J. Algebra Comb. Discrete Appl.
3(1) • 37–44

Received: 19 May 2015
Accepted: 2 December 2015

Journal of Algebra Combinatorics Discrete Structures and Applications

Generalized hypercube graph $\mathcal{Q}_n(S)$, graph products and self-orthogonal codes

Research Article

Pani Seneviratne

Abstract: A generalized hypercube graph $\mathcal{Q}_n(S)$ has $\mathbb{F}_2^n = \{0,1\}^n$ as the vertex set and two vertices being adjacent whenever their mutual Hamming distance belongs to S, where $n \geq 1$ and $S \subseteq \{1, 2, \ldots, n\}$. The graph $\mathcal{Q}_n(\{1\})$ is the n-cube, usually denoted by $\mathcal{Q}_n$. We study graph boolean products $G_1 = \mathcal{Q}_n(S) \times \mathcal{Q}_1, G_2 = \mathcal{Q}_n(S) \wedge \mathcal{Q}_1$, $G_3 = \mathcal{Q}_n(S)[\mathcal{Q}_1]$ and show that binary codes from neighborhood designs of G_1, G_2 and G_3 are self-orthogonal for all choices of n and S. More over, we show that the class of codes C_1 are self-dual. Further we find subgroups of the automorphism group of these graphs and use these subgroups to obtain PD-sets for permutation decoding. As an example we find a full error-correcting PD set for the binary $[32, 16, 8]$ extremal self-dual code.

2010 MSC: 05, 51, 94

Keywords: Graphs, Designs, Codes, Permutation decoding

1. Introduction

The generalized hypercube graphs $\mathcal{Q}_n(S)$ were introduced in Berrachedi and Mollard [1], where the authors mainly investigated the graph embeddings especially when the underlying graph is a hypercube. Their connections to $(0, 2)$-graphs were studied in Laborde and Madani [6].

Binary codes from the row span of an adjacency matrix for the n-cube were first examined in Key and Seneviratne [5] and the codes in the case of n even were found to be self-dual with minimum weight n. Further 3-PD-sets were found for partial permutation decoding. In [2], Fish, Key and Mwambene extended the results in [5] to graphs $\Gamma_n^k = \mathcal{Q}_n(\{k\})$, when $k = 1, 2, 3$.

In this paper we study generalized hypercube graphs and binary codes from the neighborhood designs of their boolean products. Similar to the n-cube, we prove that the graphs $\mathcal{Q}_n(S)$ are Cayley graphs and hence are vertex transitive. In particular we study the codes from graph boolean products and show that they are self-orthogonal and if the boolean product is the graph cartesian product, then the codes

Pani Seneviratne; Texas A&M University-Commerce, USA (email: padmapani.seneviratne@tamuc.edu).

http://dx.doi.org/10.13069/jacodesmath.13099

ISSN 2148-838X

are self-dual. This construction leads to many optimal codes and we use properties of these graphs to determine the properties of the codes.

Sections 2 gives the necessary background material and definitions. In Section 3 properties of the generalized hypercube graph are studied. The binary codes from the graph boolean products are studied in Section 4. In Section 5 we find PD-sets for permutation decoding.

2. Background and terminology

2.1. Codes

All the codes discussed in this paper are linear codes, i.e. subspaces of the vector space $\mathbb{F}^n$ where $\mathbb{F}$ is the finite field. The *support* of a vector u in $\mathbb{F}^n$ is the set of non-zero coordinates positions of u, and the *weight* of u, denoted by $wt(u)$, is the cardinality of its support. The notation $[n, k, d]_q$ will be used for a q-ary code of length n, dimension k, and minimum weight d. The *dual code* $C^\perp$ of C is the orthogonal complement of C under the standard inner product $<,>$, i.e. $C^\perp = \{v \in \mathbb{F}^n \mid < v, c >= 0 \text{ for all } c \in C\}$. The dual code $C^\perp$ is linear over the field $\mathbb{F}$. A *generator matrix* of C is a matrix whose rows are vectors of a basis for C. Two linear codes of the same length and over the same field are *isomorphic* if they can be obtained from one another by permuting the coordinate positions. An isomorphism from a code C into itself is called an *automorphism* of C, and the group of all automorphisms of C will be denoted by $Aut(C)$. Any code is isomorphic to a code with generator matrix in so-called standard form, i.e. the form $[I_k \mid A]$. In this case, a *check matrix* of C, i.e. a generator matrix of $C^\perp$, is then given by $[-A^T \mid I_{n-k}]$. An *information set* for a code is the set of the first k coordinates in the standard form and the *corresponding check set* is the set of the last $n-k$ coordinates.

2.2. Graphs

The graphs $\Gamma = (V, E)$ with vertex set V and edge set E, discussed here are simple graphs. If two distinct vertices x and y in V are adjacent, then we write $x \sim y$, and denote $[x, y]$ for the edge they define. The set of vertices in Γ that are adjacent to a vertex x is the *neighbour set* of x and is denoted by $N(x)$. The cardinality of $N(x)$ is the *valency* of x. A graph is *regular* if all the vertices have the same valency. An adjacency matrix A of a graph of order n is an $n \times n$ matrix with entries a_{ij} such that $a_{ij} = 1$ if vertices v_i and v_j are adjacent, and $a_{ij} = 0$ otherwise. The neighborhood design of a regular graph is the design formed by taking the points to be the vertices of the graph and the blocks to be the neighbor sets of the vertices. The code of a graph Γ over a finite field $\mathbb{F}_q$ is the row span of an adjacency matrix A over the field $\mathbb{F}_q$, denoted by $\mathcal{C}_q(\Gamma)$ or $\mathcal{C}(\Gamma)$ if the underlying field is obvious.

Let $J = J_p$ be the $p \times p$ matrix with all entries 1 and let $I = I_p$ be the identity matrix of order p. Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be matrices of size $p_1 \times p_1$ and $p_2 \times p_2$ respectively. Their tensor product, also known as the Kronecker product $A * B$ is defined as the partitioned matrix $[a_{ij}B]$:

$$A * B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1p_1}B \\ a_{21}B & a_{22}B & \cdots & a_{2p_1}B \\ \cdots & \cdots & \cdots & \cdots \\ a_{P_1 1}B & a_{p_1 2}B & \cdots & a_{p_1 p_1}B \end{pmatrix}.$$

A boolean operation on an ordered pair of disjoint graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ results in a graph $G = G_1 \circ G_2$ which has the cartesian product $V = V_1 \times V_2$ as its vertex set and the edge set E is expressed in terms of E_1 and E_2, differently for each boolean operation. In [3], Harary and Wilcox gave a detailed explanation of the follwoing boolean operations. The cartesian product is the boolean operation $G = G_1 \times G_2$ in which for any two points $u = (u_1, u_2)$ and $v = (v_1, v_2) \in V = V_1 \times V_2$, the edge $[u, v]$ is in $E(G)$ whenever $u_1 = v_1$ and $u_2 \sim v_2$ or $u_1 \sim v_1$ and, $u_2 = v_2$. We can express the adjacency matrix , $A(G_1 \times G_2) = (A_1 * I_{p_2}) + (I_{p_1} * A_2)$. The conjunction or the Kronecker product

$G = G_1 \wedge G_2$: For any two points $u = (u_1, u_2)$ and $v = (v_1, v_2) \in V = V_1 \times V_2$, the edge $[u, v]$ is in $E(G)$ if $[u_1, v_1] \in E(G_1)$ and $[u_2, v_2] \in E(G_2)$. The adjacency matrix of the conjunction $G_1 \wedge G_2$ is the tensor product $A(G_1 \wedge G_2) = A_1 * A_2$ of the adjacency matrices A_1 and A_2. The composition or the lexicographical product $G = G_1[G_2]$ is the graph with $u = (u_1, u_2)$ and, $v = (v_1, v_2)$ are adjacent whenever $u_1 \sim v_1$ or $u_1 = v_1$ and $u_2 \sim v_2$. The adjacency matrix of the composition is given by $A(G_1[G_2]) = (A_1 * J_{p_2}) + (I_{p_1} * A_2)$. Similarly we can define the composition $[G_1]G_2$ by its adjacency matrix $A([G_1]G_2) = (A_1 * I_{p_2}) + (J_{p_1} * A_2)$.

2.3. Permutation decoding

Permutation decoding is described fully in MacWilliams and Sloane [7, Chapter 16] and Huffman [4, Section 8]. A PD-set defined here will fully use the error-correction potential of the code which follows easily and is proved in [4].

Definition 2.1. *Let C be a t-error-correcting code with information set $\mathcal{I}$ and check set $\mathcal{C}$. 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 $\mathcal{C}$.*

Permutation decoding employs the following theorem in [4, Theorem 8.1] to ensure that all the errors in a received vector are moved out of the information symbols.

Theorem 2.2. *Let C be a t-error-correcting $[n, k, d]_q$ code with check matrix H that has the identity matrix I_{n-k} in the redundancy positions. Suppose $y = c + e$ is a vector where $c \in C$ and e has weight $s \leq t$. Then the information symbols in y are correct if and only if the weight of the syndrome Hy^T of y is $\leq s$.*

The algorithm for permutation decoding can then be stated as follows: we have a t-error-correcting $[n, k, d]_q$ code C with generator matrix G and check matrix H in standard form, i.e. $G = [I_k|A]$ and $H = [-A^T|I_{n-k}]$, where A is a $k \times (n-k)$ matrix, so that the first k coordinate positions correspond to the information symbols. Any message v of length k is then encoded as vG. Suppose x is a sent codeword and y is a received vector with at most t errors. Let $\mathcal{S} = \{g_1, \ldots, g_m\}$ be a PD-set for C. Compute the syndromes $H(yg_i)^T$ for $i = 1, \ldots, m$ 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}.

3. Generalized hypercube graph $\mathcal{Q}_n(S)$

For a positive integer n, let $S \subseteq [n] = \{1, 2, \ldots, n\}$ and let $\oplus$ denote the addition in $\mathbb{F}_2^n = \{0, 1\}^n$. The Hamming distance of vectors $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_2^n$ is $d(u, v) = |\{i \in S \mid u_i \neq v_i\}|$.

Definition 3.1. *The generalized hypercube graph $\mathcal{Q}_n(S) = (V, E)$ is an undirected graph with the vertex set $V(\mathcal{Q}_n(S)) = \mathbb{F}_2^n$ and the edge set $E(\mathcal{Q}_n(S) = \{uv \mid d(u, v) \in S\}$.*

The cardinality of the vertex set is independent of the choice of S and is equal to 2^n and is regular with valency $\sum_{i \in S} \binom{n}{i}$.

We will use the following notation: for $r \in \mathbb{Z}$ and $0 \leq r \leq 2^n - 1$, if $r = \sum_{i=1}^{n} r_i 2^{i-1}$ is the binary representation of r, let $\mathbf{r} = (r_1, r_2, \ldots, r_n)$ be the correspondng vector in $\mathbb{F}_2^n$. Standard basis of the vector space V_n will be denoted by $e_1, e_2, \ldots, e_n$.

An automorphism σ of a graph $\Gamma = (V, E)$ is a bijection $\sigma : V \mapsto V$ such that $[u, v] \in E$ if and only if $[\sigma(u), \sigma(v)] \in E$. The set of all automorphisms of Γ is a group and is denoted by $Aut(\Gamma)$. A group G acts transitively on a set V, if for every $u, v \in V$ there is a $\sigma \in G$ such that $\sigma(u) = v$. A graph $\Gamma = (V, E)$ is vertex transitive if $Aut(\Gamma)$ acts transitively on V.

Definition 3.2. *For $n \geq 1$, $u = (u_1, u_2, \dots, u_n) \in \mathbb{F}_2^n$ and $\sigma \in S_n$, where S_n is the symmetric group on the set $[n]$.*

- *A translation by u is the map $\tau_u : w \mapsto w \oplus u$, for all $w \in \mathbb{F}_2^n$.*
- *A rotation by σ is the map $r_\sigma : w \mapsto w_\sigma$, where $w_\sigma = (w_{\sigma(1)}, w_{\sigma(2)}, \dots, w_{\sigma(n)})$ for $w = (w_1, w_2, \dots, w_n)$.*

Lemma 3.3. *The group of translations $T_n = \{\tau_u \mid u \in \mathbb{F}_2^n\}$ and the group of rotations R_n are subgroups of $Aut(\mathcal{Q}_n(S))$.*

Proof. Clearly, $\tau_x \cdot \tau_y = \tau_{x \oplus y}$, $\tau_x^{-1} = \tau_x$ and $\tau_{\mathbf{0}} = \imath$. Further $d_H(u \oplus w, v \oplus w) = d_H(u, v)$. Therefore the set $T_n = \{\tau_u \mid u \in \mathbb{F}_2^n\}$ is a subgroup of $Aut(\mathcal{Q}_n(S)$. For rotations, we have $r_\sigma \cdot r_\rho = r_{\sigma \cdot \rho}$, $r_\sigma^{-1} = r_{\sigma^{-1}}$ and $r_{id} = \imath$. Hence, the set of all rotations R_n is a sugbroup of $Aut(\mathcal{Q}_n(S))$ and in fact $R_n \cong S_n$. □

Theorem 3.4. *The generalized hypercube graph $\mathcal{Q}_n(S)$ is vertex transitive.*

Proof. Every Cayley graph $\Gamma = Cay(G, S)$ is vertex transitive. We will show that the graph $\mathcal{Q}_n(S)$ is a Cayley graph. It is well known that the the hypercube graph $\mathcal{Q}_n$ can be defined as the Cayley graph $Q_n = Cay(T_n, \{e_1, e_2, \dots, e_n\})$. Similarly we can extend this result to the generalized hypercube graph $\mathcal{Q}_n(S)$. Let E_1 denote the set of weight 1 vectors $\{e_1, e_2, \dots, e_n\}$ in $\mathbb{F}_2^n$, E_2 denote the weight 2 vectors $\{\sum_{i,j}^n e_i + e_j | i \neq j\}$ and so on. Then it it easy to see that $\mathcal{Q}_n(S) = Cay(T_n, \{E_1, E_2, \dots, E_n\})$. □

4. Self-orthogonal codes from $\mathcal{Q}_n(S)$

In this Section we determine the binary codes C_1, C_2 and C_3 from the neighborhood designs of graph products $G_1 = \mathcal{Q}_n(S) \times \mathcal{Q}_1$, $G_2 = \mathcal{Q}_n(S) \wedge \mathcal{Q}_1$ and $G_3 = \mathcal{Q}_n(S)[\mathcal{Q}_1]$ respectively.

Lemma 4.1. *Let A be the adjacency matrix of the graph $\mathcal{Q}_n(S)$, then*

$$A^2 = \begin{cases} \mathbf{0} & mod\, 2 : \text{if } \sum_{i \in S} \binom{n}{i} \text{ is even.} \\ I_{2^n} & mod\, 2 : \text{otherwise.} \end{cases}$$

Proof. Let v_i, v_j be vertices of $\mathcal{Q}_n(S)$ such that $i \neq j$ and let $N(v_i)$ and $N(v_j)$ be the neighborhoods of v_i and v_j respectively. Since the $\mathcal{Q}_n(S)$ is regular $|N(v_i)| = |N(v_j)|$ and further $|N(v_i) \cup N(v_j)|$ is even. Therefore $|N(v_i) \cap N(v_j)|$ is even. But, $|N(v_i) \cap N(v_j)|$ is equal to the number of walks of length 2 between vertices v_i and v_j. Also, the $(i, j)^{th}$ entry of A^2 counts the number of walks of length 2 between the vertices v_i and v_j. Hence $(i, j)^{th}$ entry $= 0 \bmod 2$ for $i \neq j$. Next, suppose if $i = j$ then the $(i, i)^{th}$ entry of A counts the number of walks of length 2 from a vertex v_i to itself. Since $|N(v_i)|$ is equal to the valency of $\mathcal{Q}_n(S)$, $(i, i)^{th}$ entry of A is equal to 0 if valency is even and 1 if odd. Hence the result. □

Remark 4.2. *If C is the binary code from the neighborhood design of a graph G with the adjacency matrix A then we will use $\overline{C}$ to denote the corresponding binary code from the matrix $\overline{A} = A + I$. The matrix $\overline{A}$ is the adjacency matrix of the reflexive graph $\overline{G}$, which is obtained from G by adding a loop to every vertex.*

Theorem 4.3. *Let C_1, C_2 and C_3 be the binary codes from the neighborhood designs of the graph products $G_1 = \mathcal{Q}_n(S) \times \mathcal{Q}_1$, $G_2 = \mathcal{Q}_n(S) \wedge \mathcal{Q}_1$ and $G_3 = \mathcal{Q}_n(S)[\mathcal{Q}_1]$. Then the codes $C_1, \overline{C_2}$ and $\overline{C_3}$ are self-orthogonal if the valency of $\mathcal{Q}_n(S)$ is odd and $\overline{C_1}, C_2$ and $\overline{C_3}$ are self-orthogonal if the valency of $\mathcal{Q}_n(S)$ is even.*

Proof. Let A_1, A_2 and A_3 denote the adjacency matrices of the graph products G_1, G_2 and G_3 respectively. Let A denote the adjacency matrix of $\mathcal{Q}_n(S)$ and B denote the adjacency matrix of $\mathcal{Q}_1$. The identity matrix of size r is denoted by I_r and $N = 2^n$. We will use the fact that a binary code with the

generator matrix G is self-orthogonal if $GG^T = \mathbf{0}$.
Case I:

$$\begin{aligned} A_1A_1^T &= (A \otimes I_2 + I_N \otimes B)(A \otimes I_2 + I_N \otimes B)^T \\ &= (A \otimes I_2 + I_N \otimes B)(A^T \otimes I_2^T + I_N^T \otimes B^T) \\ &= (A \otimes I_2 + I_N \otimes B)(A \otimes I_2 + I_N \otimes B) \\ &= (A \otimes I_2)^2 + (I_N \otimes B)(A \otimes I_2) + (A \otimes I_2)(I_N \otimes B) + (I_N \otimes B)^2 \\ &= (A^2 \otimes I_2^2) + 2(A \otimes B) + (I_N^2 \otimes B^2) \\ &= A^2 \otimes I_2 + I_N \otimes I_2 \\ &= (A^2 + I_N) \otimes I_2. \end{aligned}$$

If the valency of $\mathcal{Q}_n(S)$ is odd, then $A^2 = I_N$ by Lemma 4.1, and hence $A_1A_1^T = \mathbf{0}$ mod 2. If valency is even then $A^2 = \mathbf{0}$. In this case $\overline{A_1} \cdot \overline{A_1}^T = A_1^2 + I_{2^{n+1}} = (A^2 + I_N) \otimes I_2 + I_{2^{n+1}} = \mathbf{0}$.
Case II:

$$A_2A_2^T = (A \otimes B)(A \otimes B)^T = (A \otimes B)(A \otimes B) = A^2 \otimes B^2 = A^2 \otimes I_2.$$

By Lemma 4.1, $A^2 = \mathbf{0}$ if valency of $\mathcal{Q}_n(S)$ is even and hence $A_2A_2^T = \mathbf{0} \otimes I_2 = \mathbf{0}$. If the valency of $\mathcal{Q}_n(S)$ is odd, consider $\overline{A_2} \cdot \overline{A_2}^T = A_2^2 + I_{2^{n+1}} = A^2 \otimes I_2 + I_{2^{n+1}} = I_N \otimes I_2 + I_{2^{n+1}} = \mathbf{0}$.
Case III:

$$\begin{aligned} \overline{A_3}\overline{A_3}^T &= (A \otimes J_2 + I_N \otimes B + I_{2^{n+1}})(A \otimes J_2 + I_N \otimes B + I_{2^{n+1}})^T \\ &= A^2 \otimes J_2^2 + A \otimes BJ_2 + A \otimes J_2 + A \otimes J_2B + I_N \otimes B^2 + I_N \otimes B \\ &\quad + A \otimes J_2 + I_N \otimes B + I_{2^{n+1}} \\ &= I_N \otimes I_2 + I_{2^{n+1}} = \mathbf{0}. \end{aligned}$$

□

Theorem 4.4. *The binary code C_1 from the neighborhood design of the graph product $G_1 = \mathcal{Q}_n(S) \times \mathcal{Q}_1$ is self-dual when the valency of $\mathcal{Q}_n(S)$ is odd and the code $\overline{C_1}$ is self-dual when the valency is even. Further the set of points $\mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots, \mathbf{2^n - 1}$ form an information set for C_1 and $\overline{C_1}$.*

Proof. We will change the ordering of points in the adjacency A_1 of the graph G_1. Use the natural ordering of points:

$$\mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots, \mathbf{2^n - 1}, \mathbf{2^n}, \ldots, \mathbf{2^{n+1} - 1}$$

to index the columns of A_1 and use the ordering

$$\mathbf{2^n}, \mathbf{2^n + 1}, \ldots, \mathbf{2^{n+1} - 1}, \mathbf{0}, \mathbf{1}, \ldots, \mathbf{2^{n-1}}$$

to index the rows. Then the $(i,i)^{th}$ entry $a_{ii} = 1$ for $1 \le i \le 2^n - 1$ and $a_{ii} = 0$ for $2^n \le i \le 2^{n+1} - 1$. By row reduction it is easy to see that the incidence vectors $v^{\mathbf{0}}, v^{\mathbf{1}}, \ldots, v^{\mathbf{2^n - 1}}$ are linear independent. Hence dimension of C_1 is 2^n and C_1 is self-dual. □

Remark 4.5. *Instead of using separate notations C_1 and $\overline{C_1}$ to denote codes from the graphs $\mathcal{Q}_n(S) \times \mathcal{Q}_1$ and $\overline{\mathcal{Q}_n(S) \times \mathcal{Q}_1}$ we will only use C_1 to denote codes from $\mathcal{Q}_n(S) \times \mathcal{Q}_1$ or $\overline{\mathcal{Q}_n(S) \times \mathcal{Q}_1}$ as it is understood when the valency is even C_1 refers to $\overline{C_1}$.*

Example 4.6. *Let $n = 3$ and $S = \{1, 3\}$. Then the valency of $\mathcal{Q}_n(S)$ is 4 with the adjacency matrix:*

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

Then $\overline{C_1} = [16, 8, 4]$ self-dual, $C_2 = [16, 4, 4]$ self-orthogonal and $\overline{C_3} = [16, 8, 2]$ self-dual codes.

5. Permutation decoding

In this Section we will find particular information sets for permutation decoding and use these sets to find partial permutation decoding sets for the codes C_1. The vertex set of the graph product $G_1 = \mathcal{Q}_n(S) \times \mathcal{Q}_1$ can be viewed as vectors of the space $\mathbb{F}_2^{n+1}$.

Theorem 5.1. *For all n and S and for $G_1 = \mathcal{Q}_n(S) \times \mathcal{Q}_1$:*

- *The translation group $T = \{\tau_u | u \in \mathbb{F}_2^{n+1}\}$ is a subgroup of $Aut(G_1)$.*
- *The group of rotations R_n is a subgroup of $Aut(G_1)$.*
- *Transpositions of the form $t_i = (i, n+1)$, where $1 \leq i < n$ are in $Aut(G_1)$.*

Proof. Since the translation group T and the group of rotations R_n are subgroups of the graph $Q_n(S)$, they are also subgroups of the graph cartesian product $G_1 = Q_n(S) \times Q_1$. Let $u = (u_1, u_2, \dots, u_{n+1}), v = (v_1, v_2, \dots, v_{n+1}) \in V(G_1)$ such that $u \sim v$. That is, $d(u, v) \in S$. Now $t_i u = (u_1, u_2, \dots, u_{n+1}, \dots, u_i)$ and $t_i v = (v_1, v_2, \dots, v_{n+1}, \dots, v_i)$, but $d(t_i u, t_i v) = d(u, v) \in S$. Hence $t_i \in Aut(G_1)$. □

The following result shows that any information set for C_1 from the graph $Q_n(\{1\})$ can be extended to a code from the graphs $Q_n(S)$, where $\{1\} \subseteq S$.

Lemma 5.2. *If $\mathcal{I}$ is an information set for C_1 with $S = \{1\}$, then $\mathcal{I}$ is an information set for C_1 for all S such that $\{1\} \subseteq S$.*

Proof. Since $\mathcal{I}$ is an information set for C_1 when $S = \{1\}$ and since the dimension of C_1 is 2^n the first 2^n incidence vectors are linearly independent. If we take any super set S that contains $\{1\}$ these first 2^n vectors will still be linearly independent and since the dimension of the code C_1 is 2^n is independent of the choice of S, the set $\mathcal{I}$ will be an information set for C_1 for all $\{1\} \subseteq S$. □

Permutation decoding method depends on the information set and hence different information sets will yield different PD-sets and results. The information set obtained in Theorem 4.4 is only useful for finding one error-correcting PD sets for C_1. We will re-order the vertices so that the resulting information set can be used for correcting more than one error.

Lemma 5.3. *An information set can be obtained for the binary code C_1 from the graph $G_1 = \mathcal{Q}_n(S) \times \mathcal{Q}_1$ for all n and $\{1\} \subseteq S$ by making the following interchange between the information and check sets from the natural ordering of the vectors: Move $\mathbf{2^n - 1} = (0, 1, 1, \dots, 1)$ into check positions and $\mathbf{2^{n+1} - 2} = (1, 1, \dots, 1, 0)$ into information positions.*

Define $P_n = \{t_i | 1 \leq i \leq n\} \cup \{\imath\}$ and $T_n = TP_n$.

Proposition 5.4. *With $\mathcal{I} = \{\mathbf{0}, \mathbf{1}, \dots, \mathbf{2^n - 2}\} \cup \{\mathbf{2^{n+1} - 2}\}$ as information set for C_1, T_n is a 3-PD set of size $(n+1)2^{n+1}$ for C_1 for all n and $\{1\} \subseteq S$.*

Proof. Let $\mathcal{T} = \{a, b, c\}$ be a set of three points in V_{n+1}. We need to show that there is an automorphism $\sigma \in T_n$ that maps $\mathcal{T}$ into $\mathcal{C}$, i.e. $\mathcal{T}^\sigma \subseteq \mathcal{C}$. We consider all the possibilities for the points in $\mathcal{T}$.
If $\mathcal{T} \subseteq \mathcal{C}$ then all the errors are in check positions and hence we can use the identity map, $\imath$ as σ. Thus, assume at least one of the points is in the information positions $\mathcal{I}$, and by using a translation, suppose one of the points, say c, is $\mathbf{0}$.
If $\mathcal{T} \subseteq \mathcal{I}$. First suppose both $a, b \in \mathcal{I}_1$, then $\sigma = T(1, 0, 0, \dots, 0)$ will map $\mathcal{T}$ to $\mathcal{C}$ unless $a, b \neq (0, 1, 1, \dots, 1, 0)$. In this case $\sigma = T(1, 1, 0, \dots, 0)$ will work. Next, suppose one of the points, say $b \in \mathcal{I}_2$ and $a \in \mathcal{I}_1$. Then $b = (1, 1, 1, \dots, 1, 0)$ and $\sigma = T(1, 0, \dots, 0, 1)$ will map $\mathcal{T}$ into $\mathcal{C}$.
The other cases for $\mathcal{T}$ involve one or more points in $\mathcal{C}$.
Case(i): $a \in \mathcal{I}_1$ and $b \in \mathcal{C}_1$. Then $a = (0, a_2, \dots, a_{n+1})$ and $b = (1, b_2, \dots, b_{n+1})$.
(1).Suppose $a = b_c$ and let $\sigma = T(1, a_2, \dots, a_{n+1})$ then $c\sigma = (1, a_2, \dots, a_{n+1})$, $a\sigma = (1, 0, \dots, 0)$ and $y\sigma = (0, 1, \dots, 1)$. This σ will work unless $a \neq (0, 1, \dots, 1, 0)$. In this case $b = a_c = (1, 0, \dots, 0, 1)$ and $\sigma = T(1, 1, \dots, 1, 0)$ will work.
(2). Suppose $a_i = b_i$ for $2 \leq i \leq n+1$. Then $a = (0, a_2, \dots, a_{n+1})$ and $b = (1, a_2, \dots, a_{n+1})$. If $\sigma = T(a_c)$, we have $c\sigma = a_c, a\sigma = (1, 1, \dots, 1), y\sigma = (0, 1, \dots, 1) \in \mathcal{C}$. (3). Suppose there exists an i such that $a_i = b_i = 0$ and $x_j \neq y_j$ for some j. The map $\sigma = T(1, 1, \dots, 1)t_i$ will work unless $a_{n+1} = b_{n+1} = 0$ is the only common zero. In this case $\sigma = T(0, \dots, 0, 1)t_i$ will work.
Case(ii): $a \in \mathcal{I}_2$ and $b \in \mathcal{C}_1$. Then $a = (1, 1, \dots, 1, 0)$ and $b = (1, b_2, \dots, b_{n+1})$. The map $\sigma = T(0, 1, \dots, 1)$ will work as $c\sigma = (0, 1, \dots, 1) \in \mathcal{C}_2, a\sigma = (1, 0, \dots, 0, 1) \in \mathcal{C}_2$ and $b\sigma = (1, b_{2c}, \dots, b_{n+1c}) \in \mathcal{C}_1$ unless $b = (1, 0, \dots, 0, 1)$, in which case the map $\sigma = T(0, \dots, 0, 1)t_{n+1}$ will work.
Case(iii): $a \in \mathcal{I}_2$ and $b \in \mathcal{C}_2$. Then $a = (1, \dots, 1, 0)$ and $b = (1, \dots, 1)$ or $b = (0, 1, \dots, 1)$. If $b = (1, \dots, 1)$ then $\sigma = T(1, 0, \dots, 0)t_{n+1}$ will work and otherwise if $b = (0, 1, \dots, 1)$, $\sigma = T(1, 0, 1, \dots, 1)t_2$ will work.
Case(iv): $a \in \mathcal{I}_1$ and $b \in \mathcal{C}_\in$. Then $a = (0, a_2, \dots, a_{n+1})$ and $b = (1, 1, \dots, 1)$ or $(0, 1, \dots, 1)$. If $a \neq (0, 1, \dots, 1, 0)$ then $\sigma = T(1, 0, \dots, 0)$ will work. If $a = (0, 1, \dots, 1, 0)$ and $b = (1, 1, \dots, 1)$ then $\sigma = T(1, 0, 1, \dots, 1)t_2$ and if $a = (0, 1, \dots, 1, 0), b = (0, 1, \dots, 1)$ then $\sigma = T(1, 0, \dots, 0, 1t_{n+1}$ will work.
Case(v): Both a and b in $\mathcal{C}_1$. Then $a = (1, a_2, \dots, a_{n+1})$ and $b = (1, b_2, \dots, b_{n+1})$. Then $\sigma = T(0, 1, \dots, 1)$ will work except when a or b equals $(1, 0, \dots, 0, 1)$. In this case $aT(1, \dots, 1)$ and $bT(1, \dots, 1)$ contain at least one common i such that $a_i = b_i = 1$. Then the map $\sigma = T(1, \dots, 1)t_i$ will work.
Case(vi): $a \in \mathcal{C}_1$ and $b \in \mathcal{C}_2$. Then $a = (1, a_2, \dots, a_{n+1})$ and $b = (1, \dots, 1)$ or $(0, 1, \dots, 1)$. If $b = (1, \dots, 1)$ then $\sigma = T(0, 1, \dots, 1)$ will work unless $a = (1, 0, \dots, 0, 1)$. In that case then $\sigma = T(1, 0, \dots, 0, 1)t_2$ will work. If $b = (0, 1 \dots, 1)$
Case (vii): Both $a, b \in \mathcal{C}_2$. In this case the map $\sigma = T(1, 0, \dots, 0)$ will work.
This completes all the cases. $\square$

Example 5.5. *Let $n = 4$ and $S = \{1, 2\}$, then $\mathcal{Q}_n(S)$ has valency 10 with the adjacency matrix:*

$$A = \begin{bmatrix}
0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0
\end{bmatrix}$$

and $\overline{C_1} = [32, 16, 8]$ *is the binary extremal doubly even self-dual code. The total error correcting capability of this code is* $t = 3$. *Then* $|T| = 32$ *and* $|P_n| = 5$ *and hence* $|TP_n| = 160$. *By Proposition 5.4 the set* TP_n *is a full error-correcting PD-set for this code.*

6. Conclusion

In this work we have considered the generalized hypercube graphs and their boolean products. We obtained self-orthogonal codes from the neighborhood designs of these graphs and used subgroups of the automorphism group of the graph to find partial permutation decoding sets for permutation decoding.

Acknowledgment: The author would like to thank the anonymous referees for their careful reading of the paper and for their insightful comments and suggestions.

References

[1] A. Berrachedi, M. Mollard, On two problems about $(0, 2)$-graphs and interval-regular graphs, Ars Combin. 49 (1998) 303–309.
[2] W. Fish, J. D. Key, E. Mwambene, Graphs, designs and codes related to the n-cube, Discrete Math. 309(10) (2009) 3255–3269.
[3] F. Harary, G. W. Wilcox, Boolean operations on graphs, Math. Scand. 20 (1967) 41–51.
[4] W. C. Huffman. Codes and groups. In V. Pless and W. C. Huffman, Eds., Handbook of coding theory, Vol. 2, pp. 1345–1440, Elsevier Science Publishers, Amsterdam, The Netherlands, 1998.
[5] J. D. Key, P. Seneviratne, Permutation decoding for binary self-dual codes from the graph Q_n, where n is even. In T. Shaska, W. C. Huffman, D. Joyner, and V. Ustimenko, Eds., Advances in Coding Theory and Cryptography, Series on Coding Theory and Cryptography, Vol. 3, pp. 152–159, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2007.
[6] J. M. Laborde, R. M. Madani, Generalized hypercubes and $(0, 2)$-graphs, Discrete Math. 165/166 (1997) 447–459.
[7] F. J. MacWilliams, N. J. A. Sloane, The theory of error-correcting codes, Amsterdam: North-Holland, 1998.
[8] M. Mulder, $(0, \lambda)$-graphs and n-cubes, Discrete Math. 28(2) (1979) 179–188.