of $A_{1,m}$ are linearly independent and so the first $m-2$ row blocks have dimension $m-1$ each, and the last two have dimension $\frac{m-1}{2}$ each.

Evidence for this conjecture is that we can prove it by hand for $m = 5, 7$ and Magma verifies it for all the odd $m$ tried, i.e. up to $m = 17$. Labelling the rows in $R_i$ as $r_{i,j}$ for $j = 0, \ldots, m-1$, proof by hand involved considering a word $w$:

$$w = \sum_{i=0}^{m-1} \sum_{j=0}^{d_i} \alpha_{i,j} r_{i,j} = 0,$$

where the $\alpha_{i,j} \in F_2$ and $d_i = m-2$ for $0 \leq i \leq m-3$, and $d_i = \frac{m-3}{2}$ for $i = m-2, m-1$. Then using the fact that $w(<i, j>) = 0$ for $0 \leq i, j \leq m-1$, and noting that any $<i,j>$ has a non-zero entry in at most four rows, the coefficients can be shown to be zero.

In fact, for the column blocks $C_j$ for $0 \leq j \leq m-1$, vertices $<j, i>$ for $0 \leq i \leq m-1$, the number $k$ of non-zero entries the the column for $<i, j>$:

- $C_j$: $<0, 0>$, $k = 3$; $<0, i>$, $i \in [1, \frac{m-3}{2}]$, $k = 4$; $<0, i>$, $i \in [\frac{m-1}{2}, m-3]$, $k = 3$; $<0, i>$, $i \in [m-2, m-1]$, $k = 2$;
- $C_j$, $j \in [1, m-4]$: $<j, 0>$, $k = 3$; $<j, i>$, $i \in [1, m-3]$, $k = 4$; $<j, m-2>$, $k = 3$; $<j, m-1>$, $k = 2$.
\[- C_{m-3} : < m - 3, 0 >, k = 3; < m - 3, i >, i \in [1, \frac{m-3}{2}], k = 4; < m - 3, i >, i \in [\frac{m-1}{2}, m-3], k = 3; < m - 3, i >, i \in [m-2, m-1], k = 2; \]

\[- C_j, j = m - 2, m - 1 : < j, 0 >, k = 3; < j, i >, i \in [1, \frac{m-5}{2}], k = 4; < j, \frac{m}{2}, m-3 >, k = 3; < j, \frac{m-1}{2}, m-1 >, k = 2; < j, i >, i \in [\frac{m+1}{2}, m-1], k = 1. \]

For example, it follows immediately from the entries in the relevant column, working successively: 

\[ < m - 1, m - 1 > \Rightarrow \alpha_{m-1,0} = 0; < m - 2, m - 1 > \Rightarrow \alpha_{m-2,0} = 0; < m - 1, m - 2 > \Rightarrow \alpha_{0,m-2} = 0; < m - 2, m - 2 > \Rightarrow \alpha_{m-3,m-2} = 0; \]

for \(0 \leq i \leq m - 3, < i, m - 1 > \Rightarrow \alpha_{i,0} = \alpha_{t,m-2}, \Rightarrow \alpha_{0,0} = \alpha_{m-3,0} = 0; < m - 1, m - 3 > \Rightarrow \alpha_{0,m-3} = 0; < m - 1, 0 > \Rightarrow \alpha_{m-1,1} = 0; < m - 2, m - 3 > \Rightarrow \alpha_{m-3,m-3} = 0. \]

\section*{References}

[1] E. F. Assmus, Jr. and J. D. Key, Designs and Their Codes, Cambridge Tracts in Mathematics, 103. Cambridge University Press, Cambridge, 1992.

[2] B. Bose, B. Broeg, Y. Kwon and Y. Ashir, Lee distance and topological properties of \(k\)-ary \(n\)-cubes, IEEE Trans. Computers, 44 (1995), 1021–1030.

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

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

[5] K. Day and A. E. Al Ayyoub, Fault diameter of \(k\)-ary \(n\)-cube networks, IEEE Trans. Parallel and Distributed Systems, 8 (1997), 903–907.

[6] W. Fish, Binary codes and permutation decoding sets from the graph products of cycles, Appl. Algebra Engrg. Comm. Comput., 28 (2017), 369–389.

[7] W. Fish, J. D. Key and E. Mwambene, LCD codes from products of graphs, In preparation.

[8] W. Fish, J. D. Key and E. Mwambene, Codes, designs and groups from the Hamming graphs, J. Combin. Inform. System Sci., 34 (2009), 169–182.

[9] W. Fish, Codes from Uniform Subset Graphs and Cycle Products, PhD thesis, University of the Western Cape, 2007.

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

[11] W. C. Huffman, Codes and groups, Handbook of Coding Theory, North-Holland, Amsterdam, 1,2 (1998), 1345–1440.

[12] J. D. Key, T. P. McDonough and V. C. Mavron, Partial permutation decoding for codes from finite planes, European J. Combin., 26 (2005), 665–682.

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

[14] J. D. Key, T. P. McDonough and V. C. Mavron, Improved partial permutation decoding for Reed-Muller codes, Discrete Math., 340 (2017), 722–728.

[15] J. D. Key and B. G. Rodrigues, LCD codes from adjacency matrices of graphs, Appl. Algebra Engrg. Comm. Comput., 29 (2018), 227–244.

[16] J. D. Key and B. G. Rodrigues, Special LCD codes from Peisert and generalized Peisert graphs, Graphs Combin., 35 (2019), 633–652.

[17] C. Kravvaritis, Determinant evaluations for binary circulant matrices, Spec. Matrices, 1 (2013), 187–199. http://dx.doi.org/10.2478/spma-2014-0019.

[18] H.-J. Kroll and R. Vincenti, PD-sets related to the codes of some classical varieties, Discrete Math., 301 (2005), 89–105.

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

[20] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes. II, North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.
[21] J. L. Massey, Linear codes with complementary duals, *Discrete Math.*, 106/107 (1992), 337–342.

[22] J. Schönheim, On coverings, *Pacific J. Math.*, 14 (1964), 1405–1411.

Received October 2019; revised December 2019.

*E-mail address:* keyj@clemson.edu

*E-mail address:* bernardo.rodrigues@up.ac.za