

SOME CONSTRUCTIONS OF LCD CODES OVER \mathbb{Z}_4

ANA GRBAC AND ANDREA ŠVOB

University of Rijeka, Croatia

ABSTRACT. In this paper, we consider linear codes with complementary duals over the ring of integers modulo 4. These codes are defined as linear codes that intersect their duals trivially and shortly called LCD codes. We focus on some constructions of LCD codes using the adjacency matrices of two-class association schemes.

1. INTRODUCTION

Nowadays, codes over rings are gaining a lot of attention. For example, see [6, 13, 22]. In [5], the authors gave a construction of self-dual codes over finite fields and over commutative rings, from two-class association schemes, generalizing Gaborit's construction of quadratic double circulant codes given in [7]. Further, in [2], the authors use two-class association schemes to construct linear codes with complementary duals (LCD codes) over the finite fields. LCD codes were introduced by Massey in [16] and further developed and studied by many authors. For example, see [12, 23]. One of the reasons why these type of codes are interesting to study, is that LCD codes meet the asymptotic Gilbert-Varshamov bound (see [19]). Although LCD codes over finite fields have been extensively studied so far, not much research is done on LCD codes over rings.

LCD codes over ring of integers modulo 4 have not been a subject of studies in many papers. Recently, the authors in [10, 20] studied the family of LCD codes, i.e., double circulant LCD codes over \mathbb{Z}_{p^2} . In their study, they were interested in obtaining the exact enumeration formula for these families of codes. Further, in [21], the authors studied LCD codes over Galois rings.

2020 *Mathematics Subject Classification.* 05E30, 94B05.

Key words and phrases. LCD code, \mathbb{Z}_4 -code, association scheme, strongly regular graph, doubly regular tournament.

There are other studies on LCD codes over rings, but in each study particular ring (different than \mathbb{Z}_4) is taken into consideration.

In this paper, following the same approach as in [2], we study conditions for constructing LCD codes over the ring \mathbb{Z}_4 from the adjacency matrices of two-class association schemes, i.e., either strongly regular graphs (SRGs) or doubly regular tournaments (DRTs), the method that has not been studied before on the ring of integers modulo 4.

Furthermore, we show how the method can be applied to adjacency matrices of some strongly regular graphs or doubly regular tournaments. The examples of codes given in this paper have been examined using Magma [1].

The paper is organised as follows. Section 2 provides the necessary definitions and notation used throughout. In Section 3, we present the main construction and in Section 4, we give conditions for constructing LCD codes over the ring \mathbb{Z}_4 using adjacency matrices of strongly regular graphs or doubly regular tournaments. Finally, in Section 5, we construct and give examples of LCD codes from some strongly regular graphs and doubly regular tournaments.

2. PRELIMINARIES

In this section, we will give some necessary definitions and notation used throughout the paper.

2.1. *d-class association scheme.* In this subsection, we define a two-class association scheme and give basic properties. For further information, see [3, 9].

Let X be a set of size v . A *d-class association scheme* on X is a partition of $X \times X$ into $d + 1$ relations R_0, R_1, \dots, R_d such that

1. $R_0 = \{(x, x) \mid x \in X\}$,
2. $R_i^T = R_j$ for some $j = 0, 1, 2, \dots, d$ and for all i ,
3. for any triple i, j, k the number of elements $z \in X$ such that $(x, z) \in R_i$ and $(z, y) \in R_j$ is a constant p_{ij}^k which does not depend on the choice of x and y that satisfy $(x, y) \in R_k$.

In this paper, we will be interested in two-class association schemes, i.e., the case $d = 2$. A two-class association scheme is commutative (see [9]), i.e., for any triple of indices i, j, k , $p_{ij}^k = p_{ji}^k$.

Let $A_0 = I$, A_1 and A_2 be the adjacency matrices of a two-class association scheme. Let J denote the all one matrix and I the identity matrix. Two cases may occur. Either $A_1^T = A_1$, $A_2^T = A_2$ and then the undirected graph (X, R_1) is strongly regular (shortly SRG) or $A_1^T = A_2$, $A_2^T = A_1$ and the directed graph (X, R_1) is a doubly regular tournament (shortly DRT). It is known that doubly regular tournaments are equivalent to skew Hadamard matrices (see [18]).

In both cases (SRGs and DRTs) we have $A_2 = J - I - A_1$. Let $\bar{A}_1 := J - I - A_1 = A_2$ and $A_1 = A$. Then $AJ = JA = kJ$.

In case of SRGs there is a positive integer k and non-negative integers λ and μ such that

$$A^2 = kI + \lambda A + \mu(J - I - A),$$

and for DRTs there are non-negative integers λ and μ such that

$$A^2 = \lambda A + \mu(J - I - A).$$

2.2. \mathbb{Z}_4 -codes. The ring \mathbb{Z}_4 is 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 $wt_H(x)$, Lee weight $wt_L(x)$ and Euclidean weight $wt_E(x)$ 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 $d_L(C)$ (respectively minimum Euclidean weight $d_E(C)$ and minimum Hamming weight $d_H(C)$) of C is the smallest Lee (respectively Euclidean and Hamming) weight among all non-zero codewords of C . Every \mathbb{Z}_4 linear code has $k_1 + k_2$ codewords and as such is usually said to be of type $4^{k_1}2^{k_2}$. For more information on codes over rings we refer the reader to [4, 11].

The dual code C^\perp is the orthogonal complement under the standard inner product $\langle \cdot, \cdot \rangle$, i.e. $C^\perp = \{v \in \mathbb{F}_q^n \mid \langle v, c \rangle = 0 \text{ for all } c \in C\}$. A linear code C is called a Euclidean or classical LCD code if $C \cap C^\perp = \{0\}$. For more information see [11]. Usually we just write an LCD code in this instance. It is easy to see that the dual of an LCD code is an LCD code. A code C is *self-orthogonal* if $C \subseteq C^\perp$ and *self-dual* if equality is attained.

2.3. LCD codes over \mathbb{Z}_4 . In [16], Massey gave the characterization of LCD codes over a field.

LEMMA 2.1. [16, Proposition 1] *Let G be a generator matrix for a code over a field. Then $\det(GG^\top) \neq 0$ if and only if G generates an LCD code.*

Since this paper deals with LCD codes over rings, we need to state some extra definitions and properties. LCD codes over chain rings were examined in [15], where a sufficient condition for an LCD code over finite chain rings was given. We begin with some definitions about finite chain rings (see [14] for more information).

A commutative ring is called a chain ring if the lattice of all its ideals is a chain. It is well known that if R is a finite chain ring, then R is a principal ideal ring and has a unique maximal ideal $\langle \gamma \rangle = R\gamma = \{r\gamma \mid r \in R\}$. Its chain of ideals is

$$R = \langle \gamma^0 \rangle \supset \langle \gamma^1 \rangle \supset \dots \supset \langle \gamma^{t-1} \rangle \supset \langle \gamma^t \rangle = \{0\}.$$

The integer t is called the nilpotency index of $\langle \gamma \rangle$.

An example of a finite chain ring is \mathbb{Z}_{p^a} , the ring of integers modulo p^a , for some prime p and $a \geq 1$. In this paper, we are interested in LCD codes over \mathbb{Z}_4 which fall into this category.

REMARK 2.2. In the case of \mathbb{Z}_4 , it holds that $\gamma = t = 2$.

Let R be a finite commutative ring with identity. Let $A = (a_{ij})_{m \times l}$ be a matrix over R . If the rows of A are linearly independent, then we say that A is a full-row-rank matrix. If there is an $l \times m$ matrix B over R such that $AB = I$, then we say that A is right-invertible and B is a right inverse of A . If $m = l$ and the determinant $\det(A)$ is a unit of R , then we say that A is non-singular.

By [15, Lemma 2.3], it holds that an $m \times m$ matrix over a finite chain ring R is invertible if and only if it is non-singular. In order to give a sufficient condition for LCD codes, we need to define the standard form of a generator matrix.

DEFINITION 2.3. [17, Definition 3.2] *Let C be a linear code over R . A generator matrix G for C is said to be in standard form if, after a suitable permutation of the coordinates, the following holds:*

$$G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & A_{0,t-1} & A_{0,t} \\ 0 & \gamma I_{k_1} & \gamma A_{1,2} & \gamma A_{1,3} & \cdots & \gamma A_{1,t-1} & \gamma A_{1,t} \\ 0 & 0 & \gamma^2 I_{k_2} & \gamma^2 A_{2,3} & \cdots & \gamma^2 A_{2,t-1} & \gamma^2 A_{2,t} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & \cdots & \gamma^{t-1} I_{k_{t-1}} & \gamma^{t-1} A_{t-1,t} \end{pmatrix} \\ = \begin{pmatrix} A_0 \\ \gamma A_1 \\ \gamma^2 A_2 \\ \vdots \\ \gamma^{t-1} A_{t-1} \end{pmatrix}.$$

In [15], the authors gave a sufficient condition for a linear code over a finite chain ring R to be LCD.

THEOREM 2.4. [15, Theorem 3.5] *Let C be a code over R with generator matrix G in standard form. If the $k \times k$ matrix GG^T is invertible, then C is an LCD code, where k is the number of rows of G .*

In what follows, we study the case when $R = \mathbb{Z}_4$. It is obvious that for \mathbb{Z}_4 -codes the condition from Theorem 2.4 can not be satisfied. However, in the following theorem we give a condition that enables us to construct LCD codes over \mathbb{Z}_4 . A statement given in Theorem 2.5 is crucial for the constructions given in this paper.

THEOREM 2.5. *Let C be a code over \mathbb{Z}_4 with generator matrix G . If GG^T is a diagonal matrix with all elements on the main diagonal equal to 1 or 3, then C is an LCD code.*

PROOF. Let v_1, v_2, \dots, v_k be the rows of G , i.e., generators of the code C . It follows that $\langle v_i, v_j \rangle = 0$ for $i \neq j$ and $\langle v_i, v_i \rangle \in \{1, 3\}$, where $1 \leq i, j \leq k$. A codeword w in C is of the form $w = \sum_{i \in A} \alpha_i v_i$, where $\alpha_i \in \mathbb{Z}_4$ for $i \in A$. If w is not a zero vector, then $\langle v_j, w \rangle \neq 0$, for some $j \in A$. Hence, $w \notin C^\perp$. Since no non-trivial element in C is also in C^\perp , it follows that C is an LCD code. \square

3. CONSTRUCTION OF LCD CODES OVER \mathbb{Z}_4

In [5], the authors presented pure and bordered constructions of self-dual codes. Following the notation given in [2, 5] we give pure and bordered constructions of LCD codes from SRGs or DRTs over the ring \mathbb{Z}_m . Here, we apply these constructions to LCD codes over \mathbb{Z}_4 .

Let $r, s, t \in \mathbb{Z}_m$ and let $Q_{\mathbb{Z}_m} = (rI + sA + t\bar{A})$. In the pure construction, the generator matrix of a code is given by

$$(3.1) \quad P_{\mathbb{Z}_m} = (I \mid Q_{\mathbb{Z}_m}(r, s, t)).$$

Let $r, s, t \in \mathbb{Z}_m$ and let $Q_{\mathbb{Z}_m} = (rI + sA + t\bar{A})$. Let α, β and γ be scalars. In the bordered construction, the generator matrix of a code is given by

$$(3.2) \quad B_{\mathbb{Z}_m} = \left(\begin{array}{c|c|c|c} 1 & 0 \dots 0 & \alpha & \beta \dots \beta \\ \hline 0 & & \gamma & \\ \vdots & I & \vdots & Q_{\mathbb{Z}_m}(r, s, t) \\ \hline 0 & & \gamma & \end{array} \right).$$

For the construction of LCD codes we will use Theorem 2.5. We state Lemma 3.1 from [5] that will be useful for our constructions.

LEMMA 3.1. [5, Lemma 3.3] *For strongly regular graphs we have*

$$\begin{aligned} & Q_{\mathbb{Z}_m}(r, s, t)Q_{\mathbb{Z}_m}(r, s, t)^T \\ &= (r^2 + s^2k - t^2 - t^2k + t^2v)I \\ &\quad + (2rs + s^2\lambda - 2st - 2st\lambda + t^2\lambda + 2stk + t^2v - 2t^2k)A \\ &\quad + (2rt + s^2\mu - 2st\mu + t^2\mu + 2stk + t^2v - 2t^2 - 2t^2k)\bar{A}. \end{aligned}$$

For doubly regular tournaments we have

$$\begin{aligned} & Q_{\mathbb{Z}_m}(r, s, t)Q_{\mathbb{Z}_m}(r, s, t)^T \\ &= (r^2 + (s^2 + t^2)k)I \\ &\quad + (rt + sr + (s^2 + t^2)(k - 1 - \lambda) + st\lambda + st\mu)A \\ &\quad + (rt + sr + (s^2 + t^2)(k - \mu) + st\mu + st\lambda)\bar{A}. \end{aligned}$$

Under certain conditions, the construction given in Theorem 3.2, i.e., the pure construction, yields LCD codes over \mathbb{Z}_4 .

THEOREM 3.2. *Let $r, s, t \in \mathbb{Z}_4$ and let $Q_{\mathbb{Z}_4} = (rI + sA + t\bar{A})$. Further, let $P_{\mathbb{Z}_4}$ be an $n \times 2n$ matrix over \mathbb{Z}_4 and suppose that $P_{\mathbb{Z}_4}$ generates a $[2n, n]$ code C over \mathbb{Z}_4 . The code $P_{\mathbb{Z}_4}(r, s, t)$ formed from an $SRG(v, k, \lambda, \mu)$ is an LCD code if $x \in \{1, 3\}$ and*

$$\begin{aligned} r^2 + s^2k - t^2 - t^2k + t^2v &= x - 1, \\ 2rs + s^2\lambda - 2st - 2st\lambda + t^2\lambda + 2stk + t^2v - 2t^2k &= 0, \\ 2rt + s^2\mu - 2st\mu + t^2\mu + 2stk + t^2v - 2t^2 - 2t^2k &= 0. \end{aligned}$$

The code $P_{\mathbb{Z}_4}(r, s, t)$ formed from a $DRT(v, k, \lambda, \mu)$ is an LCD code if $x \in \{1, 3\}$ and

$$\begin{aligned} r^2 + (s^2 + t^2)k &= x - 1, \\ rt + sr + (s^2 + t^2)(k - 1 - \lambda) + st\lambda + st\mu &= 0, \\ rt + sr + (s^2 + t^2)(k - \mu) + st\mu + st\lambda &= 0. \end{aligned}$$

PROOF. By Equation (3.1) and Lemma 3.1, $P_{\mathbb{Z}_4}P_{\mathbb{Z}_4}^\top = (a+1)I + bA + c\bar{A}$, where $Q_{\mathbb{Z}_4}Q_{\mathbb{Z}_4}^\top = aI + bA + c\bar{A}$.

If $a+1 = x \in \{1, 3\}$, $b = 0$, $c = 0$ over \mathbb{Z}_4 , it holds that $P_{\mathbb{Z}_4}P_{\mathbb{Z}_4}^\top$ is a scalar matrix with 1 or 3 on the main diagonal. Hence, by Theorem 2.5, $P_{\mathbb{Z}_4}$ is an LCD code. \square

Under certain conditions, the construction presented in Theorem 3.3, i.e., the bordered construction, yields LCD codes over \mathbb{Z}_4 .

THEOREM 3.3. *Let $r, s, t \in \mathbb{Z}_4$ and let $Q_{\mathbb{Z}_4} = (rI + sA + t\bar{A})$. Further, let $B_{\mathbb{Z}_4}$ be an $(n+1) \times (2n+2)$ matrix over \mathbb{Z}_4 and let α, β and γ be scalars and suppose that $B_{\mathbb{Z}_4}$ generates a $[2n+2, n+1]$ code C over \mathbb{Z}_4 .*

The code $B_{\mathbb{Z}_4}(r, s, t)$ formed from an $SRG(v, k, \lambda, \mu)$ is an LCD code if $x, y \in \{1, 3\}$ and

$$\begin{aligned} r^2 + s^2k - t^2 - t^2k + t^2v &= x - 1 - \gamma^2, \\ 2rs + s^2\lambda - 2st - 2st\lambda + t^2\lambda + 2stk + t^2v - 2t^2k &= -\gamma^2, \\ 2rt + s^2\mu - 2st\mu + t^2\mu + 2stk + t^2v - 2t^2 - 2t^2k &= -\gamma^2, \\ 1 + \alpha^2 + v\beta^2 &= y, \\ \alpha\gamma + \beta(r + sk + t(v - k - 1)) &= 0. \end{aligned}$$

The code $B_{\mathbb{Z}_4}(r, s, t)$ formed from a $DRT(v, k, \lambda, \mu)$ is an LCD code if $x, y \in \{1, 3\}$ and

$$\begin{aligned} r^2 + (s^2 + t^2)k &= x - 1 - \gamma^2, \\ rt + sr + (s^2 + t^2)(k - 1 - \lambda) + st\lambda + st\mu &= -\gamma^2, \\ rt + sr + (s^2 + t^2)(k - \mu) + st\mu + st\lambda &= -\gamma^2, \\ 1 + \alpha^2 + v\beta^2 &= y, \\ \alpha\gamma + \beta(r + sk + t(v - k - 1)) &= 0. \end{aligned}$$

PROOF. In order to obtain that $B_{\mathbb{Z}_4}B_{\mathbb{Z}_4}^\top$ is a diagonal matrix with elements 1 or 3 on the main diagonal the inner product of the top row of $B_{\mathbb{Z}_4}$ with itself must be 1 or 3, i.e., $1 + \alpha^2 + v\beta^2 = y \in \{1, 3\}$. The inner product of the top row of $B_{\mathbb{Z}_4}$ with any other row must be equal to 0, i.e., $\alpha\gamma + \beta(r + sk + t(v - k - 1)) = 0$. Finally, the inner products of all the other rows of $B_{\mathbb{Z}_4}$ must give a scalar matrix, i.e., $I + \gamma^2J + Q_{\mathbb{Z}_4}(r, s, t)Q_{\mathbb{Z}_4}(r, s, t)^\top = xI$, where $x \in \{1, 3\}$.

It follows that $Q_{\mathbb{Z}_4}(r, s, t)Q_{\mathbb{Z}_4}(r, s, t)^\top = (x - 1 - \gamma^2)I - \gamma^2A - \gamma^2\bar{A}$. Therefore, by Lemma 3.1 the conditions follow. \square

4. CONDITIONS FOR OBTAINING LCD CODES OVER \mathbb{Z}_4

Taking adjacency matrices of two-class association schemes one can apply Theorems 3.2 and 3.3 to obtain LCD codes over the ring \mathbb{Z}_4 . To simplify the construction, one can list the conditions for which the used adjacency matrix of two-class association scheme will produce an LCD code over \mathbb{Z}_4 . Here, we will interpret integers as their value modulo 4.

4.1. *LCD codes from SRGs over \mathbb{Z}_4 .* In Table 1 and in Table 2, we list conditions under which strongly regular graphs can be used for obtaining LCD codes over \mathbb{Z}_4 by applying pure and bordered constructions.

r	s	t	Pure construction
± 1	± 1	± 1	$v = 0$ ($x = 1$)
± 1	± 1	$0, 2$	$k = x + 2, \lambda = 2, \mu = 0$
± 1	$0, 2$	± 1	$v = k + x - 1, \lambda = \mu = 2k - v$
± 1	$0, 2$	$0, 2$	Never
$0, 2$	± 1	± 1	Never
$0, 2$	± 1	$0, 2$	$k = x - 1, \lambda = \mu = 0$
$0, 2$	$0, 2$	± 1	$v = k + x, \lambda = 2k - v, \mu = \lambda + 2$
$0, 2$	$0, 2$	$0, 2$	Always ($x = 1$)

TABLE 1. LCD codes from SRGs over \mathbb{Z}_4 , pure construction

r	s	t	Bordered construction
± 1	± 1	± 1	$v = -\gamma^2 (x = 1)$
± 1	± 1	$0, 2$	$k = x + 2 - \gamma^2, \lambda = 2 - \gamma^2, \mu = -\gamma^2$
± 1	$0, 2$	± 1	$v = k + x - 1 - \gamma^2, \lambda = \mu = 2k - v - \gamma^2$
± 1	$0, 2$	$0, 2$	Never
$0, 2$	± 1	± 1	Never
$0, 2$	± 1	$0, 2$	$k = x - 1 - \gamma^2, \lambda = \mu = -\gamma^2$
$0, 2$	$0, 2$	± 1	$v = k + x - \gamma^2, \lambda = 2k - v - \gamma^2, \mu = \lambda + 2$
$0, 2$	$0, 2$	$0, 2$	$\gamma^2 = 0 (x = 1)$

TABLE 2. LCD codes from SRGs over \mathbb{Z}_4 , bordered construction

For the bordered construction, two additional conditions involving α and β are required:

$$1 + \alpha^2 + v\beta^2 = y, \quad \alpha\gamma + \beta(r + sk + t(v - k - 1)) = 0.$$

4.2. *LCD codes from DRTs over \mathbb{Z}_4 .* In Table 3, we list conditions under which doubly regular tournaments and pure construction can be used to obtain LCD codes over \mathbb{Z}_4 . Relations among the parameters that we use in Table 3 are given in the following lemma.

LEMMA 4.1. *If Γ is a DRT with parameters (v, k, λ, μ) , then $v = 4\lambda + 3$, $k = 2\lambda + 1$ and $\mu = \lambda + 1$.*

r	s	t	Pure construction
± 1	± 1	± 1	$2k = x + 2, rt + sr + 2(k - 1 - \lambda) + st\lambda + st\mu = 0$
± 1	± 1	$0, 2$	$k = x + 2, rt + sr + k - 1 - \lambda + st\lambda + st\mu = 0$
± 1	$0, 2$	± 1	$k = x + 2, rt + sr + k - 1 - \lambda + st\lambda + st\mu = 0$
± 1	$0, 2$	$0, 2$	Never
$0, 2$	± 1	± 1	$2k = x - 1, rt + sr + 2(k - 1 - \lambda) + st\lambda + st\mu = 0$
$0, 2$	± 1	$0, 2$	$k = x - 1, sr + k - 1 - \lambda + st\lambda + st\mu = 0$
$0, 2$	$0, 2$	± 1	$k = x - 1, rt + k - 1 - \lambda + st\lambda + st\mu = 0$
$0, 2$	$0, 2$	$0, 2$	Always ($x = 1$)

TABLE 3. LCD codes from DRTs over \mathbb{Z}_4 , pure construction

In Table 4, we list conditions under which doubly regular tournaments and bordered construction can be used to obtain LCD codes over \mathbb{Z}_4 .

As stated in Subsection 4.1, for the bordered construction we have two more conditions on α and β :

$$1 + \alpha^2 + v\beta^2 = y, \quad \alpha\gamma + \beta(r + sk + t(v - k - 1)) = 0.$$

r	s	t	Bordered construction
± 1	± 1	± 1	$2k = x + 2 - \gamma^2, rt + sr + 2(k - 1 - \lambda) + st\lambda + st\mu = -\gamma^2$
± 1	± 1	$0, 2$	$k = x + 2 - \gamma^2, rt + sr + k - 1 - \lambda + st\lambda + st\mu = -\gamma^2$
± 1	$0, 2$	± 1	$k = x + 2 - \gamma^2, rt + sr + k - 1 - \lambda + st\lambda + st\mu = -\gamma^2$
± 1	$0, 2$	$0, 2$	Never
$0, 2$	± 1	± 1	$2k = x - 1 - \gamma^2, rt + sr + 2(k - 1 - \lambda) + st\lambda + st\mu = -\gamma^2$
$0, 2$	± 1	$0, 2$	$k = x - 1 - \gamma^2, sr + k - 1 - \lambda + st\lambda + st\mu = -\gamma^2$
$0, 2$	$0, 2$	± 1	$k = x - 1 - \gamma^2, rt + k - 1 - \lambda + st\lambda + st\mu = -\gamma^2$
$0, 2$	$0, 2$	$0, 2$	$\gamma^2 = 0 (x = 1)$

TABLE 4. LCD codes from DRTs over \mathbb{Z}_4 , bordered construction

5. EXAMPLES OF LCD CODES FROM SOME FAMILIES OF SRGs AND DRTs

In this section, we illustrate the methods given in Section 3 by giving examples of LCD codes constructed over \mathbb{Z}_4 .

Using the Gray map, one can check how good the linear code obtained from \mathbb{Z}_4 -codes is. In this section, we take just a few examples of SRGs and DRTs and illustrate how the method can be applied. Use of different SRGs and DRTs will produce different codes. Since the enumeration and classification of LCD codes over \mathbb{Z}_4 -codes is not finished, and there does not exist any database of such codes, we cannot state with certainty that the produced codes are new or not. The aim of this paper is to show how one can construct LCD \mathbb{Z}_4 -codes using SRGs and DRTs.

In [20], the authors examined numerical results. They were comparing the \mathbb{Z}_4 -codes with the best known binary linear code with particular parameters, obtained from \mathbb{Z}_4 code by the Gray mapping. See ([11]) for more details. In this paper, we follow the same approach.

5.1. *LCD codes from some families of SRGs.* In this subsection, we give some examples of LCD codes over \mathbb{Z}_4 obtained from some families of strongly regular graphs. The examples are obtained applying methods given in Section 3 and conditions given in Table 1.

EXAMPLE 5.1 (LCD codes from Paley strongly regular graphs). Let q be a prime power such that $q \equiv 1 \pmod{4}$ and let $P(q)$ be a Paley graph, i.e., strongly regular graph with parameters $\left(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4}\right)$. For $v \equiv 1 \pmod{4}$ and $\mu = \lambda + 1$, one can obtain LCD codes in the following cases: by pure construction, for $P_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{0, 2\}$, and by bordered construction, for $B_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{0, 2\}$, $\gamma \in \{0, 2\}$, $1 + \alpha^2 + \beta^2 \in \{1, 3\}$, $\alpha\gamma + \beta r = 0$.

EXAMPLE 5.2 (The Petersen graph). The Petersen graph is the unique SRG(10, 3, 0, 1). Taking into account that $v \equiv 2 \pmod{4}$, $\mu \equiv 1 \pmod{4}$

and $\mu = \lambda + 1$, one can obtain LCD codes in the following cases: by pure construction, for $P_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{0, 2\}$, and by bordered construction, for $B_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{0, 2\}$, $\gamma \in \{0, 2\}$, $1 + \alpha^2 + 2\beta^2 \in \{1, 3\}$, $\alpha\gamma + \beta(r + 3s) = 0$.

EXAMPLE 5.3 (The Shrikhande graph). The Shrikhande graph is a strongly regular graph with parameters $(16, 6, 2, 2)$. Taking into account that $\mu \equiv 2 \pmod{4}$ and $\lambda = \mu$, one can obtain LCD codes in the following cases. By pure construction, for $P_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{-1, 1\}$, and $P_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{0, 2\}$. By bordered construction, for $B_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{-1, 1\}$, $\alpha, \gamma \in \{0, 2\}$, $\beta(r + 2s + t) = 0$, and for $B_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{0, 2\}$, $\alpha, \gamma \in \{0, 2\}$, $\beta(r + t) = 0$.

EXAMPLE 5.4 (The Clebsch graph). The Clebsch graph is the $\text{SRG}(16, 5, 0, 2)$. Cases for which one can obtain LCD codes are the following (applying methods given in Section 3 and conditions given in Table 1). By pure construction, for $P_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{-1, 1\}$, and for $P_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{0, 2\}$. By bordered construction, for $B_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{-1, 1\}$, $\alpha, \gamma \in \{0, 2\}$, $\beta(r + s + 2t) = 0$, and for $B_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{0, 2\}$, $\alpha, \gamma \in \{0, 2\}$, $\beta(r + s) = 0$.

To illustrate, we give examples of LCD codes constructed over \mathbb{Z}_4 from above listed SRGs. For the computations we used Magma [1]. Examples of \mathbb{Z}_4 -codes in Table 5 are written in the form $(n, 4^{k_1}2^{k_2}, d)$ where n is the length of the code and d is the minimum Lee distance.

The entry in the last column is the best known minimum distance of a $[2n, n]$ binary linear code, obtained by the Gray mapping. For example, in the first row we obtained $(10, 4^5, 2)$ LCD code over \mathbb{Z}_4 . Using the Gray mapping, the $[20, 10, 2]$ binary linear code is obtained, for which it is known that 6 is the best known minimum Hamming distance (see [8]).

5.2. *LCD codes from some families of DRTs.* In this subsection, we give some examples of LCD codes over \mathbb{Z}_4 obtained from some doubly regular tournaments. The examples are obtained applying methods given in Section 3 and conditions given in Tables 3 and 4.

EXAMPLE 5.5 (DRT(3,1,0,1)). By applying conditions it follows that one can obtain LCD codes in the following cases: by pure construction, for $P_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{0, 2\}$. By bordered construction, for $B_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{-1, 1\}$, $\gamma \in \{-1, 1\}$, $1 + \alpha^2 + 3\beta^2 \in \{1, 3\}$, $\alpha\gamma + \beta(r + s + t) = 0$, and for $B_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{0, 2\}$, $\gamma \in \{0, 2\}$, $1 + \alpha^2 + 3\beta^2 \in \{1, 3\}$, $\alpha\gamma + \beta(r + s + t) = 0$.

EXAMPLE 5.6 (DRT(7,3,1,2)). One can obtain LCD codes in the following cases. For pure construction, for $P_{\mathbb{Z}_4}(r, s, t)$, where $r, s \in \{-1, 1\}$, $r \neq s$, $t \in \{0, 2\}$, for $P_{\mathbb{Z}_4}(r, s, t)$, where $r, t \in \{-1, 1\}$, $r \neq t$, $s \in \{0, 2\}$, and for

SRG	Construction	C	d_{min}
Paley	$P_{\mathbb{Z}_4}(0, 2, 0)$	$(10, 4^5, 2)$	6
	$B_{\mathbb{Z}_4}(0, 0, 2), \alpha = 1, \beta = 3, \gamma = 0$	$(12, 4^6, 2)$	8
	$P_{\mathbb{Z}_4}(2, 2, 0)$	$(18, 4^9, 2)$	8
	$B_{\mathbb{Z}_4}(0, 2, 0), \alpha = 0, \beta = \gamma = 2$	$(20, 4^{10}, 2)$	9
Petersen	$P_{\mathbb{Z}_4}(2, 0, 2)$	$(20, 4^{10}, 2)$	8
	$B_{\mathbb{Z}_4}(2, 0, 2), \alpha = \beta = 2, \gamma = 0$	$(22, 4^{11}, 2)$	10
Shrikhande	$P_{\mathbb{Z}_4}(3, 1, 3)$	$(32, 4^{16}, 4)$	12
	$P_{\mathbb{Z}_4}(2, 2, 0)$	$(32, 4^{16}, 2)$	12
	$B_{\mathbb{Z}_4}(3, 1, 3), \alpha = \gamma = 0, \beta = 3$	$(34, 4^{17}, 4)$	13
	$B_{\mathbb{Z}_4}(2, 2, 0), \alpha = \gamma = 0, \beta = 2$	$(34, 4^{17}, 2)$	13
Clebsch	$P_{\mathbb{Z}_4}(3, 1, 3)$	$(32, 4^{16}, 4)$	12
	$P_{\mathbb{Z}_4}(0, 2, 0)$	$(32, 4^{16}, 2)$	12
	$B_{\mathbb{Z}_4}(3, 1, 3), \alpha = \gamma = 0, \beta = 3$	$(34, 4^{17}, 4)$	13
	$B_{\mathbb{Z}_4}(2, 2, 0), \alpha = 0, \beta = \gamma = 2$	$(34, 4^{17}, 2)$	13

TABLE 5. Examples of LCD codes from SRGs over \mathbb{Z}_4

$P_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{0, 2\}$. For bordered construction, we obtain LCD codes for:

- $B_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{-1, 1\}$, $\gamma \in \{-1, 1\}$, $1 + \alpha^2 + 3\beta^2 \in \{1, 3\}$, $\alpha\gamma + \beta(r + 3s + 3t) = 0$,
- $B_{\mathbb{Z}_4}(r, s, t)$, where $r, s \in \{-1, 1\}$, $r \neq s$, $t \in \{0, 2\}$, $\gamma \in \{0, 2\}$, $1 + \alpha^2 + 3\beta^2 \in \{1, 3\}$, $\alpha\gamma + \beta(r + 3s + 3t) = 0$,
- $B_{\mathbb{Z}_4}(r, s, t)$, where $r, t \in \{-1, 1\}$, $r \neq t$, $s \in \{0, 2\}$, $\gamma \in \{0, 2\}$, $1 + \alpha^2 + 3\beta^2 \in \{1, 3\}$, $\alpha\gamma + \beta(r + 3s + 3t) = 0$,
- $B_{\mathbb{Z}_4}(r, s, t)$, where $r, t \in \{0, 2\}$, $r \neq t$, $s \in \{-1, 1\}$, $\gamma \in \{-1, 1\}$, $1 + \alpha^2 + 3\beta^2 \in \{1, 3\}$, $\alpha\gamma + \beta(r + 3s + 3t) = 0$,
- $B_{\mathbb{Z}_4}(r, s, t)$, where $r, s \in \{0, 2\}$, $r \neq s$, $t \in \{-1, 1\}$, $\gamma \in \{-1, 1\}$, $1 + \alpha^2 + 3\beta^2 \in \{1, 3\}$, $\alpha\gamma + \beta(r + 3s + 3t) = 0$,
- $B_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{0, 2\}$, $\gamma \in \{0, 2\}$, $1 + \alpha^2 + 3\beta^2 \in \{1, 3\}$, $\alpha\gamma + \beta(r + 3s + 3t) = 0$.

EXAMPLE 5.7 (DRT(11,5,2,3)). One can obtain LCD codes in the following cases. By pure construction, for $P_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{0, 2\}$. By bordered construction, for $B_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{-1, 1\}$, $\gamma \in \{-1, 1\}$, $1 + \alpha^2 + 3\beta^2 \in \{1, 3\}$, $\alpha\gamma + \beta(r + s + t) = 0$, and for $B_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{0, 2\}$, $\gamma \in \{0, 2\}$, $1 + \alpha^2 + 3\beta^2 \in \{1, 3\}$, $\alpha\gamma + \beta(r + s + t) = 0$.

EXAMPLE 5.8 (DRT(15,7,3,4)). One can obtain LCD codes in the following cases. For pure construction, for $P_{\mathbb{Z}_4}(r, s, t)$, where $r, s \in \{-1, 1\}$, $r = s$, $t \in \{0, 2\}$, for $P_{\mathbb{Z}_4}(r, s, t)$, where $r, t \in \{-1, 1\}$, $r = t$, $s \in \{0, 2\}$, and for

$P_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{0, 2\}$. For bordered construction, we obtain LCD codes for:

- $B_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{-1, 1\}$, $\gamma \in \{-1, 1\}$, $1 + \alpha^2 + 3\beta^2 \in \{1, 3\}$, $\alpha\gamma + \beta(r + 3s + 3t) = 0$,
- $B_{\mathbb{Z}_4}(r, s, t)$, where $r, s \in \{-1, 1\}$, $r = s$, $t \in \{0, 2\}$, $\gamma \in \{0, 2\}$, $1 + \alpha^2 + 3\beta^2 \in \{1, 3\}$, $\alpha\gamma + 3\beta t = 0$,
- $B_{\mathbb{Z}_4}(r, s, t)$, where $r, t \in \{-1, 1\}$, $r = t$, $s \in \{0, 2\}$, $\gamma \in \{0, 2\}$, $1 + \alpha^2 + 3\beta^2 \in \{1, 3\}$, $\alpha\gamma + 3\beta s = 0$,
- $B_{\mathbb{Z}_4}(r, s, t)$, where $r, t \in \{0, 2\}$, $r = t$, $s \in \{-1, 1\}$, $\gamma \in \{-1, 1\}$, $1 + \alpha^2 + 3\beta^2 \in \{1, 3\}$, $\alpha\gamma + 3\beta s = 0$,
- $B_{\mathbb{Z}_4}(r, s, t)$, where $r, s \in \{0, 2\}$, $r = s$, $t \in \{-1, 1\}$, $\gamma \in \{-1, 1\}$, $1 + \alpha^2 + 3\beta^2 \in \{1, 3\}$, $\alpha\gamma + 3\beta t = 0$,
- $B_{\mathbb{Z}_4}(r, s, t)$, where $r, s, t \in \{0, 2\}$, $\gamma \in \{0, 2\}$, $1 + \alpha^2 + 3\beta^2 \in \{1, 3\}$, $\alpha\gamma + \beta(r + 3s + 3t) = 0$.

To illustrate, we give examples of LCD codes constructed over \mathbb{Z}_4 from the above listed DRTs. For the computations we used Magma [1]. Examples of \mathbb{Z}_4 -codes in Table 6 are written in the form $(n, 4^{k_1}2^{k_2}, d)$ where n is the length of the code and d is the minimum Lee distance.

The entry in the last column is the best known minimum distance of a $[2n, n]$ binary linear code, obtained by the Gray mapping. For example, in the first row we obtained $(6, 4^3, 2)$ LCD code over \mathbb{Z}_4 . Using the Gray mapping, the $[12, 6, 2]$ binary linear code is obtained, for which it is known that 4 is the best known minimum Hamming distance (see [8]).

DRT	Construction	C	d_{min}
(3, 1, 0, 1)	$P_{\mathbb{Z}_4}(0, 2, 0)$	$(6, 4^3, 2)$	4
	$B_{\mathbb{Z}_4}(3, 1, 3)$, $\alpha = \beta = \gamma = 1$	$(8, 4^4, 4)$	5
	$B_{\mathbb{Z}_4}(0, 0, 2)$, $\alpha = \beta = 2$, $\gamma = 0$	$(8, 4^4, 2)$	5
(7, 3, 1, 2)	$P_{\mathbb{Z}_4}(3, 1, 2)$	$(14, 4^7, 4)$	8
	$P_{\mathbb{Z}_4}(0, 2, 0)$	$(14, 4^7, 2)$	8
	$B_{\mathbb{Z}_4}(0, 1, 2)$, $\alpha = 3$, $\beta = \gamma = 1$	$(16, 4^8, 8)$	8
	$B_{\mathbb{Z}_4}(0, 2, 0)$, $\alpha = \beta = 2$, $\gamma = 0$	$(16, 4^8, 2)$	8
(11, 5, 2, 3)	$P_{\mathbb{Z}_4}(0, 0, 2)$	$(22, 4^{11}, 2)$	10
	$B_{\mathbb{Z}_4}(3, 1, 3)$, $\alpha = 3$, $\beta = \gamma = 1$	$(24, 4^{12}, 4)$	12
	$B_{\mathbb{Z}_4}(0, 0, 2)$, $\alpha = \beta = 2$, $\gamma = 0$	$(24, 4^{12}, 2)$	12
(15, 7, 3, 4)	$P_{\mathbb{Z}_4}(3, 3, 2)$	$(30, 4^{15}, 6)$	12
	$P_{\mathbb{Z}_4}(0, 0, 2)$	$(30, 4^{15}, 2)$	12
	$B_{\mathbb{Z}_4}(1, 1, 3)$, $\alpha = 3$, $\beta = 2$, $\gamma = 1$	$(32, 4^{16}, 4)$	12
	$B_{\mathbb{Z}_4}(0, 0, 2)$, $\alpha = \beta = 2$, $\gamma = 0$	$(32, 4^{16}, 2)$	12

TABLE 6. Examples of LCD codes from DRTs over \mathbb{Z}_4

ACKNOWLEDGEMENTS.

The authors have been supported by Croatian Science Foundation under the projects HRZZ-IP-2022-10-4571 and HRZZ-UIP-2020-02-5713. The authors would like to thank the anonymous referees for their comments that improved the presentation of the paper.

REFERENCES

- [1] W. Bosma, J. Cannon, Handbook of Magma functions, Department of Mathematics, University of Sydney, 1994, <http://magma.maths.usyd.edu.au/magma>.
- [2] D. Crnković, A. Grbac and A. Švob, *Formally self-dual LCD codes from two-class association schemes*, Appl. Algebra Engrg. Comm. Comput. **34** (2023), 183–200.
- [3] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Reports Suppl. 1973, 10.
- [4] S. T. Dougherty, Algebraic coding theory over finite commutative rings, Springer, Cham, 2017.
- [5] S. T. Dougherty, J.-L. Kim and P. Solé, *Double circulant codes from two-class association schemes*, Adv. Math. Commun. **1** (2007), 45–64.
- [6] S. T. Dougherty, J. Gildea, A. Korban and A. M. Roberts, *Codes over a ring of order 32 with two Gray maps*, Finite Fields Appl. **95** (2024), paper no. 102384.
- [7] P. Gaborit, *Quadratic double circulant codes over fields*, J. Combin. Theory Ser. A **97** (2002), 85–107.
- [8] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, available online at <http://www.codetables.de>. Accessed on 2025-06-04.
- [9] D. G. Higman, *Coherent configuration*, Geometriae Dedicata **4** (1975), 1–32.
- [10] D. Huang, M. Shi and P. Solé, *Double circulant self-dual and LCD codes over \mathbb{Z}_{p^2}* , Internat. J. Found. Comput. Sci. **30** (2019), 407–416.
- [11] W. C. Huffman and V. Pless, Fundamentals of error-correcting codes, Cambridge University Press, Cambridge, 2003.
- [12] W. Fish, J. D. Key and E. Mwambene, *Special LCD codes from products of graphs*, Appl. Algebra Engrg. Comm. Comput. **34** (2023), 553–579.
- [13] Z. Liu, *Galois LCD codes over rings*, Adv. Math. Commun. **18** (2024), 91–104.
- [14] X. Liu, *On the characterization of cyclic codes over two classes of rings*, Acta Math. Sci. Ser. B (Engl. Ed.) **33** (2013), 413–422.
- [15] X. Liu and H. Liu, *LCD codes over finite chain rings*, Finite Fields Appl. **34** (2015), 1–19.
- [16] J. L. Massey, *Linear codes with complementary duals*, Discrete Math. **106/107** (1992), 337–342.
- [17] G. H. Norton and A. Sălăgean, *On the structure of linear and cyclic codes over finite chain rings*, Appl. Algebra Eng. Commun. Comput. **10** (2000), 489–506.
- [18] K. B. Reid and E. Brown, *Doubly regular tournaments are equivalent to skew Hadamard matrices*, J. Combinatorial Theory Ser. A **12** (1972), 332–338.
- [19] N. Sendrier, *Linear codes with complementary duals meet the Gilbert-Varshamov bound*, Discrete Math. **285** (2004), 345–347.
- [20] M. Shi, D. Huang, L. Sok and P. Solé, *Double circulant LCD codes over \mathbb{Z}_4* , Finite Fields Appl. **58** (2019), 133–144.
- [21] M. Shi, D. Huang, L. Sok and P. Solé, *Double circulant self-dual and LCD codes over Galois rings*, Adv. Math. Commun. **13** (2019), 171–183.
- [22] D. Suprijanto, *Linear codes and cyclic codes over finite rings and their generalizations: a survey*, Electron. J. Graph Theory Appl. (EJGTA) **11** (2023), 467–490.

- [23] A. Švob, *LCD codes from equitable partitions of association schemes*, Appl. Algebra Engrg. Comm. Comput. **34** (2023), 889–896.

A. Grbac
Faculty of Mathematics
University of Rijeka
51000 Rijeka
Croatia
E-mail: abaric@math.uniri.hr

A. Švob
Faculty of Mathematics
University of Rijeka
51000 Rijeka
Croatia
E-mail: asvob@math.uniri.hr

Received: 25.3.2024.

Revised: 8.6.2025.

NEKE KONSTRUKCIJE LCD KODOVA NAD \mathbb{Z}_4

A. GRBAC AND A. ŠVOB

SAŽETAK. U ovom radu promatramo linearne kodove s komplementarnim dualima nad prstenom cijelih brojeva modulo 4. Promatrani kodovi se definiraju kao kodovi koji se sa svojim dualnim kodovima sijeku trivijalno, a kraće ih zovemo LCD kodovi. U ovom radu nas zanimaju neke konstrukcije LCD kodova u kojima koristimo matrice susjedstva asocijacijskih shema s dvije klase.