AUT Journal of Mathematics and Computing

AUT J. Math. Comput., 4(1) (2023) 1-15
DOI: 10.22060/AJMC.2022.21668.1098

Review Article

Codes from m-ary n-cubes Q_n^m: A survey

Jennifer D. Key*[a], Bernardo G. Rodrigues[b]

[a]*Department of Mathematics, Aberystwyth University, Aberystwyth, SY23 3BZ, UK*
[b]*Department of Mathematics and Applied Mathematics, University of Pretoria, Hatfield 0028, South Africa*

ABSTRACT: We collect together some known results concerning the codes from adjacency matrices of the graph with vertices the nodes of the m-ary n-cube Q_n^m and with adjacency defined by the Lee metric, and include some new results.

Review History:
Received:07 August 2022
Revised:09 November 2022
Accepted:11 November 2022
Available Online:01 February 2023

Keywords:
n-Cubes
Graphs
Codes
Permutation decoding

AMS Subject Classification (2010):
05C50; 94B05; 05B05

(*Dedicated to Professor Jamshid Moori*)

1. Introduction

Linear codes that arise from the linear span over a finite field of an adjacency matrix of a graph, and their use in general coding theory or in classifying the graph, have been studied for some time. The latter property has not been as definitive as it has been in the study of codes from other incidence structures, in particular those from finite planes, as illustrated in [1]. However, some useful coding properties have arisen from the span of adjacency matrices of graphs, some of which may be seen, for example, in [7, 8, 9, 16, 19, 23, 24, 25, 26, 31], to mention but a few, however further references to other classes of graphs are given in these papers. In particular, some of the classes of graphs have large automorphism groups so that permutation decoding might be used; or, some of the codes in the class may be LCD or LCD with the special property that the code from the reflective graph (including the loops) is the dual code, in which case more decoding methods are accessible: see [10, 14, 27, 28].

We concentrate here on codes from adjacency matrices of graphs from the m-ary n-cube Q_n^m with adjacency defined by the Lee metric (see [2, 5]). They are also known as Lee graphs. We look at the linear codes that arise from the row span over a finite field of an adjacency matrix for such a graph, concentrating mostly, but not always, on binary codes.

*Corresponding author.
E-mail addresses: keyj@clemson.edu, bernardo.rodrigues@up.ac.za

Definition 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, $\mathbb{Z}_m$, or, if $m = q$ is a prime power, R could be $\mathbb{F}_m$. The graph $\Gamma = (V, E)$ on Q_n^m, has $V = R^n$, the set of n-tuples with entries in R, with adjacency defined by $x =< x_0, x_1, \ldots, x_{n-1} >$ adjacent to $y =< y_0, y_1, \ldots, y_{n-1} >$ 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 Γ is regular of degree $2n$, or n if $m = 2$.*

Note: In case $m \geq 4$ is even we will use $\mathbb{Z}_m$ rather than the field $\mathbb{F}_m$, since we need $1 \neq -1$, and our graphs to be of valency $2n$.

We will summarize the known results concerning the codes (mostly binary) from the adjacency matrices of these graphs. For $n = 2$, $m \geq 4$, the codes have been shown to contain in their dual codes LCD codes that are very suitable for permutation decoding, with PD-sets of the smallest possible size for $m \geq 4$ even and $R = \mathbb{Z}_m$, and almost as good for $m \geq 5$ odd. For $n \geq 3$, the codes also so promise, but our results are less complete. Computer searches with Magma [3, 4] have shown that they have very similar properties to the case for $n = 2$.

For $m = 2$ the graphs are Hamming graphs and the codes have been rather extensively studied elsewhere, so we only make brief mention of them here. Likewise, for $m = 3$ the graphs are Hamming graphs. We reference some earlier results concerning these codes as relate to our study of codes from the Lee graphs.

The work 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. In Section 3 we summarize the known results concerning the codes (mostly binary) from the adjacency matrices of these graphs. Our new results are mostly in Sections 4, 5, apart from a new observation (Lemma 1) in Subsection 3.2. Finally in Section 6 we show some computational results using Magma [3, 4] for the codes from the graphs with $n \geq 3$.

2. Background concepts and terminology

The notation for codes, graphs and codes from graphs is as in [1]. For an incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{J})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{J}$, the **code $C_F(\mathcal{D}) = C_p(\mathcal{D})$** of $\mathcal{D}$ over the finite field $F = \mathbb{F}_p$, p a prime, is the space spanned by the incidence vectors of the $|\mathcal{B}|$ blocks over F, and has length $|\mathcal{P}|$. If $\mathcal{Q}$ is any subset of $\mathcal{P}$, then we will denote the **incidence vector** of $\mathcal{Q}$ by $\boldsymbol{v}^{\mathcal{Q}}$, writing simply $\boldsymbol{v}^{x}$ if $\mathcal{Q} = \{x\}$ where $x \in \mathcal{P}$. For any $w \in F^{\mathcal{P}}$ and $P \in \mathcal{P}$, $\boldsymbol{w(P)}$ 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 code C over the field $\mathbb{F}_q$, q a prime power, 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. For two vectors u, v the **distance d(u, v)** between them is $\mathrm{wt}(u - v)$. The **support**, $\mathrm{Supp}(v)$, of a vector v is the set of coordinate positions where the entry in v is non-zero. So $|\mathrm{Supp}(v)| = \mathrm{wt}(v)$. 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 $(,)$, i.e. $C^{\perp} = \{v \in F^n \mid (v, c) = 0 \text{ for all } c \in C\}$. The **hull**, $\mathrm{Hull}(C)$, of a code C is the self-orthogonal code $\mathrm{Hull}(C) = C \cap C^{\perp}$. A **check matrix** for C is a generator matrix for $C^{\perp}$. The **all-one vector** will be denoted by $\boldsymbol{\jmath}$, 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 $\boldsymbol{\jmath_m}$. 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 $\mathrm{Aut}(C)$, also called the permutation group of C, and denoted by $\mathrm{PAut}(C)$ in [17].

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 Γ, 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 $|N(x)|$. Γ is **regular** if all the vertices have the same valency. If $x_i x_{i+1}$ for $i = 1$ to $r-1$, and $x_r x_1$ are all edges of Γ, and the vertices x_i are all distinct, then the sequence written $(x_1, \ldots, x_r)$ will be called a **closed path**, or **cycle**, of length r. If for every pair of vertices there is a path connecting them, the graph is **connected**. The **girth** of a graph is the length of the shortest cycle. The **diameter** of a graph is the greatest distance between any two vertices.

An **adjacency** matrix $A = [a_{x,y}]$ for Γ is a $|V| \times |V|$ symmetric matrix with rows and columns labeled by the vertices $x, y \in V$, and with $a_{x,y} = 1$ if $x \sim y$ in Γ, 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 Γ will be the row span of an adjacency matrix A for Γ, 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_n^m

The graphs are defined in Definition 1. If $1 \neq -1$ in R, then Q_n^m is regular of degree $2n$, and if $1 = -1$ then it is regular of degree n, and is a Hamming graph. If $m = |R|$ is even then Q_n^m is bipartite (see [29, Corollary 3], or [2], for example). The girth of Q_n^m is 4, and its diameter is $n\lfloor \frac{m}{2} \rfloor$ (see [5], for example), assuming $1 \neq -1$.

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 τ_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 σ 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 μ_i is defined by

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

where $-x_i = m - x_i$.

It is easy to verify that the translations τ_a for $a \in R^n$ and the permutations σ, for all σ_i, and μ_i for all i, are automorphisms of Γ, and that $\mathrm{Aut}(\Gamma)$ is both vertex and edge transitive.

Q_n^m is the cartesian product $(Q_1^m)^{\square,n}$ of n copies of Q_1^m: see [10], for example. If $A_{n,m}$ denotes the adjacency matrix for Q_n^m 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

$$A_{1,m} = \begin{bmatrix} 0 & 1 & 0 & \cdots 0 & 0 & 1 \\ 1 & 0 & 1 & \cdots 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots 1 & 0 & 1 \\ 1 & 0 & 0 & \cdots 0 & 1 & 0 \end{bmatrix},$$

the matrix for $A_{n,m}$ has the form

$$A_{n,m} = \begin{bmatrix} A_{n-1,m} & I & 0 & 0 & \cdots & 0 & I \\ I & A_{n-1,m} & I & 0 & \cdots & 0 & 0 \\ 0 & I & A_{n-1,m} & I & \cdots & 0 & 0 \\ \vdots & & \vdots & & \vdots & \vdots & \\ 0 & 0 & 0 & 0 & \cdots I & A_{n-1,m} & I \\ I & 0 & 0 & 0 & \cdots & I & A_{n-1,m} \end{bmatrix}, \tag{1}$$

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_1^m,

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

2.2. LCD codes

The background on LCD codes from [37] is described below.

Definition 2. *A linear code C over any field is a* **linear code with complementary dual (LCD)** *code if* $\mathrm{Hull}(C) = C \cap C^{\perp} = \{0\}$.

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** Π_C from F^n to C can be defined as follows: for $v \in F^n$,

$$v\Pi_C = \begin{cases} v & \text{if } v \in C, \\ 0 & \text{if } v \in C^{\perp} \end{cases}, \tag{2}$$

and Π_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 $v \in F^n$,

$$v = v\Pi_C + v\Pi_{C^\perp}. \tag{3}$$

We will use [37, Proposition 4]:

Result 1 (Massey)**.** *Let C be an LCD code of length n over the field F and let φ 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 $\tilde{\varphi} : F^n \mapsto C$ such that*

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

maps each $r \in F^n$ to one of it closest neighbours in C. [2]

The following observation was made in [27, Lemma 1] or [29, Lemma 2.2]:
If C is a q-ary code of length n such that $C + C^\perp = \mathbb{F}_q^n$ then C is LCD.

2.3. Permutation decoding

Permutation decoding was first developed by MacWilliams [36] and involves finding a set of automorphisms of a code called a PD-set. The method is described fully in MacWilliams and Sloane [35, Chapter 16, p. 513] and Huffman [17, Section 8]. In [20] and [33] the definition of PD-sets was extended to that of s-PD-sets for s-error-correction:

Definition 3. *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 $\mathcal{C}$.*

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 convenient 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 frequently with the identity automorphism 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 $S_0 \subset S_1 \ldots \subset S_t$ 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 [15], from a formula due to Schönheim [38], and quoted and proved in [17]:

Result 2. *If S is a PD-set for a t-error-correcting $[n, k, d]_q$ code C, and $r = n - k$, then*

$$|S| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \ldots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \ldots \right\rceil \right\rceil \right\rceil = G(t). \tag{4}$$

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 [22, Lemma 1]:

Result 3. *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 [21, Lemma 7] the following was proved:

[1] Note typographical error on p.338, l.-11, in [37]
[2] Note typographical error on p.341, l.-7, in [37]

Result 4. *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 $s = \min(\lceil \frac{1}{n} \rceil - 1, \lfloor \frac{d-1}{2} \rfloor)$, 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 $\mathcal{O}(nkz)$. Thus one attempts to find s-PD-sets of the smallest possible size, i.e. to attain the lower bound found in Result 4.

3. Survey of previous results

For $m = 2, 3$ the graph is the Hamming graph and the codes of these have been extensively studied, but we will state some results concerning them, for completeness. These are from [11, 12, 13] although they can be found in other references as well. The notation is a little different there: $\Gamma_n^1 = Q_n^2$ in [12, Theorem 1] and $Q_n = Q_n^2$ in [13, Theorem 1]. Note also that for $m = 2$ the graph has valency only of n, as $1 = -1$.

3.1. $m = 2, 3$

For $m = 2$, from [12, Theorem 1] stated only for the integer $k = 1$, i.e. the graphs Q_n^2:

Result 5. *For $n \geq 1$, for the codes $C_p(Q_n^2)$:*

1. *For $p = 2$: if n is even then $C_2(Q_n^2)$ is a $[2^n, 2^{n-1}, n]_2$ self-dual code; if n is odd, $C_2(Q_n^2)$ is the full space $\mathbb{F}_2^n$.*
2. *For $p = 3$:*
$$\dim(C_3(Q_n^2)) = \begin{cases} \frac{2}{3}(2^n - 1) & \text{if } n \text{ is even} \\ \frac{2}{3}(2^n + 1) & \text{if } n \text{ is odd} \end{cases}.$$
Furthermore $C_3(Q_n^2) \cap C_3(Q_n^2)^\perp = \{0\}$.
3. *If T denotes the translation group on the vector space $\mathbb{F}_2^n$, and S_n the symmetric group of degree n, then $\mathrm{Aut}(Q_n^2) = T \rtimes S_n$.*

From [13, Theorem 1]:

Result 6. *For $n \geq 2$, let A_n denote an adjacency matrix for Q_n^2, and $\mathcal{D}_n$ the 1-$(2^n, n+1, n+1)$ symmetric design with incidence matrix the rows of $A_n + I_{2^n}$. Then $\mathrm{Aut}(\mathcal{D}_n) = T \rtimes G$, where T is the translation group on $\mathbb{F}_2^n$ and G is a subgroup of $GL_n(\mathbb{F}_2)$ isomorphic to S_{n+1}; $\mathrm{Aut}(\mathcal{D}_n)$ acts primitively for n even, imprimitively for n odd.*

For $n \geq 5$ odd, $C = C_2(\mathcal{D}_n)$ is a $[2^n, 2^{n-1}, n+1]_2$ self-dual binary code, and the minimum words are the incidence vectors of the blocks of the design. Furthermore, $\mathrm{Aut}(C) = \mathrm{Aut}(\mathcal{D}_n)$. Writing $V_n = \mathbb{F}_2^n$,

$$\mathcal{I}_n = \{v \mid v \in V_n, v_n = 0\} \cup \{(1, \ldots, 1)\} \setminus \{(1, \ldots, 1, 0)\}$$

is an information set for C. If $T_n = T\{\iota, (i, n) \mid 1 \leq i \leq n-1\}$ and $T_n^* = T\{\iota, (1, n)\}$, where (i, j) denotes a transposition in S_n acting on V_n and ι is the identity element, then T_n^* is a 2-PD-set for C, of size 2^{n+1}, and for $n \geq 7$, T_n is a 3-PD-set for C of size $n2^n$.

Note that Result 6 effectively concerns the code $C_2(R\Gamma)$, i.e. the reflective graph of $\Gamma = Q_n^2$, and the minimum words of the code are the s_x, for $x \in V$, the rows of $A_n + I_{2^n}$.

An earlier result for 3-*PD*-sets for $C_2(Q_n^2)$ was established in [30, Theorem 1]:

Result 7. *For n even and $n \geq 8$, let*

$$T_n = \{T(w)t_i \mid w \in \mathbb{F}_2^n, 1 \leq i \leq n\},$$

where $T(w)$ is the translation by $w \in \mathbb{F}_2^n$, $t_i = (i, n)$ for $i < n$ is a transposition in the symmetric group S_n, and t_n is the identity map. Then T_n is a 3-PD-set of size $n2^n$ for the self-dual $[2^n, 2^{n-1}, n]_2$ code $C_2(Q_n^2)$ with the information set

$$\mathcal{I} = [\mathbf{0}, \mathbf{1}, \ldots, \mathbf{2^{n-1} - 3}, \mathbf{2^n - 2}, \mathbf{2^n - 1}].$$

Here the notation: for the vectors in Q_n^2 is as follows: $r \in \mathbb{Z}$ and $0 \leq r \leq 2^n - 1$, if $r = \sum_{i=1}^n r_i 2^{i-1}$ is the binary representation of r, let $\mathbf{r} = (r_1, \ldots, r_n)$ be the corresponding vector in $\mathbb{F}_2^n$. The translation $T(w)$ for $w \in \mathbb{F}_2^n$ is defined by $T(w) : v \mapsto v + w$ for each $v \in \mathbb{F}_2^n$.

For Q_n^3, we quote [11, Theorem 1], where the notation used there has $H(n, 3) = Q_n^3$.

Result 8. *Let $C = C_2(Q_n^3)$.*

1. *For $n \geq 1$, C is $[3^n, \frac{1}{2}(3^n - (-1)^n), 2n]_2$ code; for $n \geq 4$, $C^\perp$ is $[3^n, \frac{1}{2}(3^n + (-1)^n), 2n+1]_2$ code; $C \cap C^\perp = \{0\}$ for all n.*
2. *For $n \geq 2$, $\mathrm{Aut}(C) = \mathrm{Aut}(Q_n^3) \cong S_3 \wr S_n$, and acts primitively on vertices.*
3. *For $n \geq 3$, C and $C^\perp$ have 2-PD-sets of size 9 and 3-PD-sets of size $2n3^n$.*

3.2. Q_n^m for $m \geq 4$

These codes were studied in [29, 18]. The most complete results in those papers are for $n = 2$. We are assuming the graphs are not Hamming, so when $m \geq 4$ is even, we will have $R = \mathbb{Z}_m$ to ensure the graph has valency $2n$ and not n.

From [29, Theorem 1], for $m \geq 5$ odd and $n = 2$:

Result 9. *Let $\Gamma = Q_2^m = (V, E)$ 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

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

is an information set for $C^\perp$, and for $s < \frac{m-1}{2}$, the set of translations $S = \{\tau_{<2i,0>} \mid 0 \leq i \leq s\}$ is an s-PD-set of minimal size $s+1$ for the code $C^\perp$ with information set $\mathcal{I}$. The group $T = \{\tau_X \mid X \in R^2\}$ of translations is a PD-set for full error correction, where the translations are defined by $\tau_{<a,b>} :< x, y > \mapsto < x + a, y + b >$.[3]

Thus we see here that, for m odd, s-PD-sets of minimal size $s+1$ can be found up to $t-1$, the error-correcting capability of the code. Computational results for small odd m for full error correction, where $G(t) = t + 2$ (see Result 2), can be be found in [29] in the notes following Proposition 3 of that paper. The lower bound for $G(t)$ was not attained. However H.-J. Kroll [32] has pointed out that anti-blocking sets (see [34]) of the minimal size have been found for $m \geq 5$ odd.

Before stating what we have for the codes $C_2(Q_2^m)$ for $m \geq 4$ even, we have the following concerning words of weight m in $C_2(Q_2^m)^\perp$, for $m \geq 4$ even or odd, as described in [29, Propositions 1,2]:

Result 10. *Let $Q_2^m = (V, E)$ and $R = \{0, 1, \ldots, m-1\}$ where $m \geq 4$, $C = C_2(Q_2^m)$, and $\Lambda = \{< i, i > | \ i \in R\}$. Then the word $v^\Lambda \in C^\perp$.*

Furthermore, there are $2m$ distinct words of weight m obtained from v^Λ by applying the automorphisms $\tau_{(1,0)}$ repeatedly and μ_0 to each of these, viz. *with $u_0 = v^\Lambda$, $u_i = u_0\tau_{<i,0>}$ and $v_i = u_0\tau_{<i,0>}\mu_0 = u_i\mu_0$, for $i \in R$. Let $\mathcal{U} = \{u_i, v_i \mid i \in R\}$, $D = \langle \mathcal{U} \rangle$, the subspace of $C^\perp$ spanned by the set $\mathcal{U}$ over $\mathbb{F}_2$.*

If m is odd then D has dimension $2m-1$, $D = C^\perp$, and $\mathrm{Hull}(D) = \{0\}$. If $m \geq 4$ is even, then D has dimension $2m-2$.

We can add a new lemma here about the words of weight m in $C^\perp$ for all $m \geq 4$ by using [29, Lemma 3.5], where the minimum weight of $C_2(Q_2^m)^\perp$ is shown to be m.

Lemma 1. *For $m \geq 4$, the set of $2m$ words u_a, v_a of Result 10 are all the words of the minimum weight m in $C_2(Q_2^m)^\perp$.*

Proof: We first show that the set $\mathcal{U}$ of the $2m$ words is closed under the automorphisms of the graph from the $\tau_{<a,b>}$, for $a, b \in R$, μ_0, μ_1 and $\sigma \in S_2$, as defined in Subsection 2.1.

This can be easily verified directly: for any $a, b, c \in R$, $u_a^{\tau_{<b,c>}} = u_{a+b-c}$, $v_a^{\tau_{<b,c>}} = v_{a-b-c}$, $u_a^{\mu_1} = v_{-a}$, $v_a^{\mu_1} = u_{-a}$, $u_a^\sigma = u_{-a}$, $v_a^\sigma = v_a$.

Now the argument in the proof of [29, Lemma 3.5] constructs a minimum word in $C^\perp$ containing the point $< 0, 0 >$ in its support that is shown to be of the form with support either that of u_0 or v_0. This completes the proof. ■

For m even, the graph is bipartite as noted in Section 2.1, and we can find, with a similar information set to that in the m odd case, minimal PD-sets of size all the way up to t, i.e. PD-sets of minimal size can be found, thus using the full error-correcting capability of the code. Here the results hold for codes over $\mathbb{F}_p$ for any prime p.

Thus, for the case where $m \geq 4$ is even, from [18, Theorem 1], for any p, taking $R = \mathbb{Z}_m = \{0, 1, \ldots, m-1\}$:

[3] H.-J. Kroll [32] has pointed out in a private communication that the set $\{\tau_{<i,0>} \mid i \in R\}$ will serve as a PD-set of size m for the information set $\mathcal{I}$, i.e. for full error correction.

Result 11. *For $m \geq 4$ even, let $C = C_p(Q_2^m)$, where p is any prime. Then $C^\perp$ contains a subcode D of parameters $[m^2, 2m-2, m]_p$ for which the nested set*

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

of automorphisms is an s-PD-set of minimal size $s+1$ for the code D, for $2 \leq s \leq t = \frac{m}{2} - 1$ with information set $\mathcal{I}$ where

$$\mathcal{I} = \{< 0, i > \mid i \in R\} \cup \{< 1, i > \mid i \in R \setminus \{m-2, m-1\}\}.$$

Here $\tau_{<a,b>} :< x, y > \mapsto < x + a, y + b >$. For $s = t = \frac{m}{2} - 1$, this is a minimal PD-set for full error correction for D.

Further, $D^\perp$ is an $[m^2, m^2 - 2m + 2, 2]_p$ code, and D is LCD if $p \nmid m$.

The codes D in Result 11 are described in [18, Proposition 1]:

Result 12. *For m even and $m \geq 4$, and p any prime, $Q_2^m = (V, E)$, $C = C_p(Q_2^m)$, let*

$$S_1 = \{< 2i, 2i > \mid 0 \leq i \leq \frac{m}{2} - 1\}, S_2 = \{< 2i+1, 2i+1 > \mid 0 \leq i \leq \frac{m}{2} - 1\},$$

and $u_0 = v^{S_1} - v^{S_2}$. Write $u_i = u_0\tau_{<i,0>}$ for $i \in R$, and $v_i = u_0\tau_{<i,0>}\mu_0 = u_i\mu_0$ for $i \in R$. Let $\mathcal{U} = \{u_i, v_i \mid i \in R\}$ and $D = \langle \mathcal{U} \rangle$ over $\mathbb{F}_p$.

Then, $D \subseteq C^\perp$ and is a $[m^2, 2m-2, m]_p$ code, and $D^\perp$ is a $[m^2, m^2 - 2m + 2, 2]_p$ code.

Further, if $p = 2$ then D is self-orthogonal. For p odd, if $p \nmid m$ then $\mathrm{Hull}(D) = \{0\}$, while if $p|m$ then $\dim(\mathrm{Hull}(D)) = 2m - 6$.

For $m \geq 6$, the words in $\mathcal{U}$ and their scalar multiples are the only words of weight m in D.

A word of weight 2 in $D^\perp$ as described in [18, Proposition 1] is $v^{\{<0,0>,<\frac{m}{2},\frac{m}{2}>\}}$ if $p = 2$ or p is odd and $m \equiv 2 \pmod 4$, or $v^{<0,0>} - v^{<\frac{m}{2},\frac{m}{2}>}$ if $m \equiv 0 \pmod 4$.

From the comment at the end of Subsection 2.3, the worst-case time complexity for decoding using the smallest possible s-PD for decoding by permutation decoding is $\mathcal{O}(m^4)$ for both the odd and even case for m, correcting up to just under the full correction ability of the code for m odd, and for full correction when m is even: see Results 9, 11 above.

From [29, Lemma 3]:

Result 13. *Let $C = C_2(Q_2^m)$, where $m \geq 4$. 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 Result 10, has words of weight 2, but if $m = 2m_1$ where $m_1 \geq 3$ is odd, then C has minimum weight 4.*

In fact computation indicates that the minimum weight of $C_2(Q_2^m)$ in Result 13 is 4 for all $m \geq 4$. However the proof used in [29] uses the words of $\mathcal{U}$ to establish the minimum weight, and this does not always work when m is even, as the result indicates.

Note: In [6, Proposition 8.2.17] or [8] it was shown that $C_2(Q_n^8)$ is a $[8^n, 8^{n-1}6, 2n]_2$ code that contains its dual. Furthermore it is conjectured in [6, Conjecture 8.2.18] and [8, Conjecture 3.4] that for $m = 2^k$ where $k \geq 2$, $C_2(Q_n^m)$ is an $[m^n, (m-2)m^{n-1}, 2n]_2$ code that contains its dual, and that if $m = 4$, the code is self-dual.

For the codes $C_p(Q_2^m)$ for $m \geq 4$ even, so the graphs are bipartite, computation with Magma for $p = 2, 3, 5, 7, 11$ and $4 \leq m \leq 18$, m even, indicated that

- for $p = 2$, $C = C_2(Q_2^m)$, C is an $[m^2, m^2 - 2m, 4]_2$ code, $C^\perp$ is an $[m^2, 2m, m]_2$ code, and $C^\perp \neq D$;
- for p an odd prime, $C = C_p(Q_2^m)$, C is an $[m^2, m^2 - 2m + 2, 2]_p$ code, $C^\perp$ is an $[m^2, 2m-2, m]_p$ code, and $C^\perp = D$.

Note: Computation also yielded that the codes $C_p(Q_2^m)$ where m is odd and p is odd were the full space and thus not of interest.

4. Codes from Q_n^m where $m \geq 4$, $n \geq 3$

We now extend our results for $m \geq 4$ to the case where $n = 3$, i.e. to Q_3^m. Let $C = C_2(Q_3^m)$ where $m \geq 4$, and notation as in [29, 18]. Let $R = Z_m$ and recall the words $u_i, v_i \in C_2(Q_m^2)$, for $i \in R$, as defined in Proposition 1 of [29], or see Result 10. We use Result 6 of [29], which is Lemma 4 from [10]:

Result 14. *Let $\Gamma^{\Box} = \Gamma_1 \Box \Gamma_2$, 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 $S_1 = \mathrm{Supp}(w_1) = \{a_1, \ldots, a_{d_1}\}$, $S_2 = \mathrm{Supp}(w_2) = \{b_1, \ldots, b_{d_2}\}$, where $a_i \in V_1$, $b_j \in V_2$. Then the word with weight $d_1 d_2$ and support*

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

is in $C_2(\Gamma^{\Box})^{\perp}$.

This gives Lemma 3.4 from [29]:

Result 15. *Let $\Gamma = Q_n^m = (Q_1^m)^{\Box, n}$, 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 $\frac{m^{n-1}}{2^{n-2}}$.*

4.1. $m \geq 5$ odd

Considering m odd in this subsection, words of weight m^2 in $C_2(Q_3^m)^{\perp}$ can be constructed from the u_i, v_j and the word $\boldsymbol{\jmath}_m \in C_2(Q_m^1)^{\perp}$. For any of the u_i, v_j three words of weight m^2 in $C_2(Q_3^m)^{\perp}$ can be constructed, by choosing the position in which one inserts the element from the support of $\boldsymbol{\jmath}_m$ from R, i.e. at the beginning, in the middle, or at the end, of the triple. As in the case of $n = 2$, the supports of these words will meet the rows $r_{<a,b,c>}$ of the adjacency matrix in 0 or 2 points.

Thus, for example, for u_0 with support $\{< 0, 0 >, < 1, 1 >, \ldots, < m-1, m-1 >\}$, we get the three weight m^2 words which we will label u_0^j for $j = 1, 2, 3$, respectively, where

$$\mathrm{Supp}(u_0^1) = \{< 0, 0, 0 >, < 0, 1, 1 >, \ldots, < 0, m-1, m-1 >, < 1, 0, 0 >, < 1, 1, 1 >,$$
$$\ldots, < 1, m-1, m-1 >, \ldots, < m-1, 0, 0 >, < m-1, 1, 1 >, \ldots, < m-1, m-1, m-1 >\},$$
$$\mathrm{Supp}(u_0^2) = \{< 0, 0, 0 >, < 1, 0, 1 >, \ldots, < m-1, 0, m-1 >, < 0, 1, 0 >, < 1, 1, 1 >,$$
$$\ldots, < m-1, 1, m-1 >, \ldots, < 0, m-1, 0 >, < 1, m-1, 1 >, \ldots < m-1, m-1, m-1 >\},$$
$$\mathrm{Supp}(u_0^3) = \{< 0, 0, 0 >, < 1, 1, 0 >, \ldots, < m-1, m-1, 0 >, < 0, 0, 1 >, < 1, 1, 1 >,$$
$$\ldots, < m-1, m-1, 1 >, \ldots, < 0, 0, m-1 >, < 1, 1, m-1 >, \ldots, < m-1, m-1, m-1 >\}.$$

Similarly we label the $6m$ words we get from the u_i and v_i for $i \in R$ with $\boldsymbol{\jmath}_m$ as u_i^j and v_i^j in this way, for $j = 1, 2, 3$.. Recall that in Proposition 1 of [29] our labelling of the u_i, v_i was according to $u_i = u_0^{\tau_{<i,0>}}, v_i = u_i^{\mu_0}$, for $i \in R$, where $\tau_{<a,b>}$ is the translation mapping $< x, y >$ to $< x + a, y + b >$, and μ_0 maps $< x, y >$ to $< -x, y >$. Thus

$$\mathrm{Supp}(u_i) = \{< i + j, j > |\ j \in R\} \text{ and } \mathrm{Supp}(v_i) = \{< -i - j, j > |\ j \in R\}.$$

Further, it is shown there that the vertex $< a, b >$ is in the support of exactly two of the u_i, v_i, viz. u_{a-b} and v_{-a-b}. Also

$$\mathrm{Supp}(u_a) \cap \mathrm{Supp}(v_b) = \{< \frac{a-b}{2}, \frac{-(a+b)}{2} >\}.$$

Thus we can see that the vertex $< a, b, c >$ is in the support of the six words

$$u_{b-c}^1, v_{-b-c}^1, u_{a-c}^2, v_{-a-c}^2, u_{a-b}^3, v_{-a-b}^3, \tag{5}$$

and, for all $i \in R$,

$$\mathrm{Supp}(u_i^1) = \{< k, i + j, j > |\ j, k \in R\} \quad ; \quad \mathrm{Supp}(v_i^1) = \{< k, -i - j, j > |\ j, k \in R\} \tag{6}$$
$$\mathrm{Supp}(u_i^2) = \{< i + j, k, j > |\ j, k \in R\} \quad ; \quad \mathrm{Supp}(v_i^2) = \{< -i - j, k, j > |\ j, k \in R\} \tag{7}$$
$$\mathrm{Supp}(u_i^3) = \{< i + j, j, k > |\ j, k \in R\} \quad ; \quad \mathrm{Supp}(v_i^3) = \{< -i - j, j, k > |\ j, k \in R\}. \tag{8}$$

It is clear that:

$$\begin{aligned} |\mathrm{Supp}(u_i^j) \cap \mathrm{Supp}(u_i^k)| &= m \text{ for } j \neq k, m^2 \text{ for } j = k; \\ |\mathrm{Supp}(u_i^j) \cap \mathrm{Supp}(u_k^j)| &= 0 \text{ for } i \neq k; \\ |\mathrm{Supp}(u_i^j) \cap \mathrm{Supp}(v_k^{\ell})| &= m \ \forall i, j, k, \ell. \end{aligned}$$

and that the same holds for the v_i^j.

For example, $\mathrm{Supp}(u_i^1)\cap\mathrm{Supp}(u_i^2) = \{< i+k, i+k, k >|\ k \in R\}$, $\mathrm{Supp}(u_i^1)\cap\mathrm{Supp}(v_j^3) = \{< -j-(i+k), i+k, k >|\ k \in R\}$, and $\mathrm{Supp}(v_i^2) \cap \mathrm{Supp}(v_j^3) = \{< -j-k, k, -i+j+k >|\ k \in R\}$.

In particular, u_i^j is disjoint from precisely the $m-1$ u_k^j for all $k \in R, k \neq i$, and likewise for v_i^j. Otherwise the words meet in m or m^2 points of Q^3_m, i.e. an odd number of points.

If we let $\mathcal{B} = \{\mathrm{Supp}(u_i^j), \mathrm{Supp}(v_i^j)\ |\ j = 1,2,3, i \in R\}$ and call the vertices of the graph Q_3^m points $\mathcal{P}$, then $(\mathcal{P}, \mathcal{B})$ is a 1-design, 1-$(m^3, m^2, 6)$ with distinct blocks meeting in 0 or m points, as discussed above.

As in the case of $n = 2$, we write

$$\mathcal{U} = \{u_i^j, v_i^j\ |\ i \in R, j = 1,2,3\}. \tag{9}$$

Furthermore, the blocks of $\mathcal{B}$ are preserved under the translations, the μ_i, and the elements of S_3, as can be shown similarly to the proof in Lemma 1. For example, $(u_i^1)^{\tau_{<a,b,c>}} = u^1_{i+b-c}$. There are $6m$ of these words.

4.2. $m \geq 4$ even

When m is even, the corresponding words from the u_i, v_i in the dual space for $n = 3$ have weight $\frac{m^2}{2}$, as described in Result 15 (2), using the two vectors $\boldsymbol{\jmath}_e$ and $\boldsymbol{\jmath}_o$ of weight $\frac{m}{2}$ in $C_2^\perp(Q_1^m)$, where $\mathrm{Supp}(\boldsymbol{\jmath}_e) = \{2k \mid 0 \leq k < \frac{m}{2}\}$ and $\mathrm{Supp}(\boldsymbol{\jmath}_o) = \{2k+1 \mid 0 \leq k < \frac{m}{2}\}$. Let $\mathcal{E} = \{2k \mid 0 \leq k < \frac{m}{2}\}$ and $\mathcal{O} = \{2k+1 \mid 0 \leq k < \frac{m}{2}\}$. We denote these by ${}_eu_i^j$, ${}_ou_i^j$, ${}_ev_i^j$, ${}_ov_i^j$, for $i \in R$ and $j = 1,2,3$, as in the odd m case, where,

$$\begin{array}{lll}
\mathrm{Supp}({}_eu_i^1) = \{< k, i+j, j >|\ k \in \mathcal{E}, j \in R\} & ; & \mathrm{Supp}({}_ev_i^1) = \{< k, -i-j, j >|\ k \in \mathcal{E}, j \in R\} \\
\mathrm{Supp}({}_eu_i^2) = \{< i+j, k, j >|\ k \in \mathcal{E}, j \in R\} & ; & \mathrm{Supp}({}_ev_i^2) = \{< -i-j, k, j >|\ k \in \mathcal{E}, j \in R\} \\
\mathrm{Supp}({}_eu_i^3) = \{< i+j, j, k >|\ k \in \mathcal{E}, j \in R\} & ; & \mathrm{Supp}({}_ev_i^3) = \{< -i-j, j, k >|\ k \in \mathcal{E}, j \in R\} \\
\mathrm{Supp}({}_ou_i^1) = \{< k, i+j, j >|\ k \in \mathcal{O}, j \in R\} & ; & \mathrm{Supp}({}_ov_i^1) = \{< k, -i-j, j >|\ k \in \mathcal{O}, j \in R\} \\
\mathrm{Supp}({}_ou_i^2) = \{< i+j, k, j >|\ k \in \mathcal{O}, j \in R\} & ; & \mathrm{Supp}({}_ov_i^2) = \{< -i-j, k, j >|\ k \in \mathcal{O}, j \in R\} \\
\mathrm{Supp}({}_ou_i^3) = \{< i+j, j, k >|\ k \in \mathcal{O}, j \in R\} & ; & \mathrm{Supp}({}_ov_i^3) = \{< -i-j, j, k >|\ k \in \mathcal{O}, j \in R\}.
\end{array}$$

As in the m odd case, these words will meet any row $r_{<a,b,c>}$ of an adjacency matrix for the graph in 0 or 2 points.

In Proposition 1 of [18] it is shown that the binary code D spanned by $\mathcal{U} = \{u_i, v_i \mid i \in R\}$ is self-orthogonal.

As in the case of m odd, any vertex $< a, b, c >$ is in the support of six of the words ${}_eu_i^j, {}_ou_i^j, {}_ev_i^j, {}_ov_i^j$ for $j = 1,2,3$, i.e. in

$${}_eu^1_{b-c} \text{ and } {}_ev^1_{-b-c} \text{ for } a \text{ even or } {}_ou^1_{b-c} \text{ and } {}_ov^1_{-b-c} \text{ for } a \text{ odd;}$$
$${}_eu^2_{a-c} \text{ and } {}_ev^2_{-a-c} \text{ for } b \text{ even or } {}_ou^2_{a-c} \text{ and } {}_ov^2_{-a-c} \text{ for } b \text{ odd;}$$
$${}_eu^3_{a-b} \text{ and } {}_ev^3_{-a-b} \text{ for } c \text{ even or } {}_ou^3_{a-b} \text{ and } {}_ov^3_{-a-b} \text{ for } c \text{ odd.}$$

The words ${}_eu_i^j$, ${}_ou_i^j$, ${}_ev_i^j$, and ${}_ov_i^j$ meet in $0, \frac{m}{2}, m$ or $\frac{m^2}{2}$ points. For example , $|\mathrm{Supp}({}_eu_i^j) \cap \mathrm{Supp}({}_ov_k^j)| = 0$, for all $i, k \in R, j = 1,2,3$; $|\mathrm{Supp}({}_eu_i^1 \cap \mathrm{Supp}({}_eu_i^2)| = \frac{m}{2}$, all $i \in R$; $|\mathrm{Supp}({}_eu_i^1 \cap \mathrm{Supp}({}_ev_i^1)| = m$ for all $i \in R$.

As before, these words are preserved under the translations, the μ_i, and the elements of S_3. There are $12m$ of them. We write

$$\mathcal{U} = \{{}_eu_i^j, {}_ou_i^j, {}_ev_i^j, {}_ov_i^j\ |\ i \in R, j = 1,2,3\}. \tag{10}$$

Furthermore, as in the m odd case, we let $\mathcal{B}_e = \{\mathrm{Supp}(x)\ |\ x \in \mathcal{U}\}$ and form the 1-$(m^3, \frac{m^2}{2}, 6)$ design from the vertices of Γ as points and blocks $\mathcal{B}_e$. Thus blocks meet in $0, \frac{m}{2}, m$ or $\frac{m^2}{2}$ points.

5. Properties of codes from Q_3^m

5.1. $m \geq 5$, m odd

With notation as defined above:

Proposition 1. *Let $C = C_2(Q_3^m)$, where m is odd, and let D be the subcode of $C^\perp$ generated by the vectors u_i^j, v_k^ℓ for all $i, k \in R$, all $j, \ell \in \{1,2,3\}$. Then* $\mathrm{Hull}(D) = \{0\}$. *Furthermore,* $\dim(D) \leq 6m-5$.

Proof: We have $D = \langle\mathcal{U}\rangle$, where $\mathcal{U}$ is as in Equation (9).

We know that $D \subseteq C^\perp$. Suppose $w \in D \cap D^\perp$. Then

$$w = \sum_{i\in R, j=1,2,3} \alpha_i^j u_i^j + \sum_{i\in R, j=1,2,3} \beta_i^j v_i^j,$$

where the coefficients α_i^j, β_i^j are in $\mathbb{F}_2$. Since $w \in D^\perp$, we have $(w, u_i^j) = (w, v_k^\ell) = 0 \in F_2$ for all i, j, k, ℓ. So

$$(w, u_a^b) = \sum_{i\in R, j=1,2,3} \alpha_i^j (u_i^j, u_a^b) + \sum_{i\in R, j=1,2,3} \beta_i^j (v_i^j, u_a^b) = 0,$$

$$= m^2 \alpha_a^b + m(\sum_{i\in R, j\neq b} \alpha_i^j + \sum_{i\in R, j=1,2,3} \beta_i^j) = 0,$$

$$= \alpha_a^b + \sum_{i\in R, j\neq b} \alpha_i^j + \sum_{i\in R, j=1,2,3} \beta_i^j = 0.$$

From this we can see that α_a^b is a constant over $a \in R$, so we can write $\alpha_a^b = \alpha^b$, and the same argument for v_i^j gives $\beta_a^b = \beta^b$. Thus

$$w = \sum_{j=1,2,3} \alpha^j \sum_{i\in R} u_i^j + \sum_{j=1,2,3} \beta^j \sum_{i\in R} v_i^j = \sum_{j=1,2,3} (\alpha^j + \beta^j)\boldsymbol{\jmath}$$

since it is clear that for each j, $\sum_{i\in R} u_i^j = \sum_{i\in R} v_i^j = \boldsymbol{\jmath}$.

Now clearly $\boldsymbol{\jmath} \notin D^\perp$, so $w = 0$, proving that $\mathrm{Hull}(D) = \{0\}$.

For the bound on the dimension of D, in [28, Proposition 1] it is shown that the code spanned by the $2m$ words u_i, v_j in $C_2(Q_2^m)^\perp$ has dimension $2m-1$ for m odd. We use this result to look at the code D spanned by the vectors u_i^j, v_k^ℓ for all $i, k \in R$, all $j, \ell \in \{1, 2, 3\}$, for m is odd.

Let D_j, for $j = 1, 2, 3$ be the binary code spanned by vectors u_i^j, v_i^j, $i \in R$, respectively. Then by the above result $\dim(D_j) = 2m - 1$. Thus we can omit, say, v_{m-1}^j for $j = 1, 2, 3$. Now notice that $\sum_{i\in R} u_i^j = \boldsymbol{\jmath}$ for each $j = 1, 2, 3$. Thus we may omit two more of the spanning vectors, say, u_{m-1}^2, u_{m-1}^3 from the spanning set and still get the span to be D. This gives $6m - 5$ vectors spanning D so its dimension is at most $6m - 5$. ■

Note: $6m - 5$ is precisely what we get for the dimension of D computationally, for $m \leq 15$, odd.

Proposition 2. *Let $C = C_2(Q_3^m)$ where $m \geq 5$ and odd. Then the minimum weight of C is 6.*

Proof: C is generated by words of weight 6, so it is an even-weight code. Let $w \in C$ and suppose $\mathrm{wt}(w) = 2$. Without loss of generality we take $< 0, 0, 0 > \in \mathrm{Supp}(w)$ (since the automorphism group of the graph is transitive on points/vectors) and let $\mathrm{Supp}(w) = \{< 0, 0, 0 >, < a, b, c >\}$. Since w must meet all the u_i^j and v_i^j evenly, $< a, b, c >$ is the the support of all the u_0^j and v_0^j, $j = 1, 2, 3$. Thus $< a, b, c > \in \mathrm{Supp}(u_0^1)$ so that $b = c$, and $< a, b, c > \in \mathrm{Supp}(v_0^1)$ so that $b = -c$. So $b = c = 0$, since m is odd. But $< a, b, c > \in \mathrm{Supp}(u_0^2)$ implies that $a = c$, and thus this is impossible, and C cannot contain vectors of weight 2.

Suppose $\mathrm{Supp}(w) = \{< 0, 0, 0 >, < a_1, a_2, a_3 >, < b_1, b_2, b_3 >, < c_1, c_2, c_3 >\}$. Since w meets u_0^1 again, we can assume that $a_2 = a_3 = a$. Then w meets u_0^2 again, so either (i) $a_1 = a_3 = a$ or (ii) $b_1 = b_3$.

Suppose (i), then $\mathrm{Supp}(w)$ meets $\mathrm{Supp}(v_0^j)$, for $j = 1, 2, 3$ again, and this cannot be in $< a, a, a >$. Suppose $\mathrm{Supp}(v_0^1)$ meets in $< b_1, b_2, b_3 >$, so $b_2 = -b_3 = b$. If (iii) $\mathrm{Supp}(v_0^2)$ contains $< b_1, b, -b >$ then $< b_1, b, -b > = < b, b, -b >$ is in $\mathrm{Supp}(w)$, or (iv) $\mathrm{Supp}(v_0^2)$ contains $< c_1, c_2, c_3 >$ and $c_1 = -c_3 = c$.

Suppose (iii), so $\mathrm{Supp}(w) = \{< 0, 0, 0 >, < a, a, a >, < b, b, -b >, < c_1, c_2, c_3 >\}$. Since $\mathrm{Supp}(v_0^3)$ meets $\mathrm{Supp}(w)$ again, we must have $c_1 = -c_2 = c$, so $< c, -c, d > \in \mathrm{Supp}(w)$, where we write $c_3 = d$. Now $< c, -c, d >$ is in the supports of $u_{-c-d}^1, v_{c-d}^1, u_{c-d}^2, v_{-c-d}^2, u_{2c}^3, v_0^3$, and each of these must meet $\mathrm{Supp}(w)$ again. Now $\mathrm{Supp}(u_{2c}^3) = \{< 2c + j, j, k > | \ j, k, \in R\}$, so if $< a, a, a > = < 2c + j, j, k >$ then $a = j$ and $2c + a = a$, which is impossible, and if $< b, b, -b > = < 2c + j, j, k >$ then $b = j$ and $2c + b = b$, again impossible. Thus (iii) is not possible, and so we go back to (iv).

So if (iv), then $\mathrm{Supp}(w) = \{< 0, 0, 0 >, < a, a, a >, < d, b, -b >, < c, e, -c >\}$ writing $b_1 = d$, $c_2 = e$. Since $\mathrm{Supp}(w)$ meet $\mathrm{Supp}(v_0^3)$ again either (v) $d = -b$ or (vi) $e = -c$. Suppose (v) $d = -b$, so that $\mathrm{Supp}(w) = < a, a, a >, < -b, b, -b >, < c, e, -c >\}$. All the blocks through $< c, e, -c >$ must meet $\mathrm{Supp}(w)$ again, so in particular, u_{2c}^2. If $< a, a, a > \in \mathrm{Supp}(u_{2c}^2)$ then $a = 2c + j, k = a, j = a$, so $2c = 0$ which is impossible. If $< -b, b, -b > \in \mathrm{Supp}(u_{2c}^2)$ then $-b = 2c + j, k = b, j = -b$, again impossible. So (v) cannot hold.

Suppose (vi), i.e. $e = -c$ and $\mathrm{Supp}(w) = \{< 0, 0, 0 >, < a, a, a >, < d, b, -b >, < c, -c, -c >\}$. The block from u_{2b}^1 must meet $\mathrm{Supp}(w)$ again. If $< a, a, a > \in \mathrm{Supp}(u_{2b}^1)$ then $a = 2b + j, j = a$, which is not possible, and if $< c, -c, -c > \in \mathrm{Supp}(u_{2b}^1)$ then $-c = 2b + j, j = -c$, which is again impossible.

Thus all deductions from (i) are contradicted, so we must return to (ii), i.e. $\mathrm{Supp}(w) = \{< 0, 0, 0 >, < d, a, a >, < b, e, b >, < c_1, c_2, c_3 >\}$, where $d \neq a, e \neq b$, since such cases are covered in (i). Since $\mathrm{Supp}(w)$ meets $\mathrm{Supp}(u_0^3)$ again, we must have $c_1 = c_2 = c$, and write $c_3 = f$, and $< c_1, c_2, c_3 > = < c, c, f >$. Now $\mathrm{Supp}(v_0^1)$ meets again, so (vii) $e = -b$ or (viii) $f = -c$, but not both since otherwise $\mathrm{Supp}(v_0^1)$ meets in three points. Suppose (vii) $e = -b$. Then $\mathrm{Supp}(v_0^2)$ meets again so (ix) $d = -a$ or (x) $f = -c$ but not both. If (ix) then $\mathrm{Supp}(w) = \{< 0, 0, 0 >, <$

$-a, a, a >, < b, -b, b >, < c, c, f >\}$ which meets $\mathrm{Supp}(v_0^3)$ in three points, which is not possible. So (x) $f = -c$ and $\mathrm{Supp}(w) = \{< 0, 0, 0 >, < d, a, a >, < b, -b, b >, < c, c, -c >\}$. But now $\mathrm{Supp}(v_0^1)$ meets three times, so this case is not possible. Thus (vii) not possible.

Suppose (viii), i.e. $f = -c$, and $\mathrm{Supp}(w) = \{< 0, 0, 0 >, < d, a, a >, < b, e, b >, < c, c, -c >\}$. Since $\mathrm{Supp}(v_0^3)$ must meet again then if $d = -a$, $\mathrm{Supp}(v_0^2)$ will meet three times, and if $e = -b$ then $\mathrm{Supp}(v_0^1)$ will meet three times.

This covers all the possibilities, so C has no words of weight 4, and thus has minimum weight 6, this being the valency of the graph. ■

5.2. $m \geq 4$ even

We now use the words $\mathcal{U}$ defined in Subsection 4.2, Equation (10) to obtain some properties of the codes $C_2(Q_3^m)$ for $m \geq 4$, even.

Proposition 3. *Let $C = C_2(Q_3^m)$ for $m \geq 4$, even. If $\frac{m}{2}$ is odd, i.e. $4 \nmid m$, then the minimum weight of C is 6.*

If $\frac{m}{2}$ is even, then the binary code $D = \langle \mathcal{U} \rangle$ is self-orthogonal.

Proof: As in the m odd case, C is generated by words of weight 6, so it is an even-weight code. Let $w \in C$ and suppose $\mathrm{wt}(w) = 2$. Without loss of generality we take $< 0, 0, 0 > \in \mathrm{Supp}(w)$ and let $\mathrm{Supp}(w) = \{< 0, 0, 0 >, < a, b, c >\}$. Since $D \subseteq C^\perp$, so $C \subseteq D^\perp$, and thus w must meet all words in $\mathcal{U}$ that contain $< 0, 0, 0 >$ again, i.e. all of ${}_eu_0^j, {}_ev_0^j$ for $j = 1, 2, 3$. Thus $a = b = c$ is even, and $a = -a$ so $a = \frac{m}{2}$ is even. Thus if we suppose $\frac{m}{2}$ is odd then C has no words of weight 2. (If $\frac{m}{2}$ is even then the word with support $\{< 0, 0, 0 >, < \frac{m}{2}, \frac{m}{2}, \frac{m}{2} >\}$ is in $D^\perp$, but we cannot say whether or not it is in C.)

We now take $\frac{m}{2}$ odd and show that C cannot have a word of weight 4. First note that since $\frac{m}{2} = -\frac{m}{2}$, the word w with support

$$\{< 0, 0, 0 >, < 0, \frac{m}{2}, \frac{m}{2} >, < \frac{m}{2}, 0, \frac{m}{2} >, < \frac{m}{2}, \frac{m}{2}, 0 >\}$$

is in $D^\perp$ for all even m, but not in C if $\frac{m}{2}$ is odd, since the word with support $\{< x, y, z > |\ x, y, z \in \mathcal{E}\}$ is in $C^\perp$ but does not meet w evenly, so w is not in C.

We now show that a putative word w of weight 4 in $D^\perp$ cannot be in C. We use the fact that every block that meets w must meet w evenly, so in two or four points. Let $w \in D^\perp$ have support

$$\{Z =< 0, 0, 0 >, A =< a_1, a_2, a_3 >, B =< b_1, b_2, b_3 >, K =< c_1, c_2, c_3 >\}.$$

Suppose ${}_eu_0^1$ meets w again at A, so a_1 is even, and $a_2 = a_3 = a$, $A =< a_1, a, a >$. Suppose (i) that ${}_eu_0^2$ meets w in A, then $a_1 = a$, and also ${}_eu_0^3$ meets at $A =< a, a, a >$, a even. If ${}_ev_0^1$ meets w at A then $a = -a$, and so $a = \frac{m}{2}$ which is odd, so this is not possible. Thus suppose ${}_ev_0^1$ meets at B, so $b_2 = -b_3 = b$, and b_1 is even, $B =< b_1, b, -b >$.

Next ${}_ev_0^2$ meets again at B or K. Suppose (ia) it meets at B. Then $b_1 = b$ and $B =< b, b, -b >$, b even. Thus ${}_eu_0^3$ meets w in Z, A, B and thus also in K, so $c_1 = c_2 = c$, $K =< c, c, c_3 >$. Then ${}_ev_0^3$ must meet w again in K, so $c = -c = \frac{m}{2}$ or 0, $K =< \frac{m}{2}, \frac{m}{2}, c_3 >$ or $K =< 0, 0, c_3 >$, c_3 even. But $K =< \frac{m}{2}, \frac{m}{2}, c_3 >$ cannot be possible as ${}_ou_{\frac{m}{2}-c_3}^1$ contains K but cannot meet w again.

Thus suppose our set of four points in $\mathrm{Supp}(w)$ is

$$\{Z =< 0, 0, 0 >, A =< a, a, a >, B =< b, b, -b >, K =< 0, 0, c >\}$$

where a, b, c are all even. We now make sure that the other blocks through A, B, K meet this set again. Checking first the other four blocks containing K, we find that they meet at A and B if $c = 2a$ and $b = -a$. Thus B is $< -a, -a, a >$. Now checking the other blocks through A and B, we see that ${}_ev_{2a}^3$ through B does not contain either Z, A or K.

Thus we go back and assume our assumption (ia) was wrong, and go back to (i), and thus we have ${}_ev_0^2$ meeting $\mathrm{Supp}(w)$ at K, so $K =< c, c_2, -c >$, where c_2 is even, and the set is

$$\{Z =< 0, 0, 0 >, A =< a, a, a >, B =< b_1, b, -b >, K =< c, c_2, -c >\},$$

where a, b_1, c_2 are even. Then ${}_ev_0^3$ meets again, and not at A, so suppose at B. Then $b_1 = -b$ and $B =< -b, b, -b >$. Thus ${}_eu_0^2$ must meet also at K, so $c = -c$ and only $c = 0$ is possible as we pointed out before. Then checking the blocks through these points so that w is met evenly, we find that $c_2 = 2a = 2b$ as in a previous case, and then that ${}_ev_{-2a}^2$ meets only at A. Thus we must have ${}_ev_0^3$ meeting at K, so $K =< c, -c, -c >$. Thus B must also meet in ${}_eu_0^1$, so $b = -b$, and as before $B =< b_1, 0, 0 >$. This is similar to one of the cases above, and cannot occur.

Thus we have eliminated our assumption (i) and so $A =< a_1, a, a >$ where $a_1 \neq a$, a_1 even, and suppose that ${}_e u_0^2$ meets w in B, so $B =< b, b_1, b >$, and b_1 is even, $b_1 \neq b$. ${}_e u_0^2$ cannot also meet in K, so $c_1 \neq c_3$. ${}_e u_0^3$ must meet at K, so $c_1 = c_2$ and the set becomes

$$\{Z =< 0, 0, 0 >, A =< a_1, a, a >, B =< b, b_1, b >, K =< c, c, c_1 >\}, \tag{11}$$

where $a_1 \neq a$, $b_1 \neq b$, $c_1 \neq c$, and a_1, b_1, c_1 are even. Recall that if $w \in C$ then at least one of A, B, K will have all its entries in $\mathcal{E}$.

The words ${}_e v_0^j$ for $j = 1, 2, 3$ need to meet w again. Suppose (ii) that ${}_e v_0^1$ meets in A then $a = -a = \frac{m}{2}, 0$. If (iia) ${}_e v_0^1$ also meets in B then it meets also in K, so $B =< b, -b, b >$ and $K =< c, c, -c >$, which implies that $A =< a, 0, 0 >$ since w is in C. Then ${}_e v_0^2$ meets in K, and ${}_e v_0^3$ meets in B. Checking the blocks through the points A, B, K shows that we must have $a = 2b = 2c$, and it then follows that the block from ${}_e u_a^1$ meets w only at K. Thus (iia) does not follow, so ${}_e v_0^1$ meets only at $Z, A =< a_1, a, a >$ where $a = \frac{m}{2}$ or 0. Suppose ${}_e v_0^2$ meets at B, so $b = -b$, and $b = 0$ or $\frac{m}{2}$. Then ${}_e v_0^3$ meets at K, so $c = -c$, and one or all of a, b, c must be 0. If (iib) $a = 0$ then we find that the blocks ${}_e u_{a_1}^2$ and ${}_e v_{-a_1}^2$ through A must both pass through K, and this gives the contradiction that $a_1 = c_1 = -c_1$, and $c = 0$, so $K = Z$. Now the 3-cycle acting on the graph will place any of B and K in $A's$ position and lead to a contradiction. Thus (ii) cannot hold at all.

We revert to Equation (11) above, and observe that the argument in (ii) applies also to eliminate ${}_e v_0^2$ meeting in B, and ${}_e v_0^3$ meeting in K, by cycling the positions, as before. Thus we try (iii), ${}_e v_0^2$ meets at A (and not at B, so thus not at K). It would follow that ${}_e v_0^3$ meets at B and ${}_e v_0^1$ meets at K, and our set becomes

$$\{< 0, 0, 0 >, < -a, a, a >, < b, -b, b >, < c, c, -c >\},$$

with a, b, c all even. However this is impossible as then ${}_e v_0^3$ meets w at Z, A, B and thus also at K, from which we must have $c = -c$ which is not possible since $c \neq 0, \frac{m}{2}$.

This exhausts all possibilities for weight-4 words in C, so the minimum weight when $\frac{m}{2}$ is odd is 6.

Finally, if $\frac{m}{2}$ is even then the words in $\mathcal{U}$ meet evenly in $0, \frac{m}{2}, m$ or $\frac{m^2}{2}$ points, so $D \subseteq D^\perp$. ■

6. Computational results

We start from the words u_i and v_i from Result 10, from [29, 18], for $n = 2$, and $\jmath_m$ or $\jmath_{\frac{m}{2}}$, for $n = 1$, m odd or even, respectively. This gives the words obtained in Result 15. Let D_n^m be the code spanned by these vectors. Then $D_n^m \subseteq C_2(Q_n^m)^\perp$. The binary codes $D = D_n^m$ for $n \geq 3$ were examined using Magma [3, 4] to obtain their parameters, and determine their hulls.

Some computations with Magma for $n = 3$ and $m \geq 5$ odd are given in the table, where the third column gives the weight of the words for generating D, as constructed, the fourth column gives the number of such words, d denotes dimension, $H(X)$ denotes the hull of the code X, $D = D_3^m$, $C = C_2(Q_3^m)$, and MW is minimum weight. Note that for $m \geq 9$ the codes are too big to easily get the minimum weight with Magma.

m	m^3	wt	No.	$d(D)$	$d(H(D))$	$d(C)$	$d(C^\perp)$	$d(H(C))$	$MW(D)$
5	125	25	30	25	0	100	25	0	25
7	343	49	42	37	0	306	37	0	49
9	729	81	54	49	0	632	97	0	?
11	1331	121	66	61	0	1270	61	0	?
13	2197	169	78	73	0	2124	73	0	?
15	3375	225	90	85	0	3146	229	0	?
21	9261	441	126	121	0	8996	265	0	?
25	15625	625	150	145	0	15480	145	0	?

Table 1: Binary codes for $n = 3$, $m \geq 5$ odd

We might conjecture from these computations that for $n = 3$, $m \geq 5$ odd,

- $\dim(D_3^m) = 6m - 5$;
- if m is not divisible by 3 then $D_3^m = C^\perp$;
- the minimum weight of D_3^m is m^2, and the words of weight m^2 are precisely the $6m$ words constructed in Result 15.

- if $3 \not| m$ then C has words of weight 8, whereas if $3|m$ there are no words of weight 8 in C, but $D_3^{m\perp} \supset C$ has words of weight 8.

For $n = 3$ and $m \geq 6$ even, since $m = 4$ has other distinct properties.

m	m^3	wt	No.	$d(D)$	$d(H(D))$	$d(C)$	$d(C^\perp)$	$d(H(C))$	$MW(D)$	MW($D^\perp$)	MW(C)
6	216	18	72	54	50	160	56	48	18	4	6
8	512	32	96	60	60	384	128	128	32	2	6
10	1000	50	120	102	98	896	104	96	?	4	6
12	1728	72	144	114	114	1504	224	224	?	2	6
14	2744	98	168	150	146	2592	152	144	?	4	6
16	4096	128	192	156	156	3584	512	512	?	2	?

Table 2: Binary codes for $n = 3$, $m \geq 6$ even

Similarly for $n = 3$, $m \geq 4$ even, we may conjecture the following, since it is true for $m = 4$, by computation:

- if $4 \nmid m$ then $\dim(D_3^m) = 12m - 18$, $\dim(\text{Hull}(D_3^m)) = 12m - 22$, $\dim(C^\perp) = 12m - 16$, $\dim(\text{Hull}(C)) = 12m - 24$;
- if $4 \mid m$ then $C^\perp \subseteq C$.

Note: For $n = 4$ the binary codes are rather large, but for $m = 5, 7$ Magma found that $\text{Hull}(C) = \{0\}$, where $C = C_2(Q_4^m)$, so this might be something that can be pursued in the general case for m odd.

Conjecture 1. *For $m \geq 5$ odd, $n \geq 2$, the codes $C_2(Q_n^m)$ are LCD.*

This conjecture is proved for the case $m = 3$ when we have Hamming graphs: see Result 8. It is also true for $n = 2$ from Result 9.

Note: The codes $C_p(Q_3^m)$ for p prime, $p \neq 2$, $m \geq 4$ were examined computationally for some $p \geq 3$ and m and no pattern emerged, so that no general properties seemed likely. Some of the codes might be of interest, for example, $m = 5$, $p = 3$.

Acknowledgment

This work is based on the research supported by the National Research Foundation of South Africa (Grant Numbers 95725 and 106071).

References

[1] E. F. Assmus, Jr. and J. D. Key, *Designs and their codes*, vol. 103 of Cambridge Tracts in Mathematics, 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. Comput., 44 (1995), pp. 1021–1030.

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

[4] J. Cannon, A. Steel, and G. White, *Linear codes over finite fields, Handbook of Magma Functions (j. cannon and w. bosma, eds.), computational algebra group, department of mathematics, university of sydney, 2006, v2. 13.*

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

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

[7] W. Fish, *Binary codes and partial permutation decoding sets from the Johnson graphs*, Graphs Combin., 31 (2015), pp. 1381–1396.

[8] ——, *Binary codes and permutation decoding sets from the graph products of cycles*, Appl. Algebra Engrg. Comm. Comput., 28 (2017), pp. 369–386.

[9] W. Fish, R. Fray, and E. Mwambene, *Binary codes and partial permutation decoding sets from the odd graphs*, Cent. Eur. J. Math., 12 (2014), pp. 1362–1371.

[10] W. Fish, J. Key, and E. Mwambene, *Special lcd codes from products of graphs*, Applicable Algebra in Engineering, Communication and Computing, (2021), pp. 1–27.

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

[12] ——, *Graphs, designs and codes related to the n-cube*, Discrete Math., 309 (2009), pp. 3255–3269.

[13] ——, *Binary codes from designs from the reflexive n-cube*, Util. Math., 85 (2011), pp. 235–246.

[14] W. Fish, J. D. Key, E. Mwambene, and B. G. Rodrigues, *Hamming graphs and special LCD codes*, J. Appl. Math. Comput., 61 (2019), pp. 461–479.

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

[16] W. H. Haemers, R. Peeters, and J. M. van Rijckevorsel, *Binary codes of strongly regular graphs*, Des. Codes Cryptogr., 17 (1999), pp. 187–209.

[17] W. C. Huffman, *Codes and groups*, in Handbook of coding theory, Vol. I, II, North-Holland, Amsterdam, 1998, pp. 1345–1440.

[18] J. Key and B. G. Rodrigues, *Minimal PD-sets for codes associated with the graphs Q_2^m, m even*, Appl. Algebra Engrg. Comm. Comput., (2021), pp. 1–10.

[19] J. D. Key and J. Limbupasiriporn, *Partial permutation decoding for codes from Paley graphs*, in Proceedings of the Thirty-Fifth Southeastern International Conference on Combinatorics, Graph Theory and Computing, vol. 170, 2004, pp. 143–155.

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

[21] ——, *Information sets and partial permutation decoding for codes from finite geometries*, Finite Fields Appl., 12 (2006), pp. 232–247.

[22] ——, *Improved partial permutation decoding for Reed-Muller codes*, Discrete Math., 340 (2017), pp. 722–728.

[23] J. D. Key, J. Moori, and B. G. Rodrigues, *Binary codes from graphs on triples*, Discrete Math., 282 (2004), pp. 171–182.

[24] ——, *Partial permutation decoding of some binary codes from graphs on triples*, Ars Combin., 91 (2009), pp. 363–371.

[25] ——, *Ternary codes from graphs on triples*, Discrete Math., 309 (2009), pp. 4663–4681.

[26] ——, *Codes associated with triangular graphs and permutation decoding*, Int. J. Inf. Coding Theory, 1 (2010), pp. 334–349.

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

[28] ——, *Special LCD codes from Peisert and generalized Peisert graphs*, Graphs Combin., 35 (2019), pp. 633–652.

[29] J. D. Key and B. G. Rodrigues, *Binary codes from m-ary n-cubes Q_n^m*, Adv. Math. Commun., 15 (2021), pp. 507–524.

[30] J. D. Key and P. Seneviratne, *Permutation decoding for binary self-dual codes from the graph Q_n where n is even*, in Advances in coding theory and cryptography, vol. 3 of Ser. Coding Theory Cryptol., World Sci. Publ., Hackensack, NJ, 2007, pp. 152–159.

[31] J. D. Key and P. Seneviratne, *Partial permutation decoding for MacDonald codes*, Appl. Algebra Engrg. Comm. Comput., 27 (2016), pp. 399–412.

[32] H.-J. Kroll, *Remarks on the paper "Binary codes from designs from the reflexive n-cube"*. Private communication, 2020.

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

[34] H.-J. Kroll and R. Vincenti, *Antiblocking decoding*, Discrete Appl. Math., 158 (2010), pp. 1461–1464.

[35] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes. I*, North-Holland Mathematical Library, Vol. 16, North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.

[36] J. Macwilliams, *Permutation decoding of systematic codes*, Bell Syst. Tech. J., 43 (1964), pp. 485–505.

[37] J. L. Massey, *Linear codes with complementary duals*, vol. 106/107, 1992, pp. 337–342. A collection of contributions in honour of Jack van Lint.

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

Please cite this article using:

Jennifer D. Key, Bernardo G. Rodrigues, Codes from m-ary n-cubes Q_n^m: A survey, AUT J. Math. Comput., 4(1) (2023) 1-15
DOI: 10.22060/AJMC.2022.21668.1098