ORIGINAL PAPER

Minimal PD-sets for codes associated with the graphs Q_2^m, m even

J. D. Key[1] · **B. G. Rodrigues**[2]

Received: 6 August 2020 / Accepted: 8 December 2020

Abstract
For $m \geq 4$ even, the duals of p-ary codes, for any prime p, from adjacency matrices for the m-ary 2-cube Q_2^m are shown to have subcodes with parameters $[m^2, 2m-2, m]$ for which minimal PD-sets of size $\frac{m}{2}$ are constructed, hence attaining the full error-correction capabilities of the code, and, as such, the most efficient sets for full permutation decoding.

Keywords Lee graphs · LCD codes · Permutation decoding

Mathematics Subject Classification 05C50 · 94B05

1 Introduction

In [14] binary codes generated by the row span of adjacency matrices of the graphs from the m-ary n-cube Q_n^m with adjacency defined by the Lee metric, were studied, and some notable results were obtained when $n = 2$ and m is odd, in which case the codes are *LCD*. In particular, minimal s-PD-sets were obtained (i.e. of size $s+1$) for $s \leq t-1$, where t is the error correcting capability of the code. Such sets are as efficient in decoding as is possible for permutation decoding, so it is useful to find them, in particular to find them up to $s = t$, for the codes for which that is possible. Here we look at the p-ary codes for $n = 2$ and $m \geq 4$ even, and any prime p, and find subcodes of $C_p(Q_2^m)$ for which PD-sets of minimal size $t+1$ are found.

✉ J. D. Key
keyj@clemson.edu

B. G. Rodrigues
bernardo.rodrigues@up.ac.za

[1] Institute of Mathematics, Physics and Computer Science, Aberystwyth University, Aberystwyth SY23 3BZ, UK

[2] Department of Mathematics and Applied Mathematics, University of Pretoria, Hatfield 0028, South Africa

We follow the standard definition of the graphs, known as Lee graphs, as in, for example [5]: for $m, n \geq 2$ positive integers, and $R = \{0, 1, \ldots, m-1\}$ with addition and multiplication as in the ring of integers modulo m, $\mathbf{Z}_m$, or possibly the field $\mathbb{F}_m$ if m is a prime power, 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 $j \neq i$. It follows that Γ is regular of degree $2n$.

In this study we examine specific subcodes of the dual of the p-ary codes from the adjacency matrices of these graphs when $n = 2$ and $m \geq 4$ is even. This follows work done in [14] for which the main results were for binary codes when $m \geq 5$ is odd, specifically for Q_2^m. Some of the results from that paper generalize immediately to the p-ary case.

Since for $m = 2, 3$ the graph is the Hamming graph, the codes of which have been widely studied (see [6–9, 15], for example) we take $m \geq 4$.

A summary of our main result is:

Theorem 1 *Let $\Gamma = Q_2^m$ where $m \geq 4$ is even, and let $C = C_p(\Gamma)$, 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 code D is described in Proposition 1, and the rest of the proof of the theorem is in Proposition 2. These follow after Sect. 2 giving the terminology and background.

2 Background concepts and terminology

The notation for codes 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 $C_F(\mathcal{D}) = C_q(\mathcal{D})$** of $\mathcal{D}$ over the finite field $F = \mathbb{F}_q$ is the space spanned by the incidence vectors of the blocks over F. If $\mathcal{Q} \subseteq \mathcal{P}$, then the **incidence vector** of $\mathcal{Q}$ is written $\boldsymbol{v}^{\mathcal{Q}}$, or $\boldsymbol{v}^x$ if $\mathcal{Q} = \{x\}$. 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 q-ary code C of length n, dimension k, and minimum weight d, where the **weight wt ($\boldsymbol{v}$)**

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 $\mathrm{wt}(u - v)$. 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 $\mathrm{Hull}(C) = C \cap C^\perp$. If $\mathrm{Hull}(C) = \{0\}$ then C and $C^\perp$ are **linear codes with complementary dual** (*LCD*) codes. A **check matrix** for C is a generator matrix for $C^\perp$. The **all-one vector** will be denoted by $\boldsymbol{j}$, and is the vector with all entries equal to 1, and sometimes written $\boldsymbol{j}_\mathbf{m}$ if it has length m. A **constant vector** is a non-zero vector in which all the non-zero entries are the same. Two linear codes are **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 [11].

The **graphs**, $\Gamma = (V, E)$ with vertex set V and edge set E, discussed here are undirected with no loops. 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.

An **adjacency** matrix $A = [a_{x,y}]$ for Γ is a symmetric $|V| \times |V|$ matrix with rows and columns labelled by the vertices $x, y \in V$, and with $a_{x,y} = 1$ if $x \sim y$ in Γ, and $a_{x,y} = 0$ otherwise. The row corresponding to $x \in V$ in A will be denoted by r_x. In the following, we may simply identify r_x with the support of the row, so $r_x = \{y \mid x \sim y\} = N(x)$. 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 Sect. 1. For any $x \in R^n$, x_i denotes the i^{th} coordinate of x, for $0 \le i \le n - 1$.

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

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

If $\sigma_i \in S_n$ for $0 \le i \le n - 1$, then the map σ is defined by

$$\sigma^{-1} : x \mapsto < x_{0^{\sigma_0}}, x_{1^{\sigma_1}}, \ldots, x_{n-1^{\sigma_{n-1}}} > \tag{2}$$

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

For any i such that $0 \le i \le n - 1$, the map μ_i is defined by

$$\mu_i : x =< x_0, \ldots, x_{i-1}, x_i, x_{i+1}, \cdots > \mapsto < x_0, \ldots, x_{i-1}, -x_i, x_{i+1}, \cdots >, \tag{3}$$

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 $(Q_1^m)^{\Box,n}$ of n copies of Q_1^m. 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

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

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

$$A_{n,m} = \begin{bmatrix} A_{n-1,m} & I & 0 & 0 & \cdots & 0 & I \\ I & A_{n-1,m} & I & 0 & \cdots & 0 & 0 \\ 0 & I & A_{n-1,m} & I & \cdots & 0 & 0 \\ \vdots & & \vdots & & & \vdots & \\ 0 & 0 & 0 & 0 & \cdots I & A_{n-1,m} & I \\ I & 0 & 0 & 0 & \cdots & I & A_{n-1,m} \end{bmatrix}, \tag{4}$$

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

As was noted in [14, Corollary 3], the graphs Q_m^n are bipartite if m is even.

2.2 Permutation decoding

Permutation decoding involves finding a set of automorphisms of a code called a PD-set and was first developed by MacWilliams [18], and is described fully in MacWilliams and Sloane [19, Chapter 16, p. 513] and Huffman [11, Section 8]. In [12] and [17] the definition of PD-sets was extended to that of s-PD-sets for s-error-correction:

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

For $s \leq t$ 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: for a t-error-correcting $[n, k, d]_q$ code C with check matrix H in standard form, so that a generator matrix can be written $G = [I_k|A]$ where $H = [-A^T|I_{n-k}]$, for some A, and the first k coordinate positions correspond to the information symbols. Let $S = \{g_1, \ldots, g_s\}$ be the PD-set.

Any vector v of length k is encoded as vG. Suppose x is sent and y is received and at most t errors occur. 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}.

Since this algorithm uses the PD-set as a sequence, the elements of the set S can be indexed by $\{1, 2, \ldots, |S|\}$ 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 $S_0 \subset S_1 \ldots \subset S_t$ 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 [4], from a formula due to Schönheim [20], and quoted and proved in [11]:

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

$$|S| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \ldots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \ldots \right\rceil \right\rceil \right\rceil = G(t). \tag{5}$$

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 [13, Lemma 1]:

Result 2 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 $s \leq \lfloor \frac{n}{k} \rfloor - 1$.

Thus a set of size $s + 1$ to correct s errors is a **minimal set** for s-error correction. Such sets for some cases where $G(t) = t + 1$ have been found for sporadic codes, but an infinite class for binary codes with parameters $[\binom{n}{2}, n - 1, n - 1]_2$ from the triangular graphs $T(n)$ with n odd are found in [16]. Here $t = \frac{n-3}{2}$ and PD-sets of size $t + 1 = \frac{n-1}{2}$ were found. Minimal sets up to $s = t - 1$ have been found in various papers, for example:[10, 13].

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 clearly the size z of the PD-set is important, and for any s this is at best $s + 1$, and thus $t + 1$ for full error correction.

3 The codes

Let $\Gamma = (V, E) = Q_2^m$, $m \geq 4$ even, $R = \{0, 1, \ldots, m - 1\}$, and $C = C_p(\Gamma)$, p prime. Recall that row $r_{<x,y>}$ denotes the row of an adjacency matrix for Γ corresponding to the vertex $< x, y >$.

Lemma 1 *For m even, $m \geq 4$, and any prime p, let*

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

Then $w = v^{S_1} - v^{S_2} \in C^{\perp}$.

Proof We need to show that $(r_{<a,b>}, w) \equiv 0 \pmod{p}$ for every $< a, b > \in V$. Now the non-zero entries in $r_{<a,b>}$, i.e. the neighbours of $< a, b >$, are

$$\{< a \pm 1, b >, < a, b \pm 1 >\}.$$

Suppose $r_{<a,b>}$ meets $\mathrm{Supp}(w) = S_1 \cup S_2 = \Lambda$. Without loss of generality, suppose $< a+1, b > \in S_1$. Then $a + 1 = 2i$ and $b = 2i$, so $a = 2i - 1$ and $b - 1 = 2i - 1$, so $< a, b-1 > \in S_2$. Thus $(r_{<a,b>}, w) \equiv 0 \pmod{p}$. If $\mathrm{Supp}(r_{<a,b>})$ does not meet Λ then obviously $(r_{<a,b>}, w) \equiv 0 \pmod{p}$. This completes the proof. □

Corollary 1 *For m even, $m \geq 4$, and any prime p, the minimum weight of $C^{\perp}$ is m.*

Proof The lemma shows that there are words of weight m so the minimum weight is at most m. Now the proof of [14, Lemma 3.5] generalizes to hold for any p if it is modified to say that the minimum weight is at least m. The argument does not depend on the code being binary, or on m being even or odd. □

Similar to [14, Proposition 1] we have the following, where the automorphisms $\tau_{<a,b>}$ and μ_i are defined in Eqs. (1) and (3):

Proposition 1 *For m even and $m \geq 4$, and p any prime, $\Gamma = (V, E) = Q_2^m$, $C = C_p(\Gamma)$, 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 $\mathcal{U} = \{u_i, v_i \mid i \in R\}$. Then, over $\mathbb{F}_p$, $D = \langle \mathcal{U} \rangle \subseteq C^{\perp}$ has dimension $2m - 2$, D 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 $\mathrm{Hull}(D) = \{0\}$; *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.

Proof Clearly $|\mathcal{U}| = 2m$ and each point $< a, b >$ is in the support of exactly one u_i, *viz.* u_{a-b} and one v_j, *viz.* v_{-a-b}. Thus $\sum_{i \in R} u_i = \sum_{i \in R} v_i$, and the dimension of D is at most $2m - 1$. Notice that $a - b$ and $-a - b$ are both even or both odd.

If we arrange the points in V by first placing those with both entries even, then those with both entries odd, then those with the first entry even and the second odd, and finally those with the first entry odd and the second even, we see that $\sum_{i \text{ even}} u_i = \sum_{i \text{ even}} v_i$ and that likewise $\sum_{i \text{ odd}} u_i = \sum_{i \text{ odd}} v_i$. These

two relations are independent so $\dim(D) \leq 2m-2$. Now proceed as in the proof of [14, Proposition 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 $w = \sum_{i=0}^{m-1} \alpha_i (u_i - v_i) = 0$. Since $\alpha_{a-b} = -\beta_{-a-b} = \alpha_{-a-b}$, we have $\alpha_c = \alpha_{-c-2b}$ for all c, b and hence α_a is constant over a even and over a odd. Thus $w = \alpha \sum_{i \text{ even}} (u_i - v_i) + \beta \sum_{i \text{ odd}} (u_i - v_i) = 0$. Each of these sums is already zero so we have no new relations and $\dim(D) = 2m-2$.

For $\mathrm{Hull}(D)$, suppose $w = \sum_{i \in R} \alpha_i u_i + \sum_{i \in R} \beta_i v_i \in D \cap D^{\perp}$. Then $(w, u_i) = (w, v_i) = 0$ for all $i \in R$. Clearly $(u_i, u_i) = (v_i, v_i) = m$ for all i, and $(u_i, u_j) = (v_i, v_j) = 0$ for all $i \neq j$. Suppose $< x, y > \in \mathrm{Supp}(u_i) \cap \mathrm{Supp}(v_j)$. Then it is easy to show that $< x + \frac{m}{2}, y + \frac{m}{2} > \in \mathrm{Supp}(u_i) \cap \mathrm{Supp}(v_j)$, that the supports of u_i and v_j meet exactly twice, and that i and j are both even or both odd. Furthermore if $< x, y > \in \mathrm{Supp}(u_i) \cap \mathrm{Supp}(v_j)$ then $< x + j - i, y > \in \mathrm{Supp}(u_j) \cap \mathrm{Supp}(v_i)$. Conversely, if i, j are both even or both odd, then u_i and v_j have precisely two points in common in their supports.

If $p = 2$ then clearly D is self-orthogonal from what was said above, so $\mathrm{Hull}(D) = D$. For p odd, taking first $p \nmid m$ and i even, $w \in D \cap D^{\perp}$ as above, we have $(w, u_i) = m\alpha_i + 2 \sum_{j \text{ even}} \beta_j = 0$, and thus, since $p \nmid m$, $\alpha_i = \alpha$ for all even i. Likewise $\alpha_i = \beta$ for all odd i. Taking $(w, v_i) = 0$ gives $\beta_i = \gamma$ for i even and $\beta_i = \delta$ for i odd. Then since $m\alpha_i + 2 \sum_{j \text{ even}} \beta_j = 0$ we have $m\alpha + 2\frac{m}{2}\gamma = 0$, so $\alpha = -\gamma$ and similarly $\beta = -\delta$. Thus $w = \alpha \sum_{i \text{ even}} (u_i - v_i) + \beta \sum_{i \text{ odd}} (u_i - v_i)$. Since we showed above that each of the two sums is zero, we have also $w = 0$, proving that $D \cap D^{\perp} = \{0\}$.

Now take $p | m$. Again if $w = \sum_{i \in R} \alpha_i u_i + \sum_{i \in R} \beta_i v_i \in D^{\perp}$ then $(w, u_i) = m\alpha_i + 2 \sum_{j \text{ even}} \beta_j = 0$, and since $m\alpha_i = 0$, we have $\sum_{j \text{ even}} \beta_j = 0$, and likewise $\sum_{j \text{ even}} \alpha_j = 0$, $\sum_{j \text{ odd}} \beta_j = 0$ and $\sum_{j \text{ odd}} \alpha_j = 0$. Thus, in particular, all the words $u_i - u_j$ and $v_i - v_j$ where i, j are both even or both odd, will be in $D^{\perp}$. Thus $\langle \mathrm{Hull}(D), u_0, u_1, v_0, v_1 \rangle = D$ and hence $\dim(\mathrm{Hull}(D)) \geq 2m-6$. To show it is exactly this, note that $\langle \mathrm{Hull}(D), u_0 \rangle$ contains all the u_i for i even, but not u_i for i odd, since if $u_1 = \alpha u_0 + w$, where $w \in \mathrm{Hull}(D)$ then $u_1 - \alpha u_0 \in \mathrm{Hull}(D)$ and thus $(u_1 - \alpha u_0, v_i) = 0$, for all i and this is not possible as v_i cannot meet both u_0 or u_0. In a similar way one can argue that $v_0 \notin \langle \mathrm{Hull}(D), u_0, u_1 \rangle$, and then that $v_1 \notin \langle \mathrm{Hull}(D), u_0, u_1, v_0 \rangle$. Thus $\dim(\mathrm{Hull}(D)) = 2m-6$.

That D has minimum weight m follows from Corollary 1 since $D \subseteq C^{\perp}$ and does have words of weight m. That $D^{\perp}$ has minimum weight 2 follows as in the binary case, except that if $m \equiv 2 \pmod 4$ then $v^{<0,0>} + v^{<\frac{m}{2}, \frac{m}{2}>} \in D^{\perp}$, while if $m \equiv 0 \pmod 4$, $v^{<0,0>} - v^{<\frac{m}{2}, \frac{m}{2}>} \in D^{\perp}$.

To show that for $m \geq 6$ the words in $\mathcal{U}$ and their scalar multiples are the only words of weight m, we can proceed as in the proof of [14, Lemma 3.5]. Thus suppose $w \in D$ has support S and $|S| = m$. We use the fact $(w, u) = 0$ for all the weight-2 words in $D^{\perp}$, and $(w, r_X) = 0$ for all $X \in V$. Notice also that for any $< a, b > \in V$, $< a, b > \sim < x, y >$ if and only if $< a + \frac{m}{2}, b + \frac{m}{2} > \sim < x + \frac{m}{2}, y + \frac{m}{2} >$.

Taking $< 0, 0 > \in S$, we must also have $< \frac{m}{2}, \frac{m}{2} > \in S$, from the observation above. All the rows $r_X \ni < 0, 0 >$ must meet S again at least once, so considering the four rows containing $< 0, 0 >$, we need to include $< 1, 1 >, < -1, -1 >$ or $< 1, -1 >, < -1, 1 >$ to achieve this. Then also $< 1 + \frac{m}{2}, 1 + \frac{m}{2} >, < -1 + \frac{m}{2}, -1 + \frac{m}{2} >$ or $< 1 + \frac{m}{2}, -1 + \frac{m}{2} >, < -1 + \frac{m}{2}, 1 + \frac{m}{2} >$

must be included for the weight-2 vectors in $D^{\perp}$. This will cover the rows through $< \frac{m}{2}, \frac{m}{2} >$.

If $m = 6$ these six vertices give the support of u_0 if we make the first choice, and v_0 if we make the second. Without loss of generality, let us make the first choice, so we have $S = \mathrm{Supp}(u_0)$. If w is not a multiple of u_0 then we could produce a word of smaller weight in D. This proves the result for $m = 6$. Proceeding to $m \geq 8$, we need to consider the rows through $< 1, 1 >$ and we see that including $< 2, 2 > \sim < 1, 1 >$, and $< 2 + \frac{m}{2}, 2 + \frac{m}{2} >$ is required. If $m = 8$ we have u_0 again.

We now proceed inductively, as in the proof of [14, Lemma 3.5] where at each stage we need to include a neighbour of the vertex $< i, i > \in S$ for smallest i for which $< i + 1, i + 1 >$ is not included. The steps are similar to the proof of [14, Lemma 3.5], except that in that lemma m could be odd, and the code was binary.

This completes the proof for $m \geq 6$. For $m = 4$ there are more words of weight 4, for all p. For example, from Magma [2, 3] computations, the word with support $\{< 0, 0 >, < 2, 2 >, < 0, 2 >, < 2, 0 >\}$ is in D, but clearly not in $\mathcal{U}$. □

Extending the result obtained in Proposition 3 of [14], we have the following:

Proposition 2 *For $\Gamma = Q_2^m$ where $m \geq 4$ is even, $R = \{0, \ldots, m-1\}$, and $D = \langle \mathcal{U} \rangle$ over $\mathbb{F}_p$, p a prime, where $\mathcal{U}$ is as in Proposition 1:*

1. *the set*

$$\mathcal{I} = \{< 0, i > \mid i \in R\} \cup \{< 1, i > \mid i \in R \setminus \{m-2, m-1\}\} \tag{6}$$

   is an information set for D.
2. *For $s \leq \frac{m-2}{2}$, the set of $s + 1$ automorphisms*

$$S = \{\tau_{<2i,0>} \mid 0 \leq i \leq s\} \tag{7}$$

   is an s-PD-set of minimal size $s + 1$ for the code D with information set $\mathcal{I}$ as given in Eq. (6). *For $s = \frac{m}{2} - 1$, the full error correction property of the code is attained.*

Proof The proof follows the same lines as that of Lemma 4.1 and Proposition 3 of [14].

First we show that $\mathcal{I}$ is an information set. Use the notation of Proposition 1. Consider the generators of the code D, *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 $2m - 2$. Then the non-zero entries in these columns are: $u_0 \ni < 0, 0 >, - < 1, 1 >$; $u_{m-1} \ni - < 0, 1 >, < 1, 2 >$; $u_{m-2} \ni < 0, 2 >, - < 1, 3 >$; $\ldots$; $u_1 \ni - < 0, m-1 >, < 1, 0 >$; $v_0 \ni < 0, 0 >, - < 1, m-1 >$; $v_{m-1} \ni - < 0, 1 >, < 1, 0 >; \ldots$; $v_1 \ni - < 0, m-1 >, < 1, m-2 >$.

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

Consider now the lower m rows starting with v_0^*, and columns starting at $< 1,0 >$, we have $v_0^* \ni < 1,1 >, - < 1, m-1 >$; $v_{m-1}^* \ni < 1,0 >, - < 1,2 >$; $v_{m-2}^* \ni - < 1,1 >, < 1,3 >; \cdots; v_1^* \ni < 1, m-2 >, - < 1,0 >$. Reorder these rows as $v_{m-1}^*, v_{m-2}^*, \ldots, v_1^*, v_0^*$. Now replace the row of v_1^* by $v_1^{**} = v_1^* + v_{m-3}^* + v_{m-1}^*$ which is zero in all the columns of $< 1, i >$, and replace v_0^* by $v_0^{**} = v_0^* + v_{m-4}^* + v_{m-2}^*$ which is also zero in the columns of $< 1, i >$.There are leading entries ± 1 in the columns $< 1,0 >, \ldots < 1, m-2 >$, and thus we have an information set, since we already know the dimension is $2m-2$.

By Proposition 1, D is an $[m^2, 2m-2, m]_p$ code and can correct $t = \frac{m-2}{2}$ errors. It is quite straightforward to show that the bound $G(t)$ in Eq. (5) is $\frac{m}{2} = t+1$. Result 2 tells us that if $G(s) = s+1$ then $s \leq \lfloor \frac{m^2}{2m-2} \rfloor - 1$ which is $\frac{m}{2} - 1 = t$ here. Thus we take $s \leq \frac{m-2}{2}$ and show that the set S of Eq. (7) of size $s+1$ will correct s errors.

If all the s errors are in $\mathcal{I}$ then any non-identity element of S will take them all into $\mathcal{C}$, and if all the s errors are in $\mathcal{C}$ then the identity $\tau_{<0,0>}$ will keep all the errors in $\mathcal{C}$. 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 $1 \leq i_r \leq m-1$ 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. Thus any set of s images $i_r + 2i$, for $1 \leq i \leq s$ can contain 0 or 1 only once. 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. $\{e_r^{\tau_{<2i,0>}} \mid 1 \leq r \leq s-1\}$ 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 $\mathcal{C}$. This $\tau_{<2i,0>}$ will move the full set of s error positions to $\mathcal{C}$.

Thus S is an s-PD-set for $s \leq t$ of $s+1$ elements, and in particular, for $s = t$ we have a set of size $t+1 = \frac{m}{2}$ for full error correction. Furthermore, the set is nested by the natural order.[1] □

Thus the full proof of Theorem 1 is complete. □

Acknowledgements This work is based on the research supported by the National Research Foundation of South Africa (Grant Number 120846).

[1] Professor H.-J. Kroll has shown us a shorter, more compact, proof that the given set provides for full error correction.

References

1. Assmus, Jr, E. F., Key, J. D.: Designs and their codes. Cambridge University Press, Cambridge: 1992, Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993)
2. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system I: The user language. J. Symb. Comput. **24, 3/4**, 235–265 (1997)
3. Cannon, J., Steel, A., White, G.: Linear codes over finite fields, Handbook of Magma Functions. In: Cannon, J., Bosma, W. (eds.) Computational Algebra Group, Department of Mathematics, University of Sydney, V2.13, http://magma.maths.usyd.edu.au/magma, pp. 3951–4023 (2006)
4. Daniel, M.: Gordon, Minimal permutation sets for decoding the binary Golay codes. IEEE Trans. Inform. Theory **28**, 541–543 (1982)
5. Day, K., Ayyoub, A.E.A.: Fault diameter of k-ary n-cube networks. IEEE Trans. Parallel Distrib. Syst. **8**(9), 903–907 (1997)
6. Fish, W.: Binary codes and permutation decoding sets from the graph products of cycles. Appl. Algebra Eng. Commun. Comput. **28**(5), 369–389 (2017). https://doi.org/10.1007/s00200-016-0310-y
7. Fish, W., Key, J.D., Mwambene, E.: Graphs, designs and codes related to the n-cube. Discrete Math. **309**, 3255–3269 (2009)
8. Fish, W., Key, J.D., Mwambene, E.: Binary codes of line graphs from the n-cube. J. Symb. Comput. **45**, 800–812 (2010)
9. Fish, W., Key, J.D., Mwambene, E., Rodrigues, B.G.: Hamming graphs and LCD codes. J. Appl. Math. Comput. **61**, 461–479 (2019). https://doi.org/10.1007/s12190-019-01259-w
10. Fish, W., Key, J.D., Mwambene, E.: Partial permutation decoding for simplex codes. Adv. Math. Commun. **6**, 505–516 (2012)
11. Huffman, W.C.: Codes and groups. In: Pless, V.S., Huffman, W. C. (eds.) Handbook of Coding Theory, vol. 2, Part 2, Chapter 17, pp. 1345–1440. Elsevier, Amsterdam (1998)
12. Key, J.D., McDonough, T.P., Mavron, V.C.: Partial permutation decoding for codes from finite planes. Eur. J. Combin. **26**, 665–682 (2005)
13. Key, J.D., McDonough, T.P., Mavron, V.C.: Improved partial permutation decoding for Reed-Muller codes. Discrete Math. **340**, 722–728 (2017)
14. Key, J.D., Rodrigues, B.G.: Binary codes from m-ary n-cubes ${Q}^m_n$. Adv. Math. Commun. (2020). https://doi.org/10.3934/amc.2020079
15. Key, J. D., Seneviratne, P.: Permutation decoding for binary self-dual codes from the graph ${Q}_n$ where n is even, Advances in Coding Theory and Cryptology. Shaska, T., Huffman, W.C., Joyner, D., Ustimenko, V. (eds.) vol. 2, pp. 152–159. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, Series on Coding Theory and Cryptology (2007)
16. Kroll, H.-J., Taherian, S.-G., Vincenti, R.: Optimal antiblocking information systems for the binary codes related to triangular graphs. Adv. Math. Commun. (2020)
17. Kroll, H.-J., Vincenti, R.: PD-sets related to the codes of some classical varieties. Discrete Math. **301**, 89–105 (2005)
18. MacWilliams, F.J.: Permutation decoding of systematic codes. Bell System Tech. J. **43**, 485–505 (1964)
19. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1983)
20. Schönheim, J.: On coverings. Pac. J. Math. **14**, 1405–1411 (1964)