AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **79(3)** (2021), Pages 515–526

Graph theoretic aspects of minimum distance and equivalence of binary linear codes

Sudipta Mallik Bahattin Yildiz

Department of Mathematics and Statistics
Northern Arizona University
801 S. Osborne Dr.
PO Box: 5717, Flagstaff, AZ 86011
U.S.A.

sudipta.mallik@nau.edu bahattin.yildiz@nau.edu

Abstract

A binary linear $[2n, n]$-code with generator matrix $[I_n|A]$ can be associated with a digraph on n vertices with adjacency matrix A and vice versa. We use this connection to present a graph theoretic formula for the minimum distance of codes with information rate 1/2. We also formulate the equivalence of such codes via new transformations on corresponding digraphs.

1 Introduction

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. 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.

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. A matrix H is called a *parity check matrix* for the linear code C if it is given by

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

We can find a parity check matrix for C in the standard form if we know the generator matrix in the standard form:

ISSN: 2202-3518

Theorem 1.1. *If C is generated by $G = [I_k|A]$, then $H = [-A^T|I_k]$ is a parity check matrix of C.*

Note that over the binary field, $H = [-A^T|I_k] = [A^T|I_k]$.

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

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

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

Corollary 1.3. *[10, Theorem 2.2] 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.*

There is a natural interplay between graphs and codes and this connection has been explored extensively in the literature. For some of these works, we refer to ([1–6]) and references therein. In most of these works, the code is obtained from the graph by taking the adjacency matrix as the generator matrix. Recently in [7], the idea of generating the code from $[I_n|A]$, where A is the adjacency matrix of a simple undirected graph was explored. In this work, we consider combinatorial approaches to two classical problems in coding theory, namely the minimum distance problem and the equivalence problem, using digraphs and their transformations. Determining the minimum distance of a code is considered computationally intractable ([12]), so it takes significant time to find the minimum distance of a single code when the dimension is large.

Two codes over $\mathbb{F}_q$ are said to be equivalent if one can be obtained from the other by a permutation of columns or by multiplying a column by a fixed non-zero element in $\mathbb{F}_q$. In other words two codes are equivalent if one can be obtained from the other through a monomial transformation. If $q = 2$, code equivalence for binary codes reduces to permutation equivalence. Equivalent codes have the same parameters and share many of the same properties such as self-duality, cyclicity, etc. Code equivalence also plays an important role in cryptographic applications of codes, such as the McEliece Cryptosystem. However, determining code equivalence is considered to be a difficult problem in coding theory. For some works that explore this aspect, we refer to [9] and [11].

In this paper, we consider a special class of codes, namely rate 1/2 codes that include some important classes of codes such as isodual codes, formally self-dual codes, self-dual codes and 2-quasicyclic codes. Another important aspect of these codes is that we can construct them from digraphs. This is because the generator matrix of any such code, which has parameters $[2n, n]$ for some n, can be put into the standard form of $[I_n|A]$, where I_n is the identity matrix and A is an $n \times n$ binary matrix. We can then view A as the adjacency matrix of a digraph on n vertices. Using this connection, we have been able to give purely graph theoretic descriptions for the minimum distance of such codes and we have also been able to describe code equivalence in terms of graph theoretic properties. Moreover, new transformations on

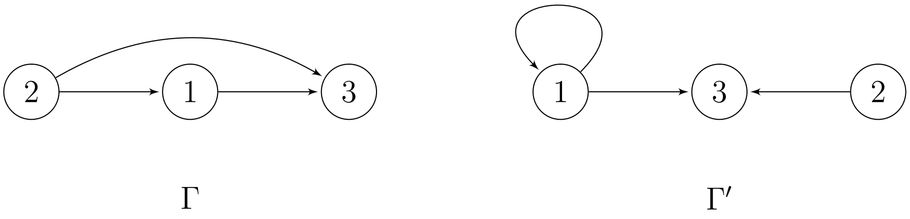

Figure 1: Directed graphs Γ and Γ′

digraphs have been explored in an effort to preserve the equivalence of the underlying code. This has resulted in some surprising results about equivalence of codes that are otherwise difficult to verify. For example, we were able to prove that if A is a non-singular $n \times n$ matrix, then the codes generated by $[I_n|A]$ and $[I_n|A^{-1}]$ are equivalent.

2 The $[I_n|A]$ Construction for Codes from Directed Graphs

A binary linear code generated by $[I_n|A]$ corresponds to a directed graph Γ on n vertices that has A as the adjacency matrix. Note that Γ may have loops but no multiple arcs (directed edges). Conversely a directed graph Γ on n vertices with adjacency matrix A and possibly with loops corresponds to a binary linear code generated by $[I_n|A]$.

Observation 2.1. Linear codes generated by $[I_n|A]$ and $[I_n|P^TA]$ are not necessarily the same for some permutation matrix P. For example, consider Γ in Figure 1 with adjacency matrix A and permutation matrix P generated by $(1, 2)$:

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

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

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

Note that AP is obtained from A by interchanging columns 1 and 2 which guarantees that $C([I_3|A])$ and $C([I_3|AP])$ are equivalent. But it may not be clear whether $C([I_3|A])$ and $C([I_3|P^TA])$ are equivalent or they have the same minimum distances. We develop combinatorial tools in this section and Section 3 that answer this.

Consider the directed graph $\Gamma = (V, A)$ with vertex set V and arc set A. For a vertex $v \in V$, an *out-neighbor* of v is a vertex $u \in V$ such that (v, u) is an arc in Γ.

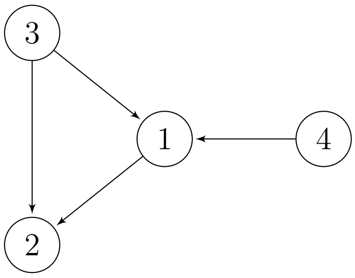

Figure 2: A directed paw

The set of out-neighbors of v, denoted by $N^+(v)$, is given by

$$N^+(v) = \{u \in V \mid (v,u) \in A\}.$$

An *in-neighbor* of v is a vertex $u \in V$ such that (u,v) is an arc in Γ. The set of in-neighbors of v, denoted by $N^-(v)$, is given by

$$N^-(v) = \{u \in V \mid (u,v) \in A\}.$$

The *out-degree* and *in-degree* of v, denoted by $d^+(v)$ and $d^-(v)$, are defined by $d^+(v) = |N^+(v)|$ and $d^-(v) = |N^-(v)|$ respectively.

To get a combinatorial interpretation of the minimum distance of $C([I_n|A])$, we study the following set of vertices of a directed 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 in-neighbors in S is denoted by $\operatorname{vonin}(S)$, i.e.,

$$\operatorname{vonin}(S) = \{v \in V \ : \ |\,\mathrm{N}^-(v) \cap S| \text{ is odd}\}.$$

The concept and notation of vonin are motivated by that of von introduced in [7] and used in [8] to find the minimum distance of an expander code. Note that S and $\operatorname{vonin}(S)$ have no inclusion-exclusion relationship that holds for all graphs as evident in the following examples.

Example 2.2.

1. Consider the directed paw in Figure 2. For S equals $\{1\}, \{3\}, \{1,2\}, \{1,2,3\}$, and $\{1,3,4\}$, we have $\operatorname{vonin}(S)$ is $\{2\}, \{1,2\}, \{2\}, \{1\}$, and $\varnothing$ respectively.

2. Note that in a directed graph, if a vertex v has $\mathrm{N}^-(v) = \varnothing$, then $v \notin \operatorname{vonin}(S)$ for all S. Also if $S = \{v\}$, then $\operatorname{vonin}(S) = \mathrm{N}^+(v)$.

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

Theorem 2.3. *Let Γ be a digraph on n vertices with vertex set V and adjacency matrix A. If S is a nonempty subset of V, then the columns of A^T indexed by S and the columns of I_n indexed by* $\operatorname{vonin}(S)$ *are* $(|S| + |\operatorname{vonin}(S)|)$ *linearly dependent columns of $[A^T|I_n]$. Conversely if the set of columns of $[A^T|I_n]$ indexed by the set $S' \subseteq \{1,2,\ldots,2n\}$ is minimally linearly dependent, then it is the union of the columns of A^T indexed by S and the columns of I_n indexed by* $\operatorname{vonin}(S)$ *for some nonempty subset S of V, in other words $S' = S \cup \{n+i \mid i \in \operatorname{vonin}(S)\}$.*

Proof. Let $\varnothing \neq S \subseteq V$. Let c be the sum of columns of A^T indexed by S. Then c_i, the ith entry of c, is the number vertices of S that are in-neighbors of vertex i. Therefore if vertex i has an even number of in-neighbors in S, then $c_i \equiv 0 \,(\text{mod } 2)$. Similarly if vertex i has an odd number of in-neighbors in S, then $c_i \equiv 1 \,(\text{mod } 2)$. Thus the only entries of c that are $1 \,(\text{mod } 2)$ correspond to $\text{vonin}(S)$. So if we add c with the columns of I_n with indices corresponding to $\text{vonin}(S)$, the sum would be a zero vector.

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

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

$$(A_1^T + A_2^T + \cdots + A_k^T)_i \equiv 1 \,(\text{mod } 2)\,,$$

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 $A_1^T, A_2^T, \ldots, A_k^T, e_{i_1}, e_{i_2}, \ldots, e_{i_{d-k}}$ are minimally linearly dependent,

$$A_1^T + A_2^T + \cdots + A_k^T + e_{i_1} + e_{i_2} + \cdots + e_{i_{d-k}} \equiv 0 \,(\text{mod } 2)\,.$$

Then

$$A_1^T + A_2^T + \cdots + A_k^T \equiv e_{i_1} + e_{i_2} + \cdots + e_{i_{d-k}} \,(\text{mod } 2)$$

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

As a consequence of the preceding theorem, we have the following combinatorial interpretation of the minimum distance of a $[2n, n]$-code:

Theorem 2.4. *Let C be the binary linear code generated by $[I_n|A]$ where A is the adjacency matrix of a digraph Γ on n vertices with vertex set V. Then the minimum distance $d(C)$ of C is given by*

$$d(C) = \min_{\varnothing \neq S \subseteq V} (|S| + |\,\text{vonin}(S)|).$$

Proof. First note that $H = [A^T|I_n]$ is a parity-check matrix of C. By Theorem 2.3, a code word in C with weight $d(C)$ corresponds to minimally dependent columns of $H = [A^T|I_n]$ indexed by $S \cup \{n+i \mid i \in \text{vonin}(S)\}$ for some nonempty subset S of V. Then

$$d(C) \geq \min_{\varnothing \neq S \subseteq V} (|S| + |\,\text{vonin}(S)|).$$

If there is a nonempty subset S of V for which $d(C) > |S| + |\,\text{vonin}(S)|$, then by Theorem 2.3 we find $(|S| + |\,\text{vonin}(S)|)$ linearly dependent columns of $H = [A^T|I_n]$ giving a codeword of C with weight less than $d(C)$ by Corollary 1.3, a contradiction. Thus the equality holds. □

Corollary 2.5. *Let A be the adjacency matrix of a directed 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 $[I_n|P^TAP]$ are not necessarily the same but they have the same minimum distance.*

Proof. The directed graph with adjacency matrix P^TAP is isomorphic to Γ. Then the binary linear codes generated by $[I_n|A]$ and $[I_n|P^TAP]$ have the same minimum distance by Theorem 2.4. □

3 Equivalent Binary Codes Generated by $[I_n|A]$

In this section we study the equivalence of binary linear codes $C([I_n|A])$ and $C([I_n|A'])$ where A and A' are two $n \times n$ matrices over $\mathbb{F}_2$. We also investigate the same given by transformations on graphs whose adjacency matrices are A and A'.

3.1 Conditions for Equivalence

Lemma 3.1. *Let A and A' be two $n \times n$ matrices over $\mathbb{F}_2$. The binary linear codes $C([I_n|A])$ and $C([I_n|A'])$ are equivalent if and only if there are an $n \times n$ invertible matrix P and a $2n \times 2n$ permutation matrix Q such that $[I_n|A'] = P[I_n|A]Q$. Moreover, if*

$$Q = \left[\begin{array}{c|c} W & Z \\ \hline Y & X \end{array}\right],$$

for some $n \times n$ matrices X, Y, W, Z, then

$$P = (W + AY)^{-1} \text{ and } A' = (W + AY)^{-1}(Z + AX).$$

Proof. Suppose $C([I_n|A])$ and $C([I_n|A'])$ are equivalent. Then there is a $2n \times 2n$ permutation matrix Q such that $\mathrm{RS}([I_n|A']) = \mathrm{RS}([I_n|A]Q)$, where RS denotes the row space. Then there is an $n \times n$ invertible matrix P such that $[I_n|A'] = P[I_n|A]Q$. Conversely suppose that $[I_n|A'] = P[I_n|A]Q$ for some $n \times n$ invertible matrix P and some $2n \times 2n$ permutation matrix Q. Then $\mathrm{RS}([I_n|A']) = \mathrm{RS}([I_n|A]Q)$ and consequently $C([I_n|A])$ and $C([I_n|A'])$ are equivalent.

Suppose $[I_n|A'] = P[I_n|A]Q$ and

$$Q = \left[\begin{array}{c|c} W & Z \\ \hline Y & X \end{array}\right],$$

for some $n \times n$ matrices X, Y, W, Z. Then

$$[I_n|A'] = [P|PA]\left[\begin{array}{c|c} W & Z \\ \hline Y & X \end{array}\right] = [P(W + AY)|P(Z + AX)]$$

which implies

$$P(W + AY) = I_n, P(Z + AX) = A'.$$

Then we have

$$P = (W + AY)^{-1}, A' = P(Z + AX) = (W + AY)^{-1}(Z + AX).$$

□

Observation 3.2. In the preceding lemma:

(a) W (respectively X) is a permutation matrix if and only if $Y = Z = O$ and X (respectively W) is a permutation matrix. In that case, $A' = W^T AX$.

(b) Y (respectively Z) is a permutation matrix if and only if $W = X = O$ and Z (respectively Y) is a permutation matrix. In that case, AY and A are invertible and $A' = (AY)^{-1}Z = Y^T A^{-1}Z$.

Theorem 3.3. *Let A be an $n \times n$ matrix over $\mathbb{F}_2$. Let P_σ and $P_{\sigma'}$ be the permutation matrices obtained by permuting columns of I_n by the permutations σ and σ' respectively. Then the binary linear codes $C([I_n|A])$ and $C([I_n|P_{\sigma'}^T AP_\sigma])$ are equivalent.*

Proof. Consider the following $2n \times 2n$ permutation matrix Q:

$$Q = \left[\begin{array}{c|c} P_{\sigma'} & O \\ \hline O & P_\sigma \end{array}\right].$$

Observe that

$$[I_n|P_{\sigma'}^T AP_\sigma] = P_{\sigma'}^T [I_n|A]Q.$$

Then $C([I_n|A])$ and $C([I_n|P_{\sigma'}^T AP_\sigma])$ are equivalent by Lemma 3.1. □

Theorem 3.4. *Let A be an $n \times n$ invertible matrix over $\mathbb{F}_2$. Let P_σ and $P_{\sigma'}$ be the permutation matrices obtained by permuting columns of I_n by the permutations σ and σ' respectively. Then the binary linear codes $C([I_n|A])$ and $C([I_n|P_{\sigma'}^T A^{-1}P_\sigma])$ are equivalent.*

Proof. Consider the following $2n \times 2n$ permutation matrix Q:

$$Q = \left[\begin{array}{c|c} O & P_\sigma \\ \hline P_{\sigma'} & O \end{array}\right].$$

Observe that

$$[I_n|P_{\sigma'}^T A^{-1}P_\sigma] = P_{\sigma'}^T A^{-1}[I_n|A]Q.$$

Then $C([I_n|A])$ and $C([I_n|P_{\sigma'}^T A^{-1}P_\sigma])$ are equivalent by Lemma 3.1. □

Corollary 3.5. *Let A be an $n \times n$ invertible matrix over $\mathbb{F}_2$. Then the binary linear codes $C([I_n|A])$ and $C([I_n|A^{-1}])$ are equivalent.*

Remark 3.6. The results in Theorem 3.3 and Corollary 3.5 are striking results in coding theory. It is quite clear that any permutation of columns of a generator matrix will leave the code equivalent. However, what is also done here is to permute the rows of A alone, and not those of the generator matrix and the results show that these will also preserve equivalence. This answers the question about the equivalence of $C([I_3|A])$ and $C([I_3|P^T A])$ in Observation 2.1.

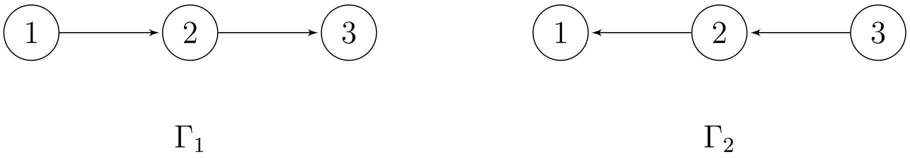

Figure 3: Directed paths Γ_1 and Γ_2

3.2 Transformations on Digraphs

Now we explore transformations on digraphs with adjacency matrices A and A' and their effects on equivalence of binary linear codes $C([I_n|A])$ and $C([I_n|A'])$.

Observation 3.7. Let Γ and Γ' be two labelled isomorphic digraphs on n vertices $1, 2, \ldots, n$ with adjacency matrices A and A' respectively. Suppose σ is a permutation on vertices giving a graph isomorphism from Γ to Γ'. Then $A' = P_\sigma^T A P_\sigma$ where P_σ is the $n \times n$ permutation matrix obtained by permuting the columns of I_n by σ.

Now we define some graph operation on digraphs which are generalization of isomorphism.

Definition 3.8. Let Γ be a labelled digraph on n vertices $1, 2, \ldots, n$ with adjacency matrix A. Let σ and σ' be permutations on $1, 2, \ldots, n$.

(a) The *permuted digraph of* Γ *by* (σ', σ) is the labelled digraph, denoted by $\Gamma_{\sigma',\sigma}$, on n vertices $1, 2, \ldots, n$ such that (i, j) is an arc in $\Gamma_{\sigma',\sigma}$ if and only if $(\sigma'(i), \sigma(j))$ is an arc in Γ.

(b) The *out-permuted digraph of* Γ *by* σ is the labelled digraph, denoted by Γ_σ, on n vertices $1, 2, \ldots, n$ and with adjacency matrix A_σ such that (i, j) is an arc in Γ if and only if $(i, \sigma(j))$ is an arc in Γ_σ.

(c) The *in-permuted digraph of* Γ *by* σ is the labelled digraph, denoted by Γ_σ^-, on n vertices $1, 2, \ldots, n$ and with adjacency matrix A_σ^- such that (i, j) is an arc in Γ if and only if $(\sigma(i), j)$ is an arc in Γ_σ^-.

Note that if $\sigma' = \sigma$, then $\Gamma_{\sigma',\sigma}$ is isomorphic to Γ. In general Γ and $\Gamma_{\sigma',\sigma}$ are not isomorphic.

Example 3.9.

1. Directed paths Γ_1 and Γ_2 in Figure 3 are isomorphic and $\Gamma_2 = (\Gamma_1)_{\sigma,\sigma}$ for the permutation $\sigma = (1, 3)$.

2. Directed graphs Γ and Γ' in Figure 1 are not isomorphic. But $\Gamma' = (\Gamma)_{\sigma',\sigma}$ for the permutations $\sigma = (1)$ and $\sigma' = (1, 2)$.

Observation 3.10. Let Γ be a digraph on n vertices $1, 2, \ldots, n$. Let σ and σ' be permutations on $1, 2, \ldots, n$. Let P_σ and $P_{\sigma'}$ be the permutation matrices obtained by permuting columns of I_n by the permutation σ and σ' respectively.

1. Γ and its permuted digraph $\Gamma_{\sigma',\sigma}$ have the same in-degree sequence and out-degree sequence.

2. The adjacency matrices of Γ_σ, Γ_σ^-, and $\Gamma_{\sigma',\sigma}$ are $A_\sigma = AP_\sigma$, $A_\sigma^- = P_\sigma^T A$, and $P_{\sigma'}^T AP_\sigma$ respectively.

3. $(\Gamma_\sigma)_\sigma^-$ is isomorphic to Γ via the permutation of vertices by σ because $A_\sigma = AP_\sigma$ implies $P_\sigma^T A_\sigma = P_\sigma^T AP_\sigma$.

The following result shows when a digraph Γ and an out-permuted digraph Γ_σ of Γ are isomorphic.

Theorem 3.11. *Let Γ be a labelled digraph on n vertices $1, 2, \ldots, n$ with adjacency matrix A. Let σ be a permutation on $1, 2, \ldots, n$. Then Γ is isomorphic to its out-permuted digraph Γ_σ via a permutation σ' on $1, 2, \ldots, n$ if and only if $\Gamma_{\sigma'}^- = \Gamma_{(\sigma')^{-1}\sigma}$.*

Proof. Let P_σ and $P_{\sigma'}$ be the permutation matrices corresponding to permutations σ and σ' respectively. Then $A_\sigma = AP_\sigma$. Note that Γ is isomorphic to Γ_σ via a permutation σ' if and only if $A_\sigma = P_{\sigma'}^T AP_{\sigma'}$. The result follows from the following:

$$AP_\sigma = P_{\sigma'}^T AP_{\sigma'} \iff AP_\sigma P_{\sigma'}^T = P_{\sigma'}^T A,$$

where $P_\sigma P_{\sigma'}^T$ is the permutation matrix corresponding to the permutation $(\sigma')^{-1}\sigma$. □

The following result shows when a digraph Γ and a permuted digraph $\Gamma_{\sigma',\sigma}$ of Γ are isomorphic.

Theorem 3.12. *Let Γ and Γ' be labelled digraphs on n vertices $1, 2, \ldots, n$ with adjacency matrices A and A' respectively without any isolated vertices. Then $\Gamma' = \Gamma_{\sigma',\sigma}$ for some permutations σ and σ' on $1, 2, \ldots, n$ if and only if bipartite digraphs given by adjacency matrices $\left[\begin{array}{c|c} O_n & A \\ \hline O_n & O_n \end{array}\right]$ and $\left[\begin{array}{c|c} O_n & A' \\ \hline O_n & O_n \end{array}\right]$ are isomorphic.*

Proof. Suppose $\Gamma' = \Gamma_{\sigma',\sigma}$ for some permutations σ and σ' on $1, 2, \ldots, n$. Then $A' = P_{\sigma'}^T A^{-1} P_\sigma$ where P_σ and $P_{\sigma'}$ are the permutation matrices obtained by permuting columns of I_n by the permutations σ and σ' respectively. Note that

$$\left[\begin{array}{c|c} O_n & A' \\ \hline O_n & O_n \end{array}\right] = \left[\begin{array}{c|c} P_{\sigma'} & O_n \\ \hline O_n & P_\sigma \end{array}\right]^T \left[\begin{array}{c|c} O_n & A \\ \hline O_n & O_n \end{array}\right] \left[\begin{array}{c|c} P_{\sigma'} & O_n \\ \hline O_n & P_\sigma \end{array}\right].$$

Thus bipartite digraphs given by adjacency matrices $\left[\begin{array}{c|c} O_n & A \\ \hline O_n & O_n \end{array}\right]$ and $\left[\begin{array}{c|c} O_n & A' \\ \hline O_n & O_n \end{array}\right]$ are isomorphic.

Conversely suppose bipartite digraphs given by adjacency matrices

$$B = \left[\begin{array}{c|c} O_n & A \\ \hline O_n & O_n \end{array}\right] \text{ and } B' = \left[\begin{array}{c|c} O_n & A' \\ \hline O_n & O_n \end{array}\right]$$

are isomorphic. Then there is a permutation matrix $X = \left[\begin{array}{c|c} P & S \\ \hline R & Q \end{array}\right]$ such that $B' = X^T BX$, i.e.,

$$\left[\begin{array}{c|c} O_n & A' \\ \hline O_n & O_n \end{array}\right] = \left[\begin{array}{c|c} P & S \\ \hline R & Q \end{array}\right]^T \left[\begin{array}{c|c} O_n & A \\ \hline O_n & O_n \end{array}\right] \left[\begin{array}{c|c} P & S \\ \hline R & Q \end{array}\right] = \left[\begin{array}{c|c} P^TAR & P^TAQ \\ \hline S^TAR & S^TAQ \end{array}\right].$$

Since X is a permutation matrix, $R = O_n$ if and only if $S = O_n$ in which case P and Q are $n \times n$ permutation matrices. So it suffices to show that $S = O_n$. Suppose $S \neq O_n$. Since $P^TAQ = A' \neq O_n$, we have $P, Q \neq O_n$. Moreover, since Γ and Γ' have no isolated vertices, A and A' have nonzero row i or nonzero column i for each $i = 1, 2, \ldots, n$. Since $P \neq O_n$ and $S \neq O_n$, column i and column $n + j$ of B are interchanged and also row i and row $n + j$ of B are interchanged to obtain $B' = X^T BX$ for some $j = 1, 2, \ldots, n$. If column j of A is nonzero, one of the first n columns of $B' = X^T BX$ is nonzero, a contradiction. If row j of A is nonzero, one of the last n rows of $B' = X^T BX$ is nonzero, a contradiction. □

3.3 Equivalence from Digraph Transformations

In this subsection we explore how digraph transformations give rise to equivalent linear codes.

Theorem 3.13. *Let Γ be a labelled digraph on n vertices $1, 2, \ldots, n$ with adjacency matrix A. Let $\Gamma_{\sigma',\sigma}$ be a permuted digraph of Γ with adjacency matrix A' for some permutation σ and σ' on $1, 2, \ldots, n$. Then the binary linear codes $C([I_n|A])$ and $C([I_n|A'])$ are equivalent.*

Proof. Let P_σ and $P_{\sigma'}$ be the permutation matrices obtained by permuting columns of I_n by the permutation σ and σ' respectively. Then $A' = P_{\sigma'}^T AP_\sigma$. Consider the following $2n \times 2n$ permutation matrix Q:

$$Q = \left[\begin{array}{c|c} P_{\sigma'} & O \\ \hline O & P_\sigma \end{array}\right].$$

Observe that

$$[I_n|A'] = [I_n|P_{\sigma'}^T AP_\sigma] = P_{\sigma'}^T [I_n|A]Q$$

and consequently $C([I_n|A])$ and $C([I_n|A'])$ are equivalent. □

Note that the preceding proof is based on that of Theorem 3.3.

Corollary 3.14. *Let Γ be a labelled digraph on n vertices $1, 2, \ldots, n$ with adjacency matrix A. Let Γ_σ be an out-permuted digraph of Γ for some permutation σ on $1, 2, \ldots, n$. Then the binary linear codes $C([I_n|A])$ and $C([I_n|A_\sigma])$ are equivalent.*

Corollary 3.15. *Let Γ be a labelled digraph on n vertices $1, 2, \ldots, n$ with adjacency matrix A. Let Γ_σ^- be an in-permuted digraph of Γ for some permutation σ on $1, 2, \ldots, n$. Then the binary linear codes $C([I_n|A])$ and $C([I_n|A_\sigma^-])$ are equivalent.*

Definition 3.16. Let Γ be a labelled digraph on n vertices $1, 2, \ldots, n$ with adjacency matrix A that is invertible in $\mathbb{F}_2$. The *inverse digraph of* Γ is the labelled digraph, denoted by Γ^{-1}, on n vertices $1, 2, \ldots, n$ that has adjacency matrix A^{-1}. Let σ, σ' be permutations on $1, 2, \ldots, n$. The *inverse-permuted digraph of* Γ *by* (σ', σ) is the labelled digraph, denoted by $\Gamma^{-1}_{\sigma',\sigma}$, on n vertices $1, 2, \ldots, n$ such that (i, j) is an arc in $\Gamma^{-1}_{\sigma',\sigma}$ if and only if $(\sigma'(i), \sigma(j))$ is an arc in Γ^{-1}.

Observation 3.17. The adjacency matrix of $\Gamma^{-1}_{\sigma',\sigma}$ is $P^T_{\sigma'} A^{-1} P_\sigma$ where P_σ and $P_{\sigma'}$ are the permutation matrices obtained by permuting columns of I_n by the permutations σ and σ' respectively.

Theorem 3.18. *Let* Γ *be a labelled digraph on* n *vertices* $1, 2, \ldots, n$ *with adjacency matrix* A *that is invertible over* $\mathbb{F}_2$. *Let* $\Gamma^{-1}_{\sigma',\sigma}$ *be an inverse-permuted digraph of* Γ *with adjacency matrix* A' *for some permutation* σ, σ' *on* $1, 2, \ldots, n$. *Then the binary linear codes* $C([I_n|A])$ *and* $C([I_n|A'])$ *are equivalent.*

Proof. Let P_σ and $P_{\sigma'}$ be the permutation matrices obtained by permuting columns of I_n by the permutations σ and σ' respectively. Then $A' = P^T_{\sigma'} A^{-1} P_\sigma$. Consider the following $2n \times 2n$ permutation matrix Q:

$$Q = \left[\begin{array}{c|c} O & P_\sigma \\ \hline P_{\sigma'} & O \end{array}\right].$$

Observe that

$$[I_n|A'] = [I_n|P^T_{\sigma'} A^{-1} P_\sigma] = P^T_{\sigma'} A^{-1} [I_n|A] Q$$

and consequently $C([I_n|A])$ and $C([I_n|A'])$ are equivalent. □

Note that the preceding proof is based on that of Theorem 3.4.

Corollary 3.19. *Let* Γ *be a labelled digraph on* n *vertices* $1, 2, \ldots, n$ *with adjacency matrix* A *that is invertible over* $\mathbb{F}_2$. *Let* Γ^{-1} *be the inverse digraph of* Γ *with adjacency matrix* A^{-1}. *Then the binary linear codes* $C([I_n|A])$ *and* $C([I_n|A^{-1}])$ *are equivalent.*

Question 3.20. Let A and A' be two $n \times n$ matrices over $\mathbb{F}_2$. Let Γ and Γ' be directed graphs with adjacency matrices A and A' respectively. Find necessary and sufficient common graph properties of Γ and Γ' for which the binary linear codes $C([I_n|A])$ and $C([I_n|A'])$ are equivalent.

This is a hard question because two digraphs such as Γ and Γ^{-1} with distinctive features produce equivalent codes by Corollary 3.19.

Acknowledgments

The authors would like to thank their colleague Dr. Michael Falk for valuable discussions and suggesting the result given in Theorem 3.12. We would also like to thank the anonymous reviewers for their valuable comments which made the article better.

References

[1] 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* 10(3) (2016), 555–582.

[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.* 312(20) (2012), 3000–3010.

[3] P. Dankelmann, J. D. Key and B. G. Rodrigues, A Characterization of Graphs by Codes from their Incidence Matrices, *Electron. J. Combin.* 20(3) (2013), 18.

[4] W. Fish, R. Fray and E. Mwambene, Binary codes from the complements of the triangular graphs, *Quaestiones Mathematicae* 33(4) (2010), 399–408.

[5] G. D. Forney, Codes on Graphs: Fundamentals, arXiv:1306.6264 .

[6] J. D. Key and B. G. Rodrigues, LCD codes from adjacency matrices of graphs, *Appl. Alg. Eng. Comm. Comp.* 29(3) (2018), 227–244.

[7] S. Mallik and B. Yildiz, Isodual and Self-dual Codes from Graphs, (under review), `https://arxiv.org/pdf/1908.03513v2.pdf`.

[8] S. Mallik, A New Formula for the Minimum Distance of an Expander Code, (under review), `https://arxiv.org/abs/2101.01339`.

[9] E. Petrank and R. M. Roth, Is code equivalence easy to decide?, *IEEE Trans. Inform. Theory* 43(5) (1997), 1602–1604.

[10] R. M. Roth, *Introduction to Coding Theory*, Cambridge University Press 2006.

[11] N. Sendrier and D. E. Simos, The hardness of code equivalence over $\mathbb{F}_q$ and its application to code-based cryptography, In: *Post-Quantum Cryptography*, (Ed. P. Gaborit), Springer Lec. Notes in Comp. Sci. 7932, Limoges, France (2013), 203–216.

[12] A. Vardy, The intractability of computing the minimum distance of a code, *IEEE Trans. Inform. Theory* 43(6) (1997), 1757–1766.

(Received 3 Sep 2020; revised 9 Jan 2021)