SELF-ORTHOGONAL CODES FROM ORBIT MATRICES OF SEIDEL AND LAPLACIAN MATRICES OF STRONGLY REGULAR GRAPHS

DEAN CRNKOVIĆ
Department of Mathematics, University of Rijeka, Croatia

RONAN EGAN
De Brún Centre for Mathematics
School of Mathematics, Statistics and Applied Mathematics
National University of Ireland, Galway

ANDREA ŠVOB*
Department of Mathematics, University of Rijeka, Croatia

(Communicated by Leo Storme)

Abstract. In this paper we introduce the notion of orbit matrices of integer matrices such as Seidel and Laplacian matrices of some strongly regular graphs with respect to their permutation automorphism groups. We further show that under certain conditions these orbit matrices yield self-orthogonal codes over finite fields $\mathbb{F}_q$, where $q$ is a prime power and over finite rings $\mathbb{Z}_m$. As a case study, we construct codes from orbit matrices of Seidel, Laplacian and signless Laplacian matrices of strongly regular graphs. In particular, we construct self-orthogonal codes from orbit matrices of Seidel and Laplacian matrices of the Higman-Sims and McLaughlin graphs.

1. Introduction

Throughout this paper we will assume familiarity with graph theory and error-correcting codes, though we state here some necessary definitions. We refer the reader to [3, 21] for background in the former and to [16] for the latter.

A graph is regular if all the vertices have the same degree; a regular graph is strongly regular of type $(v, k, \lambda, \mu)$ if it has $v$ vertices, is of degree $k$, and if any two adjacent vertices are both adjacent to $\lambda$ common vertices, while any two non-adjacent vertices are both adjacent to $\mu$ common vertices. A strongly regular graph of type $(v, k, \lambda, \mu)$ is usually denoted by SRG$(v, k, \lambda, \mu)$. The complement of a SRG with parameters $(v, k, \lambda, \mu)$ is again strongly regular graph, with parameters $(v, v - k - 1, v - 2k + \mu - 2, v - 2k + \lambda)$.

Let $G$ be a graph with adjacency matrix $A$, with rows and columns labeled by vertices $v_1, \ldots, v_v$. The Seidel adjacency matrix of $G$ is the matrix $S$ defined by
so that $S = J - I - 2A$, where $I$ and $J$ are the $v \times v$ identity and all-ones matrices respectively.

Let $\mathcal{G}$ be a simple graph with adjacency matrix $A$. Let $D$ be the diagonal matrix with the degrees of $\mathcal{G}$ on the diagonal (with the same vertex ordering as in $A$). Then $L = D - A$ is the Laplacian matrix of $\mathcal{G}$, often just called the Laplacian (or admittance matrix). The lesser known signless Laplacian matrix is defined to be $|L| = A + D$, see [13]. We refer to [20] for research regarding Seidel matrices. More information about Seidel and Laplacian matrices can be found in [6].

A $q$-ary linear code $C$ of dimension $k$ for a prime power $q$, is a $k$-dimensional subspace of a vector space $\mathbb{F}_q^n$. Elements of $C$ are called codewords. Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$. The Hamming distance between words $x$ and $y$ is the number $d(x, y) = |\{i : x_i \neq y_i\}|$. The minimum distance of the code $C$ is defined by $d = \min\{d(x, y) : x, y \in C, x \neq y\}$. The weight of a codeword $x$ is $w(x) = d(x, 0) = |\{i : x_i \neq 0\}|$. For a linear code, $d = \min\{w(x) : x \in C, x \neq 0\}$.

A $q$-ary linear code of length $n$, dimension $k$, and distance $d$ is called a $[n, k, d]_q$ code. We may use the notation $[n, k]$ if the parameters $d$ and $q$ are unspecified. An $[n, k]$ linear code $C$ is said to be a best known linear $[n, k]$ code if $C$ has the highest minimum weight among all known $[n, k]$ linear codes. It is said to be optimal if the minimum weight of $C$ achieves the theoretical upper bound on the minimum weight of $[n, k]$ linear codes, and near-optimal if its minimum weight is at most 1 less than the largest possible value.

The dual code $C^\perp$ is the orthogonal complement under the standard inner product $\langle \cdot, \cdot \rangle$, i.e. $C^\perp = \{v \in \mathbb{F}_q^n | \langle v, c \rangle = 0 \text{ for all } c \in C\}$. A code $C$ is self-orthogonal if $C \subseteq C^\perp$ and self-dual if $C = C^\perp$.

Behbahani and Lam introduced the concept of orbit matrices of SRGs in [1]. In [8], the authors presented further properties of orbit matrices of SRGs. We review the relevant details here.

Let $\mathcal{G}$ be a SRG$(v, k, \lambda, \mu)$ and $A$ be its adjacency matrix. Suppose that an automorphism group $G$ of $\mathcal{G}$ partitions the set of vertices $V$ into $t$ orbits $O_1, \ldots, O_t$, with sizes $n_1, \ldots, n_t$, respectively. The orbits divide the matrix $A$ into submatrices $[A_{ij}]$, where $A_{ij}$ is the adjacency matrix of vertices in $O_i$ versus those in $O_j$. We define the matrix $C = [c_{ij}]$, such that $c_{ij}$ is the column sum of $A_{ij}$. The matrix $C$ is the column orbit matrix of the graph $\mathcal{G}$ with respect to the group $G$. The entries of the matrix $C$ satisfy the following equations (see [1, 8]):

\begin{align}
\sum_{i=1}^{t} c_{ij} &= \sum_{j=1}^{t} \frac{n_j}{n_i} c_{ij} = k, \\
\sum_{s=1}^{t} \frac{n_s}{n_j} c_{is} c_{js} &= \delta_{ij} (k - \mu) + \mu n_i + (\lambda - \mu) c_{ij}.
\end{align}

While constructing SRGs with a presumed automorphism group, each matrix with the properties of a column orbit matrix, i.e., each matrix that satisfies equations (1) and (2), is called a column orbit matrix for parameters $(v, k, \lambda, \mu)$ and orbit length distribution $(n_1, \ldots, n_t)$. 

\[ S_{i,j} = \begin{cases} 
0, & v_i = v_j \\
-1, & v_i \sim v_j \\
1, & v_i \simeq v_j 
\end{cases} \]
Construction of self-orthogonal codes from orbit matrices of block designs was introduced in [15] and further developed in [9]. In [8] the authors presented construction of self-orthogonal codes from orbit matrices of adjacency matrix of SRGs and in [12] the authors constructed binary codes from adjacency matrices of SRGs. In [7] the authors define orbit matrices of Hadamard matrices with respect to their permutation automorphism groups and show that under certain conditions these orbit matrices yield self-orthogonal codes. In this paper we extend this definition to orbit matrices of certain integer matrices such as Seidel and Laplacian matrices of SRGs and show that for suitable graph parameters, these orbit matrices yield self-orthogonal codes over finite fields and over rings $\mathbb{Z}_m$. To demonstrate the theory, we construct codes from orbit matrices of Seidel, Laplacian and signless Laplacian matrices of suitable SRGs. As a case study we construct self-orthogonal codes from orbit matrices of Seidel and Laplacian matrices of the Higman-Sims and McLaughlin graphs. The constructed codes include optimal, near-optimal self-orthogonal and self-dual codes, over finite fields and over $\mathbb{Z}_4$.

The codes constructed in this paper have been constructed and examined using Magma [2]. Minimum distances are compared to known codes and bounds at [11].

2. Orbit matrices of Seidel and Laplacian matrices

Let $M$ be an $n \times n$ matrix. A permutation automorphism of $M$ is a pair of $n \times n$ permutation matrices $(P,Q)$ such that $PMQ^\top = M$. The set of all such pairs form the permutation automorphism group of $M$, denoted $\text{PAut}(M)$. An automorphism of a graph $G$ is a permutation of the vertex set $V$ that preserves the edge set $E$. It is well known that an automorphism $g \in \text{Aut}(G)$ induces a permutation automorphism of the adjacency matrix $A$ of the form $(P_g, P_g)$. It follows that any automorphism of a SRG $G$ induces a permutation automorphism of its Seidel, Laplacian, and signless Laplacian matrices.

Let $G$ be a permutation automorphism group of an integer matrix $M = [m_{ij}]$, acting in $t$ orbits on the set of rows and the set of columns of $M$.

Let us denote the $G$-orbits on rows and columns of $M$ by $R_1, \ldots, R_t$ and $C_1, \ldots, C_t$, respectively, and put $|R_i| = \Omega_i$ and $|C_i| = \omega_i$, $i = 1, \ldots, t$.

Let $M_{ij}$ be the submatrix of $M$ consisting of the rows belonging to the row orbit $R_i$ and the column belonging to $C_j$. We denote by $\Gamma_{ij}$ and $\gamma_{ij}$ the sum of some row and some column of $M_{ij}$, respectively. The sums of entries of any two rows (or columns) of $M_{ij}$ are equal so the choice is arbitrary, i.e., $\Gamma_{ij}$ and $\gamma_{ij}$ are well defined. The $t \times t$ matrices $R = [\Gamma_{ij}]$ and $C = [\gamma_{ij}]$ are called the row orbit matrix and column orbit matrix of $M$ with respect to $G$.

The next Lemma follows from the definitions of Seidel and Laplacian matrices of a SRG.

**Lemma 2.1.** Let $G$ be a SRG($v, k, \lambda, \mu$), and let $S$, $L$ and $|L|$ be the Seidel, Laplacian and signless Laplacian matrices of $G$ respectively. Then

\[
S_{i,j}^2 = \begin{cases} 
  v - 1, & i = j \\
  v - 4k + 4\lambda + 2, & i \neq j
\end{cases}
\]

\[
L_{i,j}^2 = \begin{cases} 
  k(k + 1), & i = j \\
  \lambda - 2k, & i \neq j
\end{cases}
\]

\[
|L|_{i,j}^2 = \begin{cases} 
  \lambda + 2k, & i = j, \ v_i \sim v_j \\
  \mu, & i \neq j, \ v_i \sim v_j
\end{cases}
\]

Note that for each of $S$, $L$ and $|L|$, the entries in the square of the matrix are determined by the edges of the graph. Hereafter we let $M$ be any of the matrices.
S, L and |L| corresponding to a SRG(v, k, λ, µ). Then we write

\[
M_{i,j}^2 = \begin{cases} 
\alpha, & i = j \\
\beta, & v_i \sim v_j \\
\pi, & v_i \not\sim v_j 
\end{cases}
\]

where \(\alpha, \beta,\) and \(\pi\) are shorthand for the corresponding terms of Equation (3). Note that \(M\) is symmetric so \(M^2 = MM^\top\).

**Lemma 2.2.** Let \(G\) be a permutation automorphism group of \(M = [m_{ij}]\) of order \(v\), and let \(R_1, \ldots, R_t\) and \(C_1, \ldots, C_t\) be the \(G\)-orbits on the rows and columns of the matrix \(M\), respectively. Further, let \(\Gamma_{ij}\) and \(\gamma_{ij}\) be defined as above. Then

\[
\sum_{j=1}^t \Gamma_{ij} \gamma_{sj} = \delta_{is} \alpha + c_{is} \beta + (\Omega_s - c_{is} - \delta_{is}) \pi
\]

**Proof.** Let \(x\) be a row from the row orbit \(R_i\), and \(y\) be a column from the column orbit \(C_j\). Then

\[
\sum_{j=1}^t \Gamma_{ij} \gamma_{sj} = \sum_{j=1}^t \left( \sum_{z \in C_j} m_{xz} \right) \left( \sum_{w \in R_s} m_{wy} \right) = \sum_{j=1}^t \sum_{z \in C_j} \sum_{w \in R_s} m_{xz} m_{wy} \\
= \sum_{j=1}^t \sum_{z \in C_j} \sum_{w \in R_s} m_{xz} m_{wz} \\
= \sum_{j=1}^t \sum_{w \in R_s} \sum_{z \in C_j} m_{xz} m_{wz}
\]

If \(i \neq s\), then

\[
\sum_{w \in R_s} \sum_{z=1}^v m_{xz} m_{wz} = c_{is} \beta + (\Omega_s - c_{is}) \pi.
\]

If \(i = s\), then

\[
\sum_{w \in R_s} \sum_{z=1}^v m_{xz} m_{wz} = \alpha + c_{ss} \beta + (\Omega_s - 1 - c_{ss}) \pi.
\]

\[\square\]

**Theorem 2.3.** Let \(G\) be a permutation automorphism group of \(M\), and let \(R_1, \ldots, R_t\) and \(C_1, \ldots, C_t\) be the \(G\)-orbits on the rows and columns of \(M\), respectively. Further, let \(\Omega_i, \omega_j, \Gamma_{ij}\) and \(\gamma_{ij}\) be defined as above. Then

\[
\sum_{j=1}^t \Omega_s \omega_j \Gamma_{sj} = \delta_{is} \alpha + c_{is} \beta + (\Omega_s - c_{is} - \delta_{is}) \pi
\]

**Proof.** The sum of entries of the submatrix \(M_{sj}\) is \(\Omega_s \Gamma_{sj}\). On the other hand, this sum is equal to \(\omega_j \gamma_{sj}\), so

\[
\gamma_{sj} = \frac{\Omega_s}{\omega_j} \Gamma_{sj}.
\]

\[\square\]

In Theorems 2.4 and 2.5 we show that under some conditions orbit matrices of Seidel and Laplacian matrices, or their submatrices, span self-orthogonal codes.
Theorem 2.4. Let $G$ be a permutation automorphism group of $M$ acting with $t$ orbits, all of the same length $w$. Further, let $R$ be the row orbit matrix of $M$ with respect to $G$. If $p$ is a prime dividing $\alpha$, $\beta$ and $\pi$, where $\alpha$, $\beta$ and $\pi$ are as given in Equation (4), and $q = p^m$ is a prime power, then the linear code spanned by the matrix $R$ over the field $\mathbb{F}_q$ is a self-orthogonal code of length $t$.

Proof. By Theorem 2.3 we have

$$
\sum_{j=1}^{t} \frac{\Omega}{\omega_j} \Gamma_{ij}\Gamma_{sj} = \sum_{j, \omega_j < w} \frac{\Omega}{\omega_j} \Gamma_{ij}\Gamma_{sj} + \sum_{j, \omega_j = w} \frac{\Omega}{\omega_j} \Gamma_{ij}\Gamma_{sj} = \sum_{j, \omega_j > w} \frac{\Omega}{\omega_j} \Gamma_{ij}\Gamma_{sj} \delta_{is} \alpha + c_{is} \beta + (\Omega_s - c_{is} - \delta_{is}) \pi.
$$

\[ \square \]

Theorem 2.5. Let $G$ be a permutation automorphism group of $M$, and $R$ the corresponding row orbit matrix. Further, let $\omega_j$, $j = 1, \ldots, t$, be the lengths of the $G$-orbits on the columns of $M$, and $w \in \{\omega_j \mid j = 1, \ldots, t\}$. Let $q = p^m$ be a prime power, where $p$ is a prime dividing $\alpha$, $\beta$ and $\pi$, and let the lengths of the column $G$-orbits of $M$ have the property that $p\omega_j | w$ if $\omega_j < w$, and $pw|\omega_j$ if $w < \omega_j$. Then the submatrix of $R$ corresponding to the row and column orbits of length $w$ span a self-orthogonal code of length $s$ over $\mathbb{F}_q$.

Proof. Let the $i$th and the $s$th row orbit have length $w$, i.e. $\Omega_i = \Omega_s = w$. Then

$$
\sum_{j=1}^{t} \frac{\Omega}{\omega_j} \Gamma_{ij}\Gamma_{sj} = \sum_{j, \omega_j < w} \frac{\Omega}{\omega_j} \Gamma_{ij}\Gamma_{sj} + \sum_{j, \omega_j = w} \frac{\Omega}{\omega_j} \Gamma_{ij}\Gamma_{sj} + \sum_{j, \omega_j > w} \frac{\Omega}{\omega_j} \Gamma_{ij}\Gamma_{sj} = \sum_{j, \omega_j < w} \frac{w}{\omega_j} \Gamma_{ij}\Gamma_{sj} + \sum_{j, \omega_j = w} \frac{w}{\omega_j} \Gamma_{ij}\Gamma_{sj} + \sum_{j, \omega_j > w} \frac{w}{\omega_j} \Gamma_{ij}\Gamma_{sj}.
$$

Therefore,

$$
\sum_{j, \omega_j = w} \Gamma_{ij}\Gamma_{sj} = \sum_{j=1}^{t} \frac{\Omega}{\omega_j} \Gamma_{ij}\Gamma_{sj} - \sum_{j, \omega_j < w} \frac{w}{\omega_j} \Gamma_{ij}\Gamma_{sj} - \sum_{j, \omega_j > w} \frac{w}{\omega_j} \Gamma_{ij}\Gamma_{sj} = \delta_{is} \alpha + c_{is} \beta + (\Omega_s - c_{is} - \delta_{is}) \pi - \sum_{j, \omega_j < w} \frac{w}{\omega_j} \Gamma_{ij}\Gamma_{sj} - \sum_{j, \omega_j > w} \frac{w}{\omega_j} \Gamma_{ij}\Gamma_{sj}.
$$

If $\omega_j < w$ then $p|\frac{w}{\omega_j}$. If $w < \omega_j$, then $\frac{w}{\omega_j} \Gamma_{ij}\Gamma_{sj} = \frac{w}{\omega_j} \gamma_{ij} \gamma_{sj}$ and $p|\frac{w}{\omega_j}$. Hence, $\sum_{j, \omega_j = w} \Gamma_{ij}\Gamma_{sj} = 0 \mod p$.

The submatrix of an orbit matrix $R$ corresponding to the fixed rows and fixed columns is called the fixed part of the orbit matrix $R$. The submatrix of $R$ corresponding to the orbits of rows and columns of lengths greater than 1 is called the non-fixed part of the orbit matrix $R$. As a direct consequence of Theorem 2.5 we have the following corollary.

Corollary 1. Let $G$ be a permutation automorphism group of $M$, and $R$ the corresponding row orbit matrix. Further, let $\omega_j$, $j = 1, \ldots, t$, be the lengths of the $G$-orbits on the columns of $M$, and $p$ be a prime that divides $\omega_j$ if $\omega_j > 1$. Then the $s$ rows of the fixed part of $R$ span a self-orthogonal code of length $s$ over the field $\mathbb{F}_q$. 

Advances in Mathematics of Communications

Volume X, No. X (200X), X–XX
The expression (5) from Theorem 2.3 may be rewritten as follows:

\[ \sum_{j=1}^{t} \frac{\Omega_j}{\omega_j} \Gamma_{sj} = \delta_{js}(\alpha - \pi) + c_{ks}(\beta - \pi) + \Omega_s(\pi). \]

Consequently, we may alter the conditions of Theorem 2.5 so as to obtain self-orthogonal codes from SRGs with different parameters, under the extra assumption that the orbit sizes are divisible by the appropriate prime.

**Theorem 2.6.** Let \( G \) be a permutation automorphism group of \( M \), and \( R \) the corresponding row orbit matrix. Further, let \( \omega_j \), \( j = 1, \ldots, t \), be the lengths of the \( G \)-orbits on the columns of \( M \), and \( w \in \{ \omega_j \mid j = 1, \ldots, t \} \). Let \( q = p^m \) be a prime power, where \( p \) is a prime dividing \( \alpha - \pi \) and \( \beta - \pi \), and let the lengths of the column \( G \)-orbits of \( S \) have the property that \( pw \omega_j \) if \( \omega_j = w \), and \( pw \omega_j \) if \( w < \omega_j \). Then the submatrix of \( R \) corresponding to the \( s \) row, column orbits of length \( w \) such that \( \omega > 1 \) span a self-orthogonal code of length \( s \) over \( \mathbb{F}_q \).

3. Codes from Seidel and Laplacian matrices of strongly regular graphs and their orbit matrices

Let \( G \) be a trivial permutation automorphism group of an integer matrix \( M = [m_{ij}] \). Then the orbit matrix is equal to the matrix \( M \). Therefore, we can consider the matrix \( M \) to be an orbit matrix of itself, and can consequently construct self-orthogonal codes using the method introduced in Section 2, in Theorem 2.4, Theorem 2.5, Corollary 1 and Theorem 2.6. To illustrate, we construct Seidel matrices of SRGs with up to 30 vertices satisfying the conditions outlined in Section 2 for obtaining self-orthogonal codes. These are SRGs with parameters \((10,3,0,1), (26,10,3,4)\) and \((28,12,6,4)\). SRGs with these parameters are all known and enumerated, see [19].

Let \( G_1 \) be the SRG with parameters \((10,3,0,1)\), also known as Petersen graph. Let \( G_2, \ldots, G_{10} \) be the SRGs with parameters \((26,10,3,4)\) and \( G_1, \ldots, G_{10} \) be the SRGs with parameters \((28,12,6,4)\). In Table 1 we list representatives of each equivalence class of self-orthogonal codes obtained from the Seidel matrices of these graphs.

| Graph | C | Dual(C) | |Aut(C)| |
|-------|---|---------|--------|--------|
| \( G_1 \) | [10, 4, 6]_{3*} | [10, 6, 4]_{3*} | 2880 |
| \( G_2 \) | [26, 11, 8]_{5} | [26, 15, 6]_{5} | 576 |
| \( G_3 \) | [26, 12, 8]_{5} | [26, 14, 6]_{5} | 48 |
| \( G_4 \) | [26, 12, 8]_{5} | [26, 14, 6]_{5} | 312 |
| \( G_5 \) | [26, 9, 14]_{5*} | [28, 17, 6]_{5} | 124800 |
| \( G_6 \) | [28, 7, 12]_{5} | [28, 21, 4]_{3*} | \( 2^{10} \cdot 3^4 \cdot 5^1 \cdot 7^1 \) |

Table 1. Self-orthogonal codes constructed from Seidel matrices of SRGs

**Remark 1.** The codes with parameters \([10, 4, 6]_{3} \) and \([10, 6, 4]_{3} \) given in Table 1 are optimal, and those with parameters \([26, 9, 14]_{5} \) and \([28, 21, 4]_{3} \) are near-optimal.

3.1. Codes from orbit matrices of Seidel matrices of SRGs. In the sections that follow, we refer to [5] for details on the SRGs \( G_1, \ldots, G_7 \).

Let \( G_1 \) be the SRG(208,75,30,25) on which the finite simple group \( U(3, 4) \) acts transitively. The full automorphism group is \( \text{Aut}(G_1) \cong U(3, 4) \times Z_4 \). In Table 2 we list self-orthogonal codes obtained from orbit matrices of the Seidel matrix of \( G_1 \).
Remark 2. The $[16, 4, 9]_3$ code given in Table 2 is optimal.

Let $G_2$ be the rank 3 graph with parameters $(136, 72, 36, 40)$, on which the simple group $O^-(8, 2)$ acts transitively. The full automorphism group is $\text{Aut}(G_2) \cong O^-(8, 2) : Z_2$. In Table 3 we list self-orthogonal codes obtained from orbit matrices of the Seidel matrix of $G_2$.

| $G \leq \text{Aut}(G_2)$ | $C$ | Dual($C$) | $|\text{Aut}(C)|$ |
|--------------------------|-----|-----------|----------------|
| $Z_3$                    | [10, 4, 6]$_3^*$ | [10, 6, 4]$_3^*$ | 2880          |
| $Z_3$                    | [36, 14, 12]$_3$ | [36, 22, 6]$_3$ | 2903040       |
| $Z_3$                    | [28, 7, 12]$_3$ | [28, 21, 4]$_3^*$ | 2903040       |
| $Z_3$                    | [42, 15, 12]$_3$ | [42, 27, 4]$_3$ | 17280         |
| $Z_3$                    | [45, 15, 12]$_3$ | [45, 30, 4]$_3$ | 5184          |
| $Z_{17}$                 | [8, 2, 6]$_3^*$ | [8, 6, 2]$_3^*$ | 768           |

Table 3. Self-orthogonal codes constructed from orbit matrices of the Seidel matrix of $G_2$

Remark 3. The codes with parameters $[8, 2, 6]_3$, $[8, 6, 2]_3$, $[10, 4, 6]_3$ and $[10, 6, 4]_3$ given in Table 3 are optimal and the $[28, 21, 4]_3$ code is near-optimal.

3.2. Codes from Orbit Matrices of Laplacian Matrices of SRGs. Let $G_3$ be the SRG(165,128,100,96) which is the complement of the rank 3 graph with parameters $(165, 36, 3, 9)$, on which the simple group $U(5, 2)$ acts transitively. Its full automorphism group is $\text{Aut}(G_3) \cong U(5, 2) : Z_2$.

In Table 4 we list self-orthogonal codes obtained from orbit matrices of the Laplacian matrix of $G_3$.

| $G \leq \text{Aut}(G_3)$ | $C$ | Dual($C$) | $|\text{Aut}(C)|$ |
|--------------------------|-----|-----------|----------------|
| $Z_3$                    | [12, 2, 3]$_3$ | [12, 10, 2]$_3^*$ | $2^{10} \cdot 3^5 \cdot 3^7$ |
| $Z_3$                    | [15, 5, 6]$_3$ | [15, 10, 3]$_3^*$ | 10            |
| $Z_3$                    | [40, 10, 18]$_3$ | [40, 30, 4]$_3$ | $2^9 \cdot 3^6 \cdot 3^5 \cdot 3^7$ |
| $Z_3$                    | [45, 15, 12]$_3$ | [45, 30, 6]$_3$ | 103680        |
| $Z_3$                    | [51, 13, 12]$_3$ | [51, 38, 4]$_3$ | 103680        |
| $Z_3$                    | [52, 13, 12]$_3$ | [52, 39, 3]$_3$ | 5184          |
| $Z_3$                    | [53, 14, 12]$_3$ | [53, 39, 4]$_3$ | 864           |
| $Z_3$                    | [33, 9, 12]$_3$ | [33, 24, 2]$_3$ | 96            |

Table 4. Self-orthogonal codes constructed from orbit matrices of the Laplacian matrix of $G_3$

Remark 4. The $[12, 10, 2]_3$ code given in Table 4 is optimal and the $[15, 10, 3]_3$ code is near-optimal.
Let $G_4$ be the SRG($280,135,70,60$) on which the simple group $J_2$ acts transitively. The full automorphism group of $G_4$ is $\text{Aut}(G_4) \cong J_2 : Z_2$. In Table 5 we list self-orthogonal codes obtained from orbit matrices of the Laplacian matrix of $G_4$.

$$
\begin{array}{|c|c|c|c|}
\hline
G \leq \text{Aut}(G_4) & C & \text{Dual}(C) & |\text{Aut}(C)| \\
\hline
Z_2 & [12, 2, 6]_2 & [12, 10, 2]_2 & 1036800 \\
Z_2 & [14, 7, 4]_2^* & [14, 7, 4]_2 & 56448 \\
Z_2 & [40, 14, 8]_2 & [40, 26, 4]_2 & 3932160 \\
Z_2 & [120, 24, 24]_2 & [120, 96, 5]_2 & 1920 \\
Z_2 & [134, 27, 24]_2 & [134, 106, 6]_2 & 336 \\
Z_2 & [134, 30, 24]_2 & [134, 104, 5]_2 & 240 \\
Z_4 & [16, 6, 6]_2^* & [16, 10, 4]_2^* & 11520 \\
Z_4 & [18, 3, 6]_2 & [18, 15, 2]_2^* & 2^{13} \cdot 3^7 \cdot 5^3 \\
Z_4 & [18, 4, 8]_2^* & [18, 14, 2]_2^* & 36864 \\
Z_4 & [36, 6, 8]_2 & [36, 30, 2]_2 & 2^{11} \cdot 3^{13} \\
Z_4 & [48, 8, 16]_2 & [48, 40, 4]_2^* & 69120 \\
Z_4 & [60, 12, 12]_2 & [60, 48, 4]_2 & 49152 \\
Z_4 & [61, 13, 16]_2 & [61, 48, 4]_2 & 17280 \\
Z_5 & [56, 10, 16]_2 & [56, 46, 2]_2 & 1440 \\
Z_7 & [40, 8, 8]_2 & [40, 32, 2]_2 & 393216 \\
Z_7 & [40, 6, 14]_2 & [40, 34, 2]_2 & 3072 \\
Z_5 & [56, 8, 20]_2 & [56, 48, 2]_2 & 115200 \\
Z_5 & [54, 8, 20]_2 & [56, 48, 2]_2 & 9129428480 \\
\hline
\end{array}
$$

**Table 5.** Self-orthogonal codes constructed from orbit matrices of Laplace matrix of $G_4$.

**Remark 5.** The codes with parameters $[14, 7, 4]_2$, $[12, 10, 2]_2$, $[16, 6, 6]_2$, $[16, 10, 4]_2$, $[48, 10, 4]_2$, $[18, 15, 2]_2$, $[18, 4, 8]_2$ and $[18, 14, 2]_2$ given in Table 5 are optimal and those with parameters $[36, 30, 2]_2$ and $[60, 48, 4]_2$ are near-optimal.

Let $G_5$ be the strongly regular graph with parameters ($136,63,30,28$), which is the complement of $G_2$, and is the rank 3 graph on which the simple group $O^-(8, 2)$ acts transitively. The full automorphism group is $\text{Aut}(G_5) \cong O^-(8, 2) : Z_2$. In Table 6 we list self-orthogonal codes obtained from orbit matrices of the signless Laplacian matrix of $G_5$.

$$
\begin{array}{|c|c|c|c|}
\hline
G \leq \text{Aut}(G_5) & C & \text{Dual}(C) & |\text{Aut}(C)| \\
\hline
Z_2 & [16, 3, 8]_2^* & [16, 13, 2]_2^* & 2^{17} \cdot 3^7 \\
Z_2 & [32, 5, 16]_2^* & [32, 27, 2]_2^* & 2^{26} \cdot 3^2 \cdot 5^1 \cdot 7^1 \\
Z_2 & [40, 5, 16]_2^* & [40, 35, 2]_2^* & 2^{24} \cdot 3^2 \cdot 5^1 \cdot 7^1 \\
Z_2 & [60, 3, 32]_2 & [60, 57, 2]_2 & 2^{25} \cdot 3^2 \cdot 5^8 \cdot 7^7 \cdot 11^1 \\
Z_2 & [64, 4, 32]_2^* & [64, 60, 2]_2^* & 2^{25} \cdot 3^2 \cdot 5^1 \cdot 7^2 \\
Z_2 & [64, 7, 32]_2^* & [64, 57, 4]_2^* & 2^{21} \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 31^1 \\
\hline
\end{array}
$$

**Table 6.** Self-orthogonal codes constructed from orbit matrices of the signless Laplacian matrix of $G_5$.

**Remark 6.** The $[64, 7, 32]_2$, $[32, 5, 16]_2$, $[16, 3, 8]_2$, $[16, 13, 2]_2$, $[64, 60, 2]_2$, $[32, 27, 2]_2$, $[64, 57, 4]_2$, $[40, 35, 2]_2$, codes given in Table 4 are optimal and the $[64, 4, 32]_2$ code is near-optimal.
3.3. Codes from Orbit Matrices of Seidel and Laplacian Matrices of Higman-Sims and McLaughlin Graphs. We conclude this section with examples for both Seidel and Laplacian matrices of SRGs with parameters satisfying the conditions of Theorem 2.6 but not Theorem 2.5. Let \( G_6 \) be the Higman-Sims graph, the SRG with parameters \((100,22,0,6)\). The graph was found by Higman & Sims in 1969. It is the unique graph with these parameters and its full automorphism group is \( \text{Aut}(G_6) \cong HS \cdot Z_2 \), where \( HS \) denotes the Higman-Sims group.

Let \( G_7 \) be the McLaughlin graph which is the strongly regular graph with parameters \((275,112,30,56)\). It is the unique graph with these parameters and its full automorphism group \( \text{Aut}(G_7) \cong McL \cdot Z_2 \), where \( McL \) denotes the McLaughlin group. For more details about \( G_6 \) and \( G_7 \) we refer the reader to [4, 5].

In Table 7 and Table 8 we give self-orthogonal codes obtained from orbit matrices of the Seidel matrix of the Higman-Sims graph, and from orbit matrices of the Laplacian matrix of the McLaughlin graph respectively.

| \( G \leq \text{Aut}(G_6) \) | \( C \) | \( \text{Dual}(C) \) | \( |\text{Aut}(C)| \) |
|---|---|---|---|
| \( Z_3 \) | \([19, 4, 10]_5\) | \([19, 15, 2]_5\) | 1920 |
| \( Z_5 \) | \([20, 3, 10]_5\) | \([20, 17, 2]_5\) | \(2^{17} \cdot 3^4 \cdot 5^4\) |
| \( Z_7 \) | \([20, 4, 14]_5^*\) | \([20, 16, 4]_5^*\) | 960 |

**Table 7.** Self-orthogonal codes constructed from orbit matrices of the Seidel matrix of \( G_6 \).

**Remark 7.** The codes with parameters \([20, 4, 14]_5\) and \([20, 16, 4]_5\) given in Table 7 are optimal and the \([20, 17, 2]_5\) code is near-optimal.

| \( G \leq \text{Aut}(G_7) \) | \( C \) | \( \text{Dual}(C) \) | \( |\text{Aut}(C)| \) |
|---|---|---|---|
| \( Z_5 \) | \([54, 4, 20]_5\) | \([54, 50, 2]_5\) | \(2^{24} \cdot 3^4 \cdot 5^4\) |
| \( Z_7 \) | \([55, 3, 20]_5\) | \([55, 52, 2]_5^*\) | \(2^{44} \cdot 3^{17} \cdot 5^{12} \cdot 7^{3} \cdot 11^2 \cdot 13 \cdot 17 \cdot 19 \cdot 23\) |

**Table 8.** Self-orthogonal codes constructed from orbit matrices of the Laplacian matrix of \( G_7 \).

**Remark 8.** The \([55, 52, 2]_5\) code given in Table 7 is optimal.

4. Codes over \( \mathbb{Z}_4 \)

Linear codes over finite rings are defined similarly as linear codes over finite fields, where the codes are modules instead of vector spaces. Let \( \mathbb{Z}_m \) denotes the ring of integers modulo \( m \), where \( m \) is a positive integer and \( m \geq 2 \). The most notable codes over rings are codes over \( \mathbb{Z}_4 \), the ring of integers modulo 4. A \( \mathbb{Z}_4 \)-code \( C \) of length \( n \) is a \( \mathbb{Z}_4 \)-submodule of \( \mathbb{Z}_4^n \). The Hamming weight \( \text{wt}_H(x) \), Lee weight \( \text{wt}_L(x) \) and Euclidean weight \( \text{wt}_E(x) \) of a codeword \( x \) of \( C \) are defined as \( n_1(x) + n_2(x) + n_3(x) \), \( n_1(x) + 2n_2(x) + n_3(x) \) and \( n_1(x) + 4n_2(x) + n_3(x) \), respectively, where \( n_i(x) \) is the number of components of \( x \) which are equal to \( i \). The minimum Lee weight \( d_L(C) \) (resp. minimum Euclidean weight \( d_E(C) \) and minimum Hamming weight \( d_H(x) \)) of \( C \) is the smallest Lee (resp. Euclidean and Hamming) weight among all non-zero codewords of \( C \).

A self-dual \( \mathbb{Z}_4 \)-code which has the property that all Euclidean weights are divisible by eight, is called Type II. A self-dual \( \mathbb{Z}_4 \)-code which is not Type II, is called...
These orbit matrices yield self-orthogonal codes over finite fields. Further, we show that under certain conditions as Seidel and Laplacian matrices, of strongly regular graphs with respect to their orbit matrices of Seidel, Laplacian and signless Laplacian matrices of some rings we refer the reader to [10, 16].

The following results are analogous to those discussed in Section 2 for finite fields. We use the notation introduced in Section 2 and omit the proofs here. We give a method for obtaining self-orthogonal $\mathbb{Z}_4$-codes from orbit matrices of Seidel and Laplacian matrices of strongly regular graphs.

**Theorem 4.1.** Let $G$ be a permutation automorphism group of $M$ acting with $t$ orbits, all of the same length $w$. Further, let $R$ be the row orbit matrix of $M$ with respect to $G$. If $m$ divides $\alpha$, $\beta$ and $\pi$, then the linear code spanned by the matrix $R$ over the ring $\mathbb{Z}_m$ is a self-orthogonal code of length $t$.

**Theorem 4.2.** Let $G$ be a permutation automorphism group of $M$, and $R$ the corresponding row orbit matrix. Further, let $\omega_j$, $j = 1, \ldots, t$, be the lengths of the $G$-orbits on the columns of $M$, and $m \mid \omega_j$, and let the lengths of the column $G$-orbits of $M$ have the property that $m\omega_j|w$ if $\omega_j < w$, and $m\omega_j|\omega_j$ if $w < \omega_j$. Then the submatrix of $R$ corresponding to the $s$ row, column orbits of length $w$ span a self-orthogonal code of length $s$ over the ring $\mathbb{Z}_m$.

**Corollary 2.** Let $G$ be a permutation automorphism group of $M$, and $R$ the corresponding row orbit matrix. Further, let $\omega_j$, $j = 1, \ldots, t$, be the lengths of the $G$-orbits on the columns of $M$, and $m \mid \omega_j$ if $\omega_j > 1$. Then the $s$ rows of the fixed part of $R$ span a self-orthogonal code of length $s$ over the ring $\mathbb{Z}_m$.

**Theorem 4.3.** Let $G$ be a permutation automorphism group of $M$, and $R$ the corresponding row orbit matrix. Further, let $\omega_j$, $j = 1, \ldots, t$, be the lengths of the $G$-orbits on the columns of $M$, and $m \mid \omega_j$ and $\beta - \pi$, and let the lengths of the column $G$-orbits of $S$ have the property that $m\omega_j|w$ if $\omega_j < w$, and $m\omega_j|\omega_j$ if $w < \omega_j$. Then the submatrix of $R$ corresponding to the $s$ row, column orbits of length $w$ such that $w > 1$ span a self-orthogonal code of length $s$ over the ring $\mathbb{Z}_m$.

To demonstrate the method we constructed self-dual $\mathbb{Z}_4$-codes from the graph $G_5$ described in Section 3.2 with parameters (136,63,30,28). Moreover, we obtained self-dual $\mathbb{Z}_4$-codes from $G_8$, a strongly regular graph with parameters (120,63,30,36). The graph $G_8$ is the complement of a SRG(120,56,28,24), and is the graph on which the simple group $A_8$ acts transitively. The full automorphism group of $G_8$ is isomorphic to $O^{-}(8,2) : Z_2$. In Table 9 we list self-dual $\mathbb{Z}_4$-codes obtained from orbit matrices of the signless Laplacian matrices of $G_5$ and $G_8$. The $\mathbb{Z}_4$-codes with parameters $((8,4^{126}))$ and $((16,4^{210}))$ are extremal.

5. Conclusion

In this paper we introduce the notion of orbit matrices of integer matrices, such as Seidel and Laplacian matrices, of strongly regular graphs with respect to their permutation automorphism groups. Further, we show that under certain conditions these orbit matrices yield self-orthogonal codes over finite fields $\mathbb{F}_q$, where $q$ is a prime power and over finite rings $\mathbb{Z}_m$. As a case study, we construct codes from orbit matrices of Seidel, Laplacian and signless Laplacian matrices of some...
Codes from Seidel and Laplacian matrices of SRGs

| Graph | $C$               | $d_H(C)$, $d_E(C)$, $d_L(C)$ | Type |
|-------|-------------------|-------------------------------|------|
| $G_5$ | $\langle (8, 4^2 2^8) \rangle$ | 2,8,4                         | II   |
| $G_5$ | $\langle (10, 4^3 2^{10}) \rangle$ | 2,8,4                         | II   |
| $G_5$ | $\langle (32, 4^4 2^{22}) \rangle$ | 2,8,4                         | II   |
| $G_5$ | $\langle (30, 4^2 2^{24}) \rangle$ | 2,8,4                         | I    |
| $G_5$ | $\langle (40, 4^3 2^{30}) \rangle$ | 2,8,4                         | II   |
| $G_8$ | $\langle (24, 4^1 2^{22}) \rangle$ | 2,8,4                         | II   |
| $G_8$ | $\langle (24, 4^3 2^{14}) \rangle$ | 2,8,4                         | II   |
| $G_8$ | $\langle (28, 4^1 2^{26}) \rangle$ | 2,8,4                         | I    |
| $G_8$ | $\langle (30, 4^0 2^{30}) \rangle$ | 1,4,2                         | I    |

Table 9. Self-dual codes over $\mathbb{Z}_4$ constructed from orbit matrices of signless Laplacian matrices of SRGs $G_5$ and $G_8$

strongly regular graphs. Thereby we show that using the described methods one can obtain interesting codes. The majority of self-orthogonal codes constructed in this paper have large automorphism groups. Codes with large automorphism groups are suitable for permutation decoding (see [17, 18]), the decoding method developed by Jessie MacWilliams in the early 60’s that can be used when a linear code has a sufficiently large automorphism group to ensure the existence of a set of automorphisms, called a PD-set, that has some specific properties. Therefore, most of the codes constructed in this paper are suitable for permutation decoding.

Acknowledgments

The authors would like to thank the anonymous referee for helpful comments that improved the presentation of the paper.

References

[1] M. Behbahani and C. Lam, Strongly regular graphs with non-trivial automorphisms, Discrete Math., 311 (2011), 132–144.
[2] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, J. Symbolic Comput., 24 (1997), 235–265.
[3] A. E. Brouwer, A. M. Cohen and A. Neumaier, Distance-Regular Graphs, Results in Mathematics and Related Areas, 18, Springer-Verlag, Berlin, 1989.
[4] A. E. Brouwer, Strongly regular graphs, in Handbook of Combinatorial Designs, Chapman & Hall/CRC, Boca Raton, FL, 2007, 852–868.
[5] A. E. Brouwer, Parameters of strongly regular graphs, Available from: http://www.win.tue.nl/~aeb/grahps/srg/srgtab.html.
[6] A. E. Brouwer and W. H. Haemers, Spectra of Graphs, Universitext, Springer, New York, 2012.
[7] D. Crnković, R. Egan and A. Švob, Orbit matrices of Hadamard matrices and related codes, Discrete Math., 341 (2018), 1199–1209.
[8] D. Crnković, M. Maksimović, B. G. Rodrigues and S. Rukavina, Self-orthogonal codes from the strongly regular graphs on up to 40 vertices, Adv. Math. Commun., 10 (2016), 555–582.
[9] D. Crnković, B. G. Rodrigues, S. Rukavina and L. Simčić, Self-orthogonal codes from orbit matrices of 2-designs, Adv. Math. Commun., 7 (2013), 161–174.
[10] S. T. Dougherty, Algebraic Coding Theory Over Finite Commutative Rings, SpringerBriefs in Mathematics, Springer, Cham, 2017.
[11] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, Available from: http://www.codetables.de.
[12] W. H. Haemers, R. Peeters and J. M. van Rijckevorsel, Binary codes of strongly regular graphs, Des. Codes Cryptogr., 17 (1999), 187–209.
[13] W. H. Haemers and E. Spence, Enumeration of cospectral graphs, European J. Combin., 25 (2004), 199–211.
[14] M. Harada, Note on the residue codes of self-dual $\mathbb{Z}_4$-codes having large minimum Lee weights, *Adv. Math. Commun.*, 10 (2016), 695–706.

[15] M. Harada and V. Tonchev, Self-orthogonal codes from symmetric designs with fixed-point-free automorphisms, *Discrete Math.*, 264 (2003), 81–90.

[16] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.

[17] J. D. Key, T. P. McDonough and V. C. Mavron, Improved partial permutation decoding for Reed-Muller codes, *Discrete Math.*, 340 (2017), 722–728.

[18] F. J. MacWilliams, Permutation decoding of systematic codes, *Bell System Tech. J.*, 43 (1964), 485–505.

[19] E. Spence, Strongly regular graphs on at most 64 vertices, Available from: [http://www.maths.gla.ac.uk/~es/srgraphs.php](http://www.maths.gla.ac.uk/~es/srgraphs.php).

[20] F. Szöllösi and P. R. J. Östergård, Enumeration of Seidel matrices, *European J. Combin.* 69 (2018), 169–184.

[21] V. D. Tonchev, *Combinatorial Configurations: Designs, Codes, Graphs*, Pitman Monographs and Surveys in Pure and Applied Mathematics, 40, John Wiley & Sons, Inc., New York, 1988.

Received April 2018; revised April 2019.

E-mail address: deanc@math.uniri.hr
E-mail address: ronan.egan@nuigalway.ie
E-mail address: asvob@math.uniri.hr