© Algebra and Discrete Mathematics
Volume **32** (2021). Number 1, pp. 49–64
DOI:10.12958/adm1645 RESEARCH ARTICLE

Isodual and self-dual codes from graphs

S. Mallik and B. Yildiz

Communicated by V. A. Artamonov

Abstract. Binary linear codes are constructed from graphs, in particular, by the generator matrix $[I_n|A]$ where A is the adjacency matrix of a graph on n vertices. A combinatorial interpretation of the minimum distance of such codes is given. We also present graph theoretic conditions for such linear codes to be Type I and Type II self-dual. Several examples of binary linear codes produced by well-known graph classes are given.

1. Introduction

There is a strong connection between graphs and codes. The adjacency matrix of a simple graph is a symmetric binary matrix which has made it suitable for constructing binary codes. Depending on the structure of the graphs, special types of codes can be obtained.

We start with some basic definitions about codes that will be used throughout the paper. Let $\mathbb{F}_2$ be the binary field. A binary linear code C of length n is defined as a subspace of $\mathbb{F}_2^n$. If the dimension of C is k, we say C is an $[n,k]$-code. A matrix whose rows form a basis for C is called a *generator matrix* for C and is denoted by G. We also denote C by $C(G)$. By using elementary row and column operations, we can bring the generator matrix G into a standard form $[I_k|A]$ where A is a $k \times (n-k)$ matrix. Two binary codes are said to be *equivalent* if one can be obtained from the other by a permutation of coordinates.

2020 MSC: 94B05, 94B25.

Key words and phrases: self-dual codes, isodual codes, graphs, adjacency matrix, strongly regular graphs.

The *Hamming weight* $w_H(\boldsymbol{x})$ of a vector $\boldsymbol{x} \in \mathbb{F}_2^n$ is defined as the number of non-zero coordinates in $\boldsymbol{x}$. The *Hamming distance* between two vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ in $\mathbb{F}_2^n$, denoted by $d_H(\boldsymbol{x}, \boldsymbol{y})$, is defined as

$$d_H(\boldsymbol{x}, \boldsymbol{y}) = w_H(\boldsymbol{x} - \boldsymbol{y}).$$

The *minimum distance* of a code C, denoted by $d(C)$, is defined to be the minimum distance between distinct codewords in C. We write the standard parameters $[n, k, d]$ to describe a code C where n denotes the length of C, k its dimension, and d its minimum distance.

Definition 1. Let C be a binary linear code of length n. The *dual* of C, denoted by $C^\perp$, is given by

$$C^\perp := \{\boldsymbol{y} \in \mathbb{F}_2^n \mid \langle \boldsymbol{y}, \boldsymbol{x} \rangle = 0 \ \forall\, \boldsymbol{x} \in C\}.$$

Note that, if C is a linear $[n, k]$-code, then $C^\perp$ is a linear $[n, n-k]$-code.

Definition 2. A binary linear code C is *self-orthogonal* if $C \subseteq C^\perp$ and *self-dual* if $C = C^\perp$.

Definition 3. Let C be a self-dual binary code. If the Hamming weights of all the codewords in C are divisible by 4, then C is called **Type II** (or doubly-even), otherwise it is called **Type I** (or singly even).

The following theorem gives an upper bound for the minimum distance of self-dual codes:

Theorem 1 ([13]). *Let $d_I(n)$ and $d_{II}(n)$ be the minimum distances of a Type I and Type II binary code of length n respectively. Then*

$$d_{II}(n) \leqslant 4\lfloor \frac{n}{24} \rfloor + 4$$

and

$$d_I(n) \leqslant \begin{cases} 4\lfloor \frac{n}{24} \rfloor + 4 & \text{if } n \not\equiv 22 \pmod{24} \\ 4\lfloor \frac{n}{24} \rfloor + 6 & \text{if } n \equiv 22 \pmod{24}. \end{cases}$$

Self-dual codes that attain the bounds given in the previous theorem are called *extremal*.

Definition 4. A binary code C is said to be *isodual* if it is permutation equivalent to its dual.

Theorem 2. *If C is generated by $G = [I_k|A]$, then the generator matrix of $C^\perp$ is given by $H = [-A^T|I_k]$.*

H is also called the parity-check matrix of C, namely C is given by

$$C = \{\boldsymbol{c} \in \mathbb{F}_2^n | H\boldsymbol{c}^T = 0\}.$$

There is a natural connection between the parity-check matrix of a linear code and the minimum distance which is given by the following theorem:

Theorem 3. *Let C be a linear code and H a parity check matrix for C. Then*

(i) *$d(C) \geqslant d$ if and only if any $d-1$ columns of H are linearly independent.*

(ii) *$d(C) \leqslant d$ if and only if H has d columns that are linearly dependent.*

Corollary 1. *If C is a linear code and H is a parity check matrix for C, then C has minimum distance d if and only if any $d-1$ columns of H are linearly independent and some d columns of H are linearly dependent.*

The connection of codes and graphs has been explored from different aspects in the literature. The main theme in these works is to take a special class of graphs and construct codes from the adjacency matrix of the graph. The structure of the graph may lead to different types of codes as a result, such as self-dual codes, self-orthogonal codes, etc. We refer the reader to [2]–[12], [14] and [15] for some of these works.

In this work we focus on the following type of construction which was discussed in [15]. Let A be the adjacency matrix of a simple graph on n vertices. We construct the binary code C from the generator matrix $[I_n|A]$. Such a construction has several advantages which we can describe as follows:

1) The dimension of the codes is automatically determined as n. So we are looking at $[2n, n]$-codes.
2) A parity-check matrix of such a code is given by $[A^T|I_n] = [A|I_n]$ since A is symmetric
3) Note that a permutation of columns of $[A|I_n]$ will bring the matrix into $[I_n|A]$, which means any such code C is isodual.
4) Since the codes are isodual, to determine the conditions for self-duality, we just need to factor in the orthogonality conditions.

In addition to the conditions on the graph that would ensure self-duality of the constructed code, we also find upper bounds on the minimum distances of codes obtained via this construction. We give a combinatorial description to the exact minimum distances of such codes as well as codes obtained from just the adjacency matrix A as the generator matrix. We give examples of isodual and self-dual codes obtained through this construction.

The rest of the work is organized as follows. In section 2, we give the upper bounds and combinatorial descriptions for the minimum distances of codes obtained from graphs. In section 3, we give necessary and sufficient conditions for the codes to be self-dual, Type I and Type II. In addition, we describe how the join operation on graphs affects the self-duality conditions. We give several examples of self-dual codes obtained through the construction.

2. The $[I_n|A]$ construction for codes

As was mentioned in the Introduction, we focus mainly on the construction of binary codes generated by $[I_n|A]$ where A is the adjacency matrix of a simple graph. We start with the following observation:

Observation 4. Linear codes generated by $[I_n|A]$ and $[I_n|PAP^T]$, where P is a permutation matrix, are not necessarily the same. For example, consider the graph P_3 with adjacency matrix A and permutation matrix P generated by $(1,2)$:

$$[I_3|A] = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{array}\right]$$

$$[I_3|PAP^T] = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right]$$

$$(1,0,0,0,1,0) \in C([I_3|A]) = \{(a,b,c,b,a+c,b) \mid a,b,c \in \mathbb{F}_2\}$$

$$(1,0,0,0,1,0) \notin C([I_3|PAP^T]) = \{(a,b,c,b+c,a,a) \mid a,b,c \in \mathbb{F}_2\}.$$

It is not obvious that $C([I_3|A])$ and $C([I_3|PAP^T])$ have the same minimum distance.

The following result gives an upper bound of the minimum distance of a binary code in terms of the 2-rank (see [1]) of the corresponding graph.

Theorem 5. *Let A be the adjacency matrix of a graph on n vertices and let C be the binary linear code generated by $[I_n|A]$. Then we have*

$$d(C) \leqslant rk_2(A) + 1,$$

where $rk_2(A)$ denotes the rank of A as a matrix over $\mathbb{F}_2$.

Proof. Let $G = [I_n|A]$ be the generator matrix of C. Then $H = [-A^T|I_n]$ $= [A|I_n]$ is the parity-check matrix of C. By the definition of the rank, any set of $rk_2(A)+1$ columns of A are linearly dependent. By Theorem 2, $d(C) \leqslant rk_2(A)+1$. □

To get a combinatorial interpretation of the minimum distance of $C([I_n|A])$, we study the following set of vertices of a graph Γ with adjacency matrix A and vertex set V: for a nonempty subset S of V, the set of vertices of Γ with odd number of neighbors in S is denoted by $\mathrm{von}(S)$, i.e.,

$$\mathrm{von}(S) = \{v \in V \ : |\mathrm{N}(v) \cap S| \text{ is odd}\},$$

where $\mathrm{N}(v)$ denotes the set of neighbors of the vertex v in Γ. Note that S and $\mathrm{von}(S)$ have no inclusion-exclusion relationship that holds for all graphs as evident in the following examples.

Example 1.

1) Consider $\Gamma = C_4$ with vertices $1, 2, 3, 4$ consecutively adjacent. For $S = \{1\}$, $\mathrm{von}(S) = \{2, 4\} = \mathrm{N}(1)$. For $S = \{1, 2\}$, $\mathrm{von}(S) = \{1, 2, 3, 4\}$. For $S = \{1, 3\}$, $\mathrm{von}(S) = \varnothing$.
2) Consider $\Gamma = K_n$, $n \geqslant 4$ with vertex set $\{1, 2, \ldots, n\}$. For $S = \{1\}$, $\mathrm{von}(S) = \{2, 3, \ldots, n\} = \mathrm{N}(1)$. For $S = \{1, 2\}$, $\mathrm{von}(S) = \{1, 2\}$. For $S = \{1, 2, \ldots, n-1\}$ with even n, $\mathrm{von}(S) = \{n\}$. For $S = \{1, 2, \ldots, n-1\}$ with odd n, $\mathrm{von}(S) = \{1, 2, \ldots, n-1\}$.

Definition 5. Two vertices u and v of a graph are called *duplicate vertices* if they are not adjacent and $\mathrm{N}(u) = \mathrm{N}(v)$, i.e., they have the same neighbors.

Observation 6. Let Γ be a graph. If S is a set of two duplicate vertices of Γ, then $\mathrm{von}(S) = \varnothing$.

Proof. Let A be the adjacency matrix of Γ and A_i denote the column i of A. Without loss of generality, let $S = \{1, 2\}$. If 1 and 2 are duplicate vertices, then $A_1 + A_2 \equiv 0 \pmod 2$ which implies $\mathrm{von}(S) = \varnothing$. □

Linear dependency relations among columns of a matrix associated with graphs have been studied in [11]. We study the same in connection with von.

Theorem 7. *Let G be a graph with vertex set V and adjacency matrix A. Let S be a nonempty subset of V. If $\mathrm{von}(S) = \varnothing$, then the columns of A corresponding to S are linearly dependent. Conversely, if the columns of A corresponding to S are minimally linearly dependent, then $\mathrm{von}(S) = \varnothing$.*

Proof. Suppose $S = \{i_1, i_2, \ldots, i_k\}$ and $\mathrm{von}(S) = \varnothing$. Then

$$A_{i_1} + A_{i_2} + \cdots + A_{i_k} \equiv 0 \pmod 2$$

which implies columns $A_{i_1}, A_{i_2}, \ldots, A_{i_k}$ of A are linearly dependent.

Conversely, suppose $S = \{1, 2, \ldots, k\}$ and $A_1, A_2, \ldots, A_k$ are minimally linearly dependent. Then $A_1 + A_2 + \cdots + A_k \equiv 0 \pmod 2$. If $i \in \mathrm{von}(S)$, then

$$(A_1 + A_2 + \cdots + A_k)_i \equiv 1 \pmod 2,$$

a contradiction. Thus $\mathrm{von}(S) = \varnothing$. □

Corollary 2. *Let Γ be a graph with vertex set V and adjacency matrix A. Let S be a nonempty subset of V. The columns of A corresponding to S are minimally linearly dependent if and only if one of the following is true:*

(a) *S consists of a single isolated vertex of Γ.*
(b) *$\mathrm{von}(S \setminus \{i\}) = \mathrm{N}(i)$ for each $i \in S$ and there is no proper subset S' of S for which $\mathrm{von}(S' \setminus \{i\}) = \mathrm{N}(i)$ for each $i \in S'$.*

Now we discuss linear dependence among columns of $[A|I_n]$ where A is the adjacency matrix of a graph Γ on n vertices.

Theorem 8. *Let Γ be a graph on n vertices with vertex set V and adjacency matrix A. If S is a nonempty subset of V, then the columns of A indexed by S and the columns of I_n indexed by $\mathrm{von}(S)$ are $(|S| + |\mathrm{von}(S)|)$ linearly dependent columns of $[A|I_n]$. Conversely, if the set of columns of $[A|I_n]$ indexed by the set $S' \subseteq \{1, 2, \ldots, 2n\}$ is minimally linearly dependent, then it is the union of the columns of A indexed by S and the columns of I_n indexed by $\mathrm{von}(S)$ for some nonempty subset S of V, in other words $S' = S \cup \{n + i \mid i \in \mathrm{von}(S)\}$.*

Proof. Let $\varnothing \neq S \subseteq V$. Let c be the sum of columns of A indexed by S. Then c_i, the ith entry of c, is the number of vertices of S adjacent to vertex i. Therefore if vertex i is adjacent to an even number of vertices in S, then $c_i \equiv 0 \pmod 2$. Similarly if vertex i is adjacent to an odd number of vertices in S, then $c_i \equiv 1 \pmod 2$. Thus the only entries of c that are

$1 \pmod 2$ correspond to $\mathrm{von}(S)$. So if we add c with the columns of I_n with indices corresponding to $\mathrm{von}(S)$, the sum would be a zero vector.

Conversely, suppose the set of d columns of $[A|I_n]$ indexed by the set $S' \subseteq \{1, 2, \ldots, 2n\}$ is minimally linearly dependent. Without loss of generality suppose S' is the union of $S = \{1, 2, \ldots, k\}$, $k \leqslant n$ and $T \subseteq \{n+1, n+2, \ldots, 2n\}$.

Case 1. $T = \varnothing$ (i.e., $S' = S$)
Since $A_1, A_2, \ldots, A_k$ are minimally linearly dependent, $A_1 + A_2 + \cdots + A_k \equiv 0 \pmod 2$. It suffices to show that $\mathrm{von}(S) = \varnothing$. If not, let $i \in \mathrm{von}(S)$. Then

$$(A_1 + A_2 + \cdots + A_k)_i \equiv 1 \pmod 2\,,$$

a contradiction.

Case 2. $T \neq \varnothing$
Let $T = \{n + i_1, n + i_2, \ldots, n + i_{d-k}\}$ and e_j be column j of I_n for $j = i_1, i_2, \ldots, i_{d-k}$. Since $A_1, A_2, \ldots, A_k, e_{i_1}, e_{i_2}, \ldots, e_{i_{d-k}}$ are minimally linearly dependent,

$$A_1 + A_2 + \cdots + A_k + e_{i_2} + \cdots + e_{i_{d-k}} \equiv 0 \pmod 2\,.$$

Then

$$A_1 + A_2 + \cdots + A_k \equiv e_{i_1} + e_{i_2} + \cdots + e_{i_{d-k}} \pmod 2$$

which implies $\mathrm{von}(S) = \{i_1, i_2, \ldots, i_{d-k}\}$ because $e_{i_1}, e_{i_2}, \ldots, e_{i_{d-k}}$ are columns of I_n. Thus $S' = S \cup \{n + i \mid i \in \mathrm{von}(S)\}$. □

As a consequence of the preceding theorem, we have the following result.

Theorem 9. *Let A be the adjacency matrix of a graph Γ on n vertices with vertex set V. Let C be the binary linear code generated by $[I_n|A]$. Then the minimum distance $d(C)$ of C is given by*

$$d(C) = \min_{\varnothing \neq S \subseteq V} (|S| + |\mathrm{von}(S)|).$$

Proof. First note that $H = [A|I_n]$ is the parity-check matrix of C. By Theorem 8, a codeword in C with weight $d(C)$ corresponds to minimally dependent columns of $H = [A|I_n]$ indexed by $S \cup \{n + i \mid i \in \mathrm{von}(S)\}$ for some nonempty subset S of V. Then

$$d(C) \geqslant \min_{\varnothing \neq S \subseteq V} (|S| + |\mathrm{von}(S)|).$$

If there is a nonempty subset S of V for which $d(C) > |S| + |\operatorname{von}(S)|$, then by Theorem 8 we find $(|S| + |\operatorname{von}(S)|)$ linearly dependent columns of $H = [A|I_n]$ giving a codeword of C with weight less than $d(C)$, a contradiction. Thus the equality holds. □

Corollary 3. *Let A be the adjacency matrix of a graph Γ on n vertices. Let P be an $n \times n$ permutation matrix. Then the binary linear codes generated by $[I_n|A]$ and $[I_n|PAP^T]$ are not necessarily the same but they have the same minimum distance.*

Proof. The graph with adjacency matrix PAP^T is isomorphic to Γ. Then the binary linear codes generated by $[I_n|A]$ and $[I_n|PAP^T]$ have the same minimum distance by Theorem 9. □

By Theorem 5 and Theorem 9, we have the following lower bound of the 2-rank of a graph:

Corollary 4. *Let A be the adjacency matrix of a graph Γ with vertex set V. Then*

$$-1 + \min_{\varnothing \neq S \subseteq V} (|S| + |\operatorname{von}(S)|) \leqslant rk_2(A).$$

Question 10. Characterize the graphs Γ with the adjacency matrix A and the vertex set V for which

$$rk_2(A) = -1 + \min_{\varnothing \neq S \subseteq V} (|S| + |\operatorname{von}(S)|).$$

Example 2. The following are examples of binary linear code C generated by $[I_n|A]$ where A is the adjacency matrix of a graph Γ on n vertices.

1) For $\Gamma = P_n,\ n \geqslant 2$, $d(C) = 2 = |S| + |\operatorname{von}(S)|$ where $S = \{1\}$ and $\operatorname{von}(S) = \{2\}$.
   For $\Gamma = P_1$, $d(C) = 1 = |S| + |\operatorname{von}(S)|$ where $S = \{1\}$ and $\operatorname{von}(S) = \varnothing$.
2) When Γ is a tree on $n \geqslant 2$ vertices, $d(C) = 2 = |S| + |\operatorname{von}(S)|$ where $S = \{v\}$ consisting of a pendant vertex v and $\operatorname{von}(S) = \{w\}$ where w is adjacent to v.
3) For $\Gamma = C_n,\ n \geqslant 5$, $d(C) = 3 = |S| + |\operatorname{von}(S)|$ where $S = \{1\}$ and $\operatorname{von}(S) = \{2, n\}$.
   For $\Gamma = C_4$, $d(C) = 2 = |S| + |\operatorname{von}(S)|$ where $S = \{1, 3\}$ and $\operatorname{von}(S) = \varnothing$.
   For $\Gamma = C_3$, $d(C) = 3 = |S| + |\operatorname{von}(S)|$ where $S = \{1\}$ and $\operatorname{von}(S) = \{2, 3\}$.

4) For $\Gamma = K_n,\ n \geqslant 4$, $d(C) = 4 = |S| + |\operatorname{von}(S)|$ where $S = \{1, 2\}$ and $\operatorname{von}(S) = \{1, 2\}$.
5) For star $\Gamma = K_{1,n},\ n \geqslant 1$ centered at 1, $d(C) = 2 = |S| + |\operatorname{von}(S)|$ where $S = \{2\}$ and $\operatorname{von}(S) = \{1\}$.
6) For $\Gamma = K_{m,n},\ m$ or $n \geqslant 2$, $d(C) = 2 = |S| + |\operatorname{von}(S)|$ where $S = \{1, 2\}$ and $\operatorname{von}(S) = \varnothing$ because of duplicate vertices 1 and 2. Recall $C_4 = K_{2,2}$.
7) For $G = W_n = K_1 \vee C_{n-1},\ n \geqslant 6$ centered at 1, $d(C) = 4 = |S| + |\operatorname{von}(S)|$ where $S = \{2\}$ and $\operatorname{von}(S) = \{1, 3, n\}$.
   For $\Gamma = W_5$, $d(C) = 2 = |S| + |\operatorname{von}(S)|$ where $S = \{2, 4\}$ and $\operatorname{von}(S) = \varnothing$.
   For $\Gamma = W_4$, $d(C) = 4 = |S| + |\operatorname{von}(S)|$ where $S = \{1\}$ and $\operatorname{von}(S) = \{2, 3, 4\}$.
8) When Γ is the Petersen graph which is the $srg(10, 3, 0, 1)$, $d(C) = 4 = |S| + |\operatorname{von}(S)|$ where $S = \{1\}$ and $\operatorname{von}(S) = \mathrm{N}(1) = \{2, 5, 6\}$ where the outer vertices are 1,2,3,4 in the standard drawing.

Remark 1. Suppose V is the vertex set of K_n and let $S \subseteq V$. It is easy to observe that

$$\operatorname{von}(S) = \begin{cases} S & \text{if } |S| \text{ is even} \\ V \setminus S & \text{if } |S| \text{ is odd.} \end{cases}$$

Observation 11. Let A be the adjacency matrix of a graph Γ on n vertices with vertex set V. Let C be the binary linear code generated by $[I_n|A]$ and S be a nonempty subset of V for which $d(C) = |S| + |\operatorname{von}(S)|$. From the preceding remark for K_n, we have either $S = \operatorname{von}(S)$ or $S \cap \operatorname{von}(S) = \varnothing$. At least one of these two properties seems to hold for other graphs also.

Conjecture 12. Let A be the adjacency matrix of a graph Γ on n vertices with vertex set V. Let C be the binary linear code generated by $[I_n|A]$. Suppose S is a nonempty subset of V for which $d(C) = |S| + |\operatorname{von}(S)|$. Then either $S = \operatorname{von}(S)$ or $S \cap \operatorname{von}(S) = \varnothing$.

The following observation may be helpful for the future work on the preceding conjecture.

Observation 13. If $v \in S \cap \operatorname{von}(S)$ and $|S| \geqslant 2$, then

$$\operatorname{von}(S \backslash \{v\}) \backslash \mathrm{N}(v) = \operatorname{von}(S) \backslash \mathrm{N}(v) \text{ and } \operatorname{von}(S \backslash \{v\}) \cap \operatorname{von}(S) \cap \mathrm{N}(v) = \varnothing.$$

3. Self-dual codes from graphs

We start by observing that if A is an $n \times n$ matrix, then the binary code generated by $[I_n|A]$ is a self-dual code if and only if $AA^T = I_n$, where the matrix multiplication is done in $\mathbb{F}_2$. If A is the adjacency matrix of a simple graph, then this condition is reduced to $A^2 \equiv I_n \pmod 2$. We first give some results on the graphs for which this condition is satisfied.

Theorem 14. *Let Γ be a graph on n vertices $1, 2, \ldots, n$ with adjacency matrix A. Then $A^2 \equiv I_n \pmod 2$ if and only if the following are true:*
(a) $\deg(i)$ *is odd for all vertices $i = 1, 2, \ldots, n$ (This implies n is even).*
(b) $|N(i) \cap N(j)|$ *is even for all vertices $i \neq j$.*

Proof. Suppose $A^2 \equiv I_n \pmod 2$. Then for all $i = 1, 2, \ldots, n$, $\sum_{k=1}^{n} a_{ik}^2 \equiv 1 \pmod 2$, i.e., $\sum_{k=1}^{n} a_{ik}^2$ is odd and consequently $\deg(i)$ is odd. Since every graph has an even number of odd-degree vertices, n is even by (a). Since $A^2 \equiv I_n \pmod 2$, for all vertices $i \neq j$, $\sum_{k=1}^{n} a_{ik}a_{jk}$ is even and consequently $|N(i) \cap N(j)|$ is even. The converse follows by similar arguments. □

We prove the following lemma which will be used in the proof of the subsequent theorem:

Lemma 1. *Let C be a self-orthogonal code and assume $\boldsymbol{c}_1, \boldsymbol{c}_2$ are two codewords with*

$$w(\boldsymbol{c}_1) \equiv w(\boldsymbol{c}_2) \equiv 0 \pmod 4.$$

Then $w(\boldsymbol{c}_1 + \boldsymbol{c}_2) \equiv 0 \pmod 4$.

Proof. Since C is self-orthogonal, we have $\langle \boldsymbol{c}_1, \boldsymbol{c}_2 \rangle = 0$, which implies the weight $w(\boldsymbol{c}_1 \circ \boldsymbol{c}_2)$ of the entry-wise product $\boldsymbol{c}_1 \circ \boldsymbol{c}_2$ of $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ is even. Thus we have

$$w(\boldsymbol{c}_1 + \boldsymbol{c}_2) = w(\boldsymbol{c}_1) + w(\boldsymbol{c}_2) - 2w(\boldsymbol{c}_1 \circ \boldsymbol{c}_2) \equiv 0 \pmod 4.$$

□

We are now ready to prove the following theorem which gives a necessary and sufficient condition for a graph to generate a Type II code:

Theorem 15. *Let A be the adjacency matrix of a simple graph on n vertices, which satisfies the hypothesis of Theorem 14. Then $[I_n|A]$ generates a Type II code if and only if $\deg(v) \equiv 3 \pmod 4$ for all vertices v of the graph.*

Proof. The necessity being clear, we proceed to proving the sufficiency.

Suppose $\deg(v) \equiv 3 \pmod 4$ for all vertices v. Then each row of $G = [I_n|A]$ has weight divisible by 4. Suppose the rows of G are denoted by $\boldsymbol{r}_1, \boldsymbol{r}_2, \ldots, \boldsymbol{r}_n$. So we have $w(\boldsymbol{r}_i) \equiv 0 \pmod 4$ for $i = 1, 2, \ldots, n$. Then we claim that all the codewords will have weight divisible by 4. Note that every codeword of $C([I_n|A])$ is obtained from a sum of the form $\boldsymbol{r}_{i_1} + \boldsymbol{r}_{i_2} + \cdots + \boldsymbol{r}_{i_k}$, where $1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n$ and $k \geqslant 1$. We proceed by induction on k.

If $k = 1$, then we have just the rows $\boldsymbol{r}_i$, which all have weights divisible by 4.

Assume the assertion to be true for all sums with $k \geqslant 1$ summands.

Let

$$\boldsymbol{c} = \boldsymbol{r}_{i_1} + \boldsymbol{r}_{i_2} + \cdots + \boldsymbol{r}_{i_k} + \boldsymbol{r}_{i_{k+1}} = (\boldsymbol{r}_{i_1} + \boldsymbol{r}_{i_2} + \cdots + \boldsymbol{r}_{i_k}) + \boldsymbol{r}_{i_{k+1}}.$$

By induction hypothesis, $(\boldsymbol{r}_{i_1} + \boldsymbol{r}_{i_2} + \cdots + \boldsymbol{r}_{i_k})$ has weight divisible by 4. Note that both $(\boldsymbol{r}_{i_1} + \boldsymbol{r}_{i_2} + \cdots + \boldsymbol{r}_{i_k})$ and $\boldsymbol{r}_{i_{k+1}}$ are codewords in C, which is self-dual and both codewords have weights divisible by 4. So by Lemma 1, the weight of c is divisible by 4. □

Since Type II binary self-dual codes only exist for lengths that are multiple of 8, we have the following combinatorial result as a consequence of the previous theorem:

Corollary 5. *Let $n \equiv 2 \pmod 4$. Then a simple graph on n vertices that satisfies the hypotheses of Theorem 14 has at least one vertex whose degree is $1 \pmod 4$.*

In the following theorem, we explore the special case of complete graphs.

Theorem 16. *Let C be the code generated by $[I_n|A]$, where A is the adjacency matrix of K_n. C is a self-dual code if and only if n is even. Moreover, if $n \geqslant 4$ we have*

a) *C is a Type II self-dual code of parameters $[2n, n, 4]$ if n is divisible by 4.*

b) *C is a Type I self-dual code of parameters $[2n, n, 4]$ if n is not divisible by 4.*

Proof. By Theorem 14, C is self-dual if and only if n is even.

a) If $n = 4k$, then the degree of every vertex of K_n is $4k - 1$, which, by Theorem 15, implies that the code generated by $[I_n|A]$ is Type II. This means $d(C) \geqslant 4$. But the sum of any two rows of $[I_n|A]$ has weight 4, which means $d(C) = 4$.

b) If $n = 4k+2$ with $k \geqslant 1$, then every row of $[I_n|A]$ has weight $4k+2$, which makes C Type I. To find the minimum distance, we use Theorem 9. Let S be a nonempty subset of the vertices of K_n. If $S = \{x\}$, then $|\operatorname{von}(S)| = n-1$, which means $|S| + |\operatorname{von}(S)| = n \geqslant 4$.

If $S = \{x, y\}$, then $\operatorname{von}(S) = S$, which means $|S| + |\operatorname{von}(S)| = 4$.

If $S = \{x, y, z\}$, then $|\operatorname{von}(S)| = n-3$, which means $|S| + |\operatorname{von}(S)| = n \geqslant 4$.

If $|S| \geqslant 4$, then $|S| + |\operatorname{von}(S)| \geqslant 4$. Thus the minimum distance is 4. □

Corollary 6. *The code generated by K_n is an extremal Type II self-dual code for $n = 4$ and $n = 8$. The code generated by K_n is an extremal Type I self-dual code for $n = 6$.*

Example 3. Consider the regular graph $\Gamma = 2K_4$ which is the strongly regular graph $srg(8, 3, 2, 0)$ with the following adjacency matrix A. Since $A^2 \equiv I_8 \pmod 2$ and each vertex of Γ has degree 3, the binary code $C = C([I_8|A])$ is an extremal Type II self-dual $[16, 8, 4]$ code by Theorems 14, 15, and 1.

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

Theorem 17. *Let Γ be a strongly regular graph with parameters (n, k, λ, μ) and adjacency matrix A. Suppose C is a linear code generated by $[I_n|A]$. Then C is self-dual if and only if k is odd and n, λ, μ are even.*

Proof. For a strongly regular graph with parameters (n, k, λ, μ), $\deg(i) = k$ for all $i = 1, 2, \ldots, n$ and $|N(i) \cap N(j)|$ is λ or μ for all $i \neq j$. Thus $A^2 \equiv I_n \pmod 2$ if and only if k is odd and λ, μ are even by Theorem 14. □

Question 18. Let Γ be a strongly regular graph with parameters (n, k, λ, μ) and adjacency matrix A. Find the minimum distance of the linear code $C([I_n|A])$ in terms of n, k, λ, μ.

Now we explore effects of graph operations on corresponding linear codes. In particular, we study the join $\Gamma_1 \vee \Gamma_2$ of two graphs Γ_1 and Γ_2 with disjoint vertex sets V_1 and V_2 respectively. Note that $\Gamma_1 \vee \Gamma_2$ has the vertex set $V_1 \cup V_2$ and the edge set consisting of all edges of Γ_1 and Γ_2 together with all edges between them. For example, $K_{m,n}$ is the join of mK_1 and nK_1.

Theorem 19. *Let Γ_1 and Γ_2 be two graphs on n_1 and n_2 vertices with adjacency matrices A_1 and A_2 respectively. Suppose $\Gamma_1 \vee \Gamma_2$ is the join of Γ_1 and Γ_2 with adjacency matrix A. If $C([I_{n_1}|A_1])$ and $C([I_{n_2}|A_2])$ are self-dual codes, then so is $C([I_{n_1+n_2}|A])$.*

Proof. First note that

$$A = \begin{bmatrix} A_1 & J_{n_1,n_2} \\ J_{n_2,n_1} & A_2 \end{bmatrix}$$

and

$$A^2 = \begin{bmatrix} n_2 J_{n_1,n_1} + A_1^2 & A_1 J_{n_1,n_2} + J_{n_1,n_2} A_2 \\ J_{n_2,n_1} A_1 + A_2 J_{n_2,n_1} & n_1 J_{n_2,n_2} + A_2^2 \end{bmatrix}.$$

Suppose $C([I_{n_1}|A_1])$ and $C([I_{n_2}|A_2])$ are self-dual codes. By Theorem 14, $A_1^2 \equiv I_{n_1} \pmod 2$ and $A_2^2 \equiv I_{n_2} \pmod 2$ which imply $n_1 \equiv n_2 \equiv 0 \pmod 2$ and degree of each vertex in Γ_1 and Γ_2 is $1 \pmod 2$. Then

$$A_1 J_{n_1,n_2} + J_{n_1,n_2} A_2 \equiv J_{n_1,n_2} + J_{n_1,n_2} \equiv O_{n_1,n_2} \pmod 2,$$

$$J_{n_2,n_1} A_1 + A_2 J_{n_2,n_1} \equiv J_{n_2,n_1} + J_{n_2,n_1} \equiv O_{n_2,n_1} \pmod 2.$$

$$\begin{aligned} A^2 &= \begin{bmatrix} n_2 J_{n_1,n_1} + A_1^2 & A_1 J_{n_1,n_2} + J_{n_1,n_2} A_2 \\ J_{n_2,n_1} A_1 + A_2 J_{n_2,n_1} & n_1 J_{n_2,n_2} + A_2^2 \end{bmatrix} \\ &\equiv I_{n_1+n_2} \pmod 2. \end{aligned}$$

Thus $C([I_{n_1+n_2}|A])$ is a self-dual code by Theorem 14. □

The following theorem describes the type of the join of self-dual codes.

Theorem 20. *Let Γ_1 and Γ_2 be two graphs on n_1 and n_2 vertices and with generator matrices A_1 and A_2 respectively. Suppose that A is the generator matrix of $\Gamma_1 \vee \Gamma_2$.*

(a) *When $n_1 \equiv n_2 \equiv 0 \pmod 4$, $C([I_{n_1+n_2}|A])$ is Type II if and only if both $C([I_{n_1}|A_1])$ and $C([I_{n_2}|A_2])$ are Type II.*

(b) *When* $n_1 \equiv n_2 \equiv 2 \pmod 4$, *if* $C([I_{n_1+n_2}|A])$ *is Type II, then both* $C([I_{n_1}|A_1])$ *and* $C([I_{n_2}|A_2])$ *are Type I and the converse is true if each vertex of* Γ_1 *and* Γ_2 *has degree* $1 \pmod 4$.

(c) *If exactly one of* n_1 *and* n_2 *is divisible by* 4, *then* $C([I_{n_1+n_2}|A])$ *is Type I.*

Proof. First we observe that for any vertex v in Γ_1, the degree of v in $\Gamma_1 \vee \Gamma_2$ is $n_2 + deg(v)$. Similarly for any vertex w in Γ_2, the degree of w in $\Gamma_1 \vee \Gamma_2$ is $n_1 + deg(w)$. Then the cases $n_1 \equiv n_2 \equiv 0 \pmod 4$ and $n_1 \equiv n_2 \equiv 2 \pmod 4$ follow from Theorem 15.

Now consider the case when exactly one of n_1 and n_2 is divisible by 4. Then we have $n_1 + n_2 \equiv 2 \pmod 4$, which implies $2(n_1 + n_2) \equiv 4 \pmod 8$. Since Type II codes only exist for lengths that are multiples of 8, $C([I_{n_1+n_2}|A])$ is not Type II, hence Type I. □

We end by the following results about the minimum distance of $C([I_{n_1+n_2}|A])$ and its connection to the minimum distances of $C([I_{n_1}|A_1])$ and $C([I_{n_2}|A_2])$.

Theorem 21. *Let* Γ_1 *and* Γ_2 *be two graphs with disjoint vertex sets* V_1 *and* V_2 *of sizes* n_1 *and* n_2 *respectively. Let* A_1, A_2, *and* A *be the adjacency matrices of* Γ_1, Γ_2, *and* $\Gamma_1 \vee \Gamma_2$ *respectively. Suppose that* d_1, d_2, *and* d *are the minimum distances of the codes generated by* $[I_{n_1}|A_1]$, $[I_{n_2}|A_2]$, *and* $[I_{n_1+n_2}|A]$ *respectively.*

(a) *Suppose* S_i *is a nonempty subset of* V_i *for which* $d_i = |S_i| + |\operatorname{von}(S_i)|$ *for* $i = 1, 2$. *If* $|S_i|$ *is even for some* $i = 1, 2$, *then*

$$d \leqslant d_i.$$

If $|S_1|$ *and* $|S_2|$ *are odd, then*

$$d \leqslant \min\{n_2 + d_1, n_1 + d_2\}.$$

(b) *Suppose* $S = S_1 \cup S_2$ *is a nonempty subset of* $V_1 \cup V_2$ *for which* $d = |S| + |\operatorname{von}(S)|$ *where* $\varnothing \neq S_1 \subseteq V_1$ *and* $\varnothing \neq S_2 \subseteq V_2$. *If at least one of* $|S_1|$ *and* $|S_2|$ *is even, then*

$$d_1 + d_2 \leqslant d.$$

Proof. (a) We prove this by the following cases:
Case 1. $|S_1|$ is even.
For $S = S_1 \subseteq V_1 \cup V_2$ in $\Gamma_1 \vee \Gamma_2$, we have $\operatorname{von}(S) = \operatorname{von}(S_1)$ in Γ_1. Then by Theorem 9,

$$d \leqslant |S_1| + |\operatorname{von}(S_1)| = d_1.$$

Case 2. $|S_2|$ is even.
For $S = S_2 \subseteq V_1 \cup V_2$ in $\Gamma_1 \vee \Gamma_2$, we have $\mathrm{von}(S) = \mathrm{von}(S_2)$ in Γ_2. Then by Theorem 9,

$$d \leqslant |S_2| + |\,\mathrm{von}(S_2)| = d_2.$$

Case 3. $|S_1|$ and $|S_2|$ are odd.
In $\Gamma_1 \vee \Gamma_2$, let $S = S_1$. Thus $\mathrm{von}(S) = \mathrm{von}(S_1) \cup V_2$. Then by Theorem 9,

$$d \leqslant |S_1| + |\,\mathrm{von}(S_1)| + |V_2| = n_2 + d_1.$$

Similarly

$$d \leqslant |S_2| + |\,\mathrm{von}(S_2)| + |V_1| = n_1 + d_2.$$

(b) We prove this by the following cases:
Case 1. $|S_1|$ and $|S_2|$ are even.
$\mathrm{von}(S)$ is the union of $\mathrm{von}(S_1)$ in Γ_1 and $\mathrm{von}(S_2)$ in Γ_2. Then by Theorem 9,

$$d_1 + d_2 \leqslant |S_1| + |S_2| + |\,\mathrm{von}(S_1)| + |\,\mathrm{von}(S_2)| = d.$$

Case 2. $|S_1|$ is odd and $|S_2|$ is even.
$\mathrm{von}(S)$ is the union of V_2 and $\mathrm{von}(S_1)$ in Γ_1. Then by Theorem 9,

$$d_1 + d_2 \leqslant |S_1| + |S_2| + |\,\mathrm{von}(S_1)| + |V_2| = d.$$

Case 3. $|S_1|$ is even and $|S_2|$ is odd.
Similar to Case 2, we have

$$d_1 + d_2 \leqslant d.$$ □

References

[1] A. Abiad, W. H. Haemers, "Switched symplectic graphs and their 2-ranks", *Des. Codes Crypt.*, vol. 81, no. 1, pp. 35–41, 2016.

[2] D. Crnković, B.G. Rodrigues, S. Rukavina and L. Simčić, "Ternary codes from the strongly regular (45, 12, 3, 3) graphs and orbit matrices of 2-(45, 12, 3) designs", *Discrete Math.*, vol. 312, no. 20, pp. 3000–3010, 2012.

[3] D. Crnković, M. Maximović, B. Rodrigues and S. Rukavina, "Self-orthogonal codes from the strongly regular graphs on up to 40 vertices", *Adv. Math. Communications*, vol. 10, no. 3, pp. 555–582, 2016.

[4] P. Dankelmann, J.D. Key and B. G. Rodrigues, "A Characterization of Graphs by Codes from their Incidence Matrices", *Elect. J. Combinatorics*, vol. 20, no. 3, P18, 2013.

[5] W. Fish, R. Fray and E. Mwambene, "Binary codes from the complements of the triangular graphs", *Quaestiones Mathematicae*, vol. 33, no. 4, pp. 399–408, 2010.

[6] G. D. Forney, “Codes on Graphs: Fundamentals", arXiv:1306.6264

[7] C. D. Godsil and G. F. Royle, “Chromatic Number and the 2-Rank of a Graph ", *J. Comb. Series B*, vol. 81, pp. 142–149, 2001.

[8] M. Grassl and M. Harada, “New self-dual additive $\mathbb{F}_4$-codes constructed from circulant graphs", *Discrete Math.*, vol. 340, no. 3, pp.399–403, 2017.

[9] J.D. Key and B.G. Rodrigues, “LCD codes from adjacency matrices of graphs", *Appl. Alg. Eng. Comm. Comp.*, vol. 29, no. 3, pp.227–244, 2018.

[10] K. Kumwenda and E. Mwambene, “Codes from graphs related to the categorical product of triangular graphs and K_n", *IEEE Trans. Inform. Theory Workshop*, ITW 2010 Dublin.

[11] S. Mallik and B. L. Shader, “Classes of graphs with minimum skew rank 4", *Linear Algebra Appl.* 439 (2013) 3643–3657.

[12] H. Oral, “Self-dual Codes and Graphs", **Thesis**, Simon Frasier University, 1989.

[13] E.M. Rains, “Shadow Bounds for Self Dual Codes", *IEEE Trans. Inf. Theory*, vol.44, pp.134–139, 1998.

[14] V. Tonchev, “Error-correcting codes from graphs", *Discrete Math.*, vol. 257, no. 2-3, pp.549–557, 2002.

[15] V. Tonchev, “Rank-3 Graphs, Block Designs, and Codes with Unequal Symbol Protection", *Problemy Peredaci Informatsii*, vol. 17, no. 2, pp.89–93, 1981.

Contact information

Sudipta Mallik
Department of Mathematics and Statistics,
Northern Arizona University,
801 S. Osborne Dr. PO Box: 5717, Flagstaff,
AZ 86011, USA
E-Mail(s): sudipta.mallik@nau.edu
Web-page(s): http://oak.ucc.nau.edu/sm2825/

Bahattin Yildiz
Department of Mathematics and Statistics,
Northern Arizona University,
801 S. Osborne Dr. PO Box: 5717, Flagstaff,
AZ 86011, USA
E-Mail(s): bahattin.yildiz@nau.edu
Web-page(s): profile.directory.nau.edu/person/by96

Received by the editors: 17.06.2020
and in final form 24.02.2021.