J. Algebra Comb. Discrete Appl.
10(3) • 119–129

Received: 24 November 2021
Accepted: 31 December 2022

Journal of Algebra Combinatorics Discrete Structures and Applications

A new construction of quadratic double circulant LCD codes

Research Article

Shikha Yadav, Om Prakash

Abstract: Let $GF(l)$ be the Galois field with $l = p^m$ elements where p is a prime number and integer $m \geq 1$. Here, we present three constructions for linear codes over $GF(l)$ (depending on the parity of l) by using the quadratic residue approach and obtain some sufficient conditions for these codes to be LCD with respect to the Euclidean and Hermitian inner products, respectively. Furthermore, several examples of codes, including optimal and near to optimal codes, are provided to support our study.

2010 MSC: 94B05, 94B15, 94B60

Keywords: Cyclic codes, Quasi-cyclic codes, Quadratic double circulant codes, LCD codes

1. Introduction

Quasi-cyclic (QC) codes of index s are the linear codes invariant under T^s where T is the cyclic shift operator, and s is a positive integer. These codes are the generalization of cyclic codes and have been extensively studied in ([6, 16]). In 2001, Ling and Solé [18] introduced a new algebraic approach to study quasi-cyclic codes over finite fields, which was extended over finite chain rings [19] in 2003. Double circulant codes are a special class of quasi-cyclic codes of index 2. Using the approach in [18], Alahmadi et al. [2] showed that self-dual double circulant codes of odd dimension are dihedral in even characteristic and consta-dihedral in odd characteristic. Later, many researchers studied these codes and investigated their asymptotic behaviour, see [24, 29, 31, 33]. On the other hand, in 2022, quadratic double circulant self-dual codes were studied by Gaborit [10] in terms of their generator matrices. Several conditions were presented there under which these codes are self-dual. Later, Dougherty et al. [9] constructed self-dual double circulant codes from the adjacency matrices in 2007. Recently, Gildea et al. extended the work of Gaborit [10] and presented a modified construction to investigate self-dual codes.

LCD codes were introduced in 1992 by Massey [23] over finite fields. These codes were shown to be optimum linear coding solutions for the two-user binary adder channel (2-BAC). Also, in 1994,

*Shikha Yadav, Om Prakash (Corresponding Author); Department of Mathematics, Indian Institute of Technology Patna, Patna–*801106*, Bihar, India (email: 1821ma10@iitp.ac.in, om@iitp.ac.in).*

complementary dual cyclic codes were studied by Yang and Massey [32] in terms of their generator polynomials. In 2004, Sendrier [26] showed that the LCD codes meet Gilbert-Varshamov bound. In 2015, Liu and Liu [20] obtained necessary and sufficient conditions for linear codes over finite chain rings to have complementary dual while Islam et al. [15] established such conditions over a non-chain ring. In 2016, Guneri et al. [13] characterized quasi-cyclic complementary dual codes. Afterwards, Carlet and Guilley [4] showed the application of binary LCD codes as a counter-measures to side-channel attacks. In 2018, Li [17] provided construction of the Hermitian LCD cyclic codes over finite fields and investigated their parameters. These codes were further explored in [5, 21]. In 2018 itself, Zhu and Shi [34] studied complementary dual four circulant codes over a finite field and obtained bound on their relative distance. Later, Carlet et al. [5] introduced a general construction of LCD codes and showed the equivalence of linear codes over $\mathbb{F}_q$ (resp. $\mathbb{F}_{q^2}$) with Euclidean LCD code, for $q > 3$ (resp. Hermitian LCD code, for $q > 2$). Meanwhile, Shi et al. [28] studied double circulant self-dual and LCD codes over Galois rings and later LCD codes over $\mathbb{Z}_4$ [27]. These codes were later studied by Huang et al. [14] over $\mathbb{Z}_{p^2}$, and an exact enumeration of these codes were presented. In 2019, Liu and Wang [22] studied LCD codes over finite rings. In 2020, Sok [30] provided some constructions of Hermitian LCD codes via new methods and algorithms. Meanwhile, Prakash et al. [25] presented LCD codes over the ring $\mathbb{F}_q + u\mathbb{F}_q$ and expounded an application of Hermitian LCD codes in the multi-secret sharing scheme, which was first presented for Euclidean LCD codes by Alahmadi et al. [1]. Recently, LCD codes have been studied by using weighing matrices, and adjacency matrices in [7, 8] using the concepts of (r, λ) design and strongly regular graphs (SRGs) or doubly regular tournament (DRTs), respectively.

Most of the above works on double circulant LCD codes have been studied in terms of generator polynomials. As per our survey, little work uses the generator matrices to study double circulant LCD codes. The quadratic double circulant self-dual codes have already been studied in [10, 11]. Inspired by these works, we first establish conditions for the linear codes obtained from the construction given in [10] to be LCD. Further, we provide new construction to obtain linear codes and derive conditions for these linear codes to be LCD. We also consider the modified construction used in [11] to derive some conditions for the linear codes obtained from this construction to be LCD.

This article is organized as follows: Section 2 contains basic definitions and essential background for Quadratic double circulant codes. Section 3 characterizes several conditions for quadratic double circulant codes to be LCD and provides a new modified construction for quadratic double circulant LCD codes. Finally, we present several examples of optimal and near-to-optimal codes in support of our study.

2. Notations and definitions

Throughout this article, we assume that q is an odd prime and $l = p^m$ for $m \geq 1$ and a prime p. For any matrix $A = [a_{ij}]$, its transpose is defined as $A^{'} = [a_{ji}]$. For an even positive integer m, conjugate matrix $\bar{A}$ is defined as $\bar{A} = [a_{ij}^{\sqrt{l}}] = [a_{ij}^{p^{\frac{m}{2}}}]$ and conjugate transpose is defined as $A^* = [a_{ji}^{\sqrt{l}}]$. Here, I denotes the identity matrix of order q, the matrix with all entries as 1 is denoted by J, and O denotes the zero matrix of order q.

An $[n, k]-$ *linear code* C over the Galois field $GF(l)$ is defined as a $k-$ dimensional subspace of the vector space $GF(l)^n$ under the usual componentwise addition and scalar multiplication. The *generator matrix* G of the code C is a $k \times n$ matrix whose rows form a basis for C. The *Euclidean inner product* of vectors $a = (a_0, \ldots, a_{n-1})$ and $b = (b_0, \ldots, b_{n-1})$ in $GF(l)^n$ is defined as

$$a \cdot b = a_0b_0 + a_1b_1 + \cdots + a_{n-1}b_{n-1}.$$

We define the *Hermitian inner product* (when m is even) of vectors $a = (a_0, \ldots, a_{n-1})$ and $b = (b_0, \ldots, b_{n-1})$ in $GF(l)^n$ as

$$\langle a, b\rangle_H = a_0b_0^{\sqrt{l}} + a_1b_1^{\sqrt{l}} + \cdots + a_{n-1}b_{n-1}^{\sqrt{l}}.$$

The *Euclidean dual* $C^{\perp}$ and *Hermitian dual* $C^{\perp_H}$ of a linear code C over the finite field $GF(l)$ are defined

as

$$C^{\perp} = \{v \in GF(l)^n : v \cdot c = 0 \text{ for all } c \text{ in } C\}$$

and

$$C^{\perp_H} = \{v \in GF(l)^n : \langle v, c\rangle_H = 0 \text{ for all } c \text{ in } C\},$$

respectively. A linear code C is said to be *Euclidean* (or *Hermitian* resp.) LCD code if and only if $C \cap C^{\perp} = \{0\}$ (or $C \cap C^{\perp_H} = \{0\}$ resp.). Throughout this article, the term LCD code refers to Euclidean LCD code until and unless specified. The *Hamming weight* $w_H(a)$ of any vector a is the number of non-zero components in it while the *Hamming distance* $d_H(a, b)$ between two vectors a and b is the number of components in which the two vectors differ. The minimum *Hamming distance* of a linear code is defined as

$$d_H(C) = \min\{d_H(a, b) : a, b \in C, a \neq b\}.$$

Now, we define quadratic residue, which will be used in the next subsection. An element $d \in GF(q)$ is said to be a quadratic residue in $GF(q)$ if there exists $x \in GF(q)$ such that

$$x^2 = d.$$

2.1. Quadratic double circulant codes

Let $GF(l)$ and $GF(q)$ be the Galois fields containing l and q elements, respectively. Following the notations of [10], we define a one-one map $\boldsymbol{a}$ from the set $\{0, 1, \ldots, q-1\}$ to $GF(q)$. In particular, we consider $\boldsymbol{a}$ as the identity map when q is a prime number. Also, we enumerate the elements of $GF(q)$ as $a_0 = \boldsymbol{a}(0)$, $a_1 = \boldsymbol{a}(1)$, $\ldots$, $a_{q-1} = \boldsymbol{a}(q-1)$. For $r, s, t \in GF(l)$, we denote quadratic residue circulant matrix of order q by $Q_q(r, s, t)$ which is a matrix over $GF(l)$ with $(i, j)^{th}$ entry $q_{ij} = \chi(a_j - a_i)$ where χ is a function over $GF(q)$ defined by

$$\chi(x) = \begin{cases} r, & \text{if } x = 0 \\ s, & \text{if } x \text{ is a quadratic residue in } GF(q) \\ t, & \text{otherwise,} \end{cases}$$

for $x \in GF(q)$. The following lemma is crucial for characterizing Euclidean and Hermitian LCD codes in our construction.

Lemma 2.1. *[10, Theorem 3.1] Let q be a power of an odd prime and $Q_q(a, b, c)$ be a quadratic residue circulant matrix with a, b and c in $GF(l)$. We have the following two cases:*

(i) For $q = 4k + 1$,

$Q_q(a, b, c)[Q_q(a, b, c)]' = Q_q(a^2 + 2k(b^2 + c^2), 2ab - b^2 + k(b + c)^2, 2ac - c^2 + k(b + c)^2)$,
and
$Q_q(a, b, c)[Q_q(a, c, b)]' = Q_q(a^2 + 4bck, ab + ac - bc + (b + c)^2k, ab + ac - bc + (b + c)^2k)$.

(ii) For $q = 4k + 3$,

$Q_q(a, b, c)[Q_q(a, b, c)]' = Q_q(a^2 + (2k+1)(b^2 + c^2), ab + ac + k(b^2 + c^2) + (2k+1)bc, ab + ac + k(b^2 + c^2) + (2k+1)bc)$,
and
$Q_q(a, b, c)[Q_q(a, c, b)]' = Q_q(a^2 + 2bc(2k+1), 2ab + c^2 + (b + c)^2k, 2ac + b^2 + (b + c)^2k)$.

Now, we recall that a *quadratic double circulant code* [10] over $GF(l)$ is a linear code with the generator matrix one of the following forms:

$$G_1 = [I | Q_q(a, b, c)], \tag{1}$$

$$G_2 = \left[\begin{array}{c|c|c|c} 1 & 0\cdots 0 & \alpha & \beta\cdots\beta \\ \hline 0 & & \gamma & \\ \vdots & I & \vdots & Q_q(a,b,c) \\ 0 & & \gamma & \end{array}\right], \tag{2}$$

where $a, b, c, \alpha, \beta, \gamma \in GF(l)$. The linear codes obtained from pure (1) and bordered (2) quadratic double circulant forms are $[2q, q]$ and $[2q+2, q+1]$ codes, respectively. We can also modify the construction (1) to obtain a new construction with the generator matrix

$$G_3 = [A|Q_q(a,b,c)], \tag{3}$$

where A is a circulant matrix over $GF(l)$.

3. Construction of LCD codes

In this section, we first determine some conditions under which the obtained linear codes through constructions (1) and (3) are LCD codes. Later, we provide another construction (4) for linear codes, which is a generalization of construction (2) and obtain conditions under which these codes are Euclidean or Hermitian LCD codes. For this, we first state two basic lemmas.

Lemma 3.1. *[23] Let G be a generator matrix for a linear code C over a finite field. Then $det(GG^{'}) \neq 0$ if and only if C is an LCD code.*

Lemma 3.2. *[5] Let G be a generator matrix for a linear code C over a finite field. Then $det(GG^{*}) \neq 0$ if and only if C is a Hermitian LCD code.*

Now, we impose several conditions on q, l to obtain LCD codes from construction (1) and present some examples (using the Magma computation system [3]) to validate our results.

Theorem 3.3. *Let q be an odd prime and $l = p^s$ for $s \geq 1$ and an odd prime p such that $p \nmid (1+q^2)$. Then a linear code C over $GF(l)$ with generator matrix $G = [I|Q_q(1,1,1)]$ is an LCD code over $GF(l)$.*

Proof. By Lemma 2.1, we have

$$Q_q(1,1,1)Q_q(1,1,1)^{'} = Q_q(q,q,q) = qJ.$$

Therefore,

$$GG' = I + Q_q(1,1,1)Q_q(1,1,1)^{'} = I + qJ$$

and $det(GG^{'}) = 1 + q^2 \neq 0$ in $GF(l)$ if $p \nmid (1+q^2)$. Hence, C is an LCD code by Lemma 3.1. □

Example 3.4. *Let $q = 5$ and $l = 5$. Then $5 \nmid (q^2+1)$ and the linear code with generator matrix*

$$G = [I|Q_5(1,1,1)]$$

is a $[10, 5, 2]$ LCD code over $GF(5)$.

Theorem 3.5. *For two odd primes p, q such that $p \nmid (q^2 - 2q + 2)$ and $l = p^s$ $(s \geq 1)$, a linear code C over $GF(l)$ with generator matrix $G = [I|Q_q(0,1,1)]$ is an LCD code.*

Proof. By Lemma 2.1, we have

$$Q_q(0,1,1)Q_q(0,1,1)^{'} = Q_q(q-1, q-2, q-2) = I + (q-2)J.$$

Therefore,

$$GG' = I + Q_q(0,1,1)Q_q(0,1,1)^{'} = 2I + (q-2)J$$

and $det(GG^{'}) = 2^{q-1}(2 + q(q-2)) \neq 0$ in $GF(l)$ if $p \nmid (q^2 - 2q + 2)$. Hence, C is an LCD code. □

Example 3.6. *Let $q = 5$ and $l = 5$. Then $5 \nmid (q^2 - 2q + 2)$ and the linear code with generator matrix*

$$G = [I|Q_5(0, 1, 1)]$$

is a $[10, 5, 4]$ LCD code over $GF(5)$. It is a near to optimal code.

Theorem 3.7. *Let $q = 3+4k$ be an odd prime and $l = p^s$ for $s \geq 1$ and a prime p such that $p \nmid (k+2), p \nmid (q+1)(k+1)+1$. Then a linear code C over $GF(l)$ with generator matrix $[I|Q_q(1, 0, 1)]$ or $[I|Q_q(1, 1, 0)]$ is an LCD code over $GF(l)$.*

Proof. By Lemma 2.1, we have

$$\begin{aligned} Q_q(1, 0, 1,)Q_q(1, 0, 1)^{'} = Q_q(1, 1, 0)Q_q(1, 1, 0)^{'} &= Q_q(2k + 2, k + 1, k + 1) \\ &= (k + 1)I + (k + 1)J. \end{aligned}$$

Therefore,

$$GG' = I + Q_q(1, 0, 1,)Q_q(1, 0, 1)^{'} = I + Q_q(1, 1, 0)Q_q(1, 1, 0)^{'} = (k + 2)I + (k + 1)J$$

and $det(GG^{'}) = (k + 2)^{q-1}(k + 2 + q(k + 1)) \neq 0$ in $GF(l)$ if $p \nmid (k + 2), p \nmid (q + 1)(k + 1) + 1$. Hence, C is an LCD code.

□

Example 3.8. *Let $q = 7 = 3 + 4 \times 1$ and $l = 5$. Then $5 \nmid (k + 2), 5 \nmid (q + 1)(k + 1) + 1$ and the linear code with generator matrix*

$$G = [I|Q_5(1, 0, 1)] \text{ or } [I|Q_5(1, 1, 0)]$$

is a $[14, 7, 5]$ LCD code over $GF(5)$. It is a near to optimal code.

Theorem 3.9. *Let $q = 3 + 4k$ be an odd prime and $l = p^s$ for $s \geq 1$ and a prime p such that $p \nmid (k + 2)$ and $p \nmid (q + 1)k + 2$. Then a linear code C over $GF(l)$ with generator matrix $[I|Q_q(0, 0, 1)]$ or $[I|Q_q(0, 1, 0)]$ is an LCD code over $GF(l)$.*

Proof. By Lemma 2.1, we have

$$Q_q(0, 0, 1,)Q_q(0, 0, 1)^{'} = Q_q(0, 1, 0)Q_q(0, 1, 0)^{'} = Q_q(2k + 1, k, k) = (k + 1)I + kJ.$$

Therefore,

$$GG' = I + Q_q(0, 0, 1,)Q_q(0, 0, 1)^{'} = I + Q_q(0, 1, 0)Q_q(0, 1, 0)^{'} = (k + 2)I + kJ$$

and $det(GG^{'}) = (k + 2)^{q-1}(k + 2 + kq) \neq 0$ in $GF(l)$ if $p \nmid (k + 2), p \nmid (q + 1)k + 2$. Hence, C is an LCD code. □

Example 3.10. *Let $q = 3$ and $l = 5$. Then $5 \nmid (k+2), 5 \nmid (q+1)k+2$ and the linear code with generator matrix*

$$G = [I|Q_3(0, 1, 0)]$$

is a $[6, 3, 2]$ LCD code over $GF(5)$.

Example 3.11. *Let $q = 11$ and $l = 3$. Then $3 \nmid (k+2), 3 \nmid (q+1)k+2$ and the linear code with generator matrix*

$$G = [I|Q_{11}(0, 0, 1)]$$

is a $[22, 11, 6]$ LCD code over $GF(3)$.

The following result is associated with the construction (3) in which we consider A to be a matrix satisfying $AA^{'} = \delta_1 I$, for some $\delta_1 \in GF(l)$. In particular, we can also choose the circulant matrix A to be an orthogonal matrix.

Theorem 3.12. *Let C be a linear code over the finite field $GF(l)$ with the generator matrix $G = [A|Q_q(a,b,c)]$. If $Q_q(a,b,c)Q_q(a,b,c)^{'} = \delta_2 I$ for some $\delta_2 \in GF(l)$ and $\delta_1 \neq -\delta_2$, then C is an LCD code over $GF(l)$.*

Proof. Since $GG^{'} = AA^{'} + Q_q(a,b,c)Q_q(a,b,c)^{'} = (\delta_1 + \delta_2)I$, the result follows by Lemma 3.1. □

We can also choose A such that it does not satisfy the above mentioned condition and get the following results.

Theorem 3.13. *Let $q = 3 + 4k$ and C be a linear code over a finite field $GF(l)$ of characteristic p and the generator matrix of C be $G = [Q_q(1,0,1)|Q_q(0,1,1)]$ or $G = [Q_q(1,1,0)|Q_q(0,1,1)]$. If $p \nmid k+2$ and $p \mid q+k-1$, then C is an LCD code over $GF(l)$.*

Proof. Since

$$Q_q(0,1,1)Q_q(0,1,1)^{'} = Q_q(q-1,q-2,q-2) = I + (q-2)J$$

and

$$Q_q(1,0,1,)Q_q(1,0,1)^{'} = Q_q(1,1,0)Q_q(1,1,0)^{'} = (k+1)I + (k+1)J,$$

we have $GG' = (k+2)I + (q+k-1)J$. The result now follows using Lemma 3.1. □

Example 3.14. *Take $q = 7$ and $k = 1$, i.e., $p = 7$. Then $p \nmid k+2$ and $p \mid q+k-1 = 0$. Therefore, the linear codes with the generator matrix $G = [Q_q(1,0,1)|Q_q(0,1,1)]$ or $G = [Q_q(1,1,0)|Q_q(0,1,1)]$ are LCD codes over $GF(l)$. The parameters of both codes are $[14,7,4]$.*

Theorem 3.15. *Let $q = 3 + 4k$ and C be a linear code over a finite field $GF(l)$ of characteristic p and the generator matrix of C be $G = [Q_q(0,1,0)|Q_q(0,1,1)]$. If $p \nmid k+2$ and $p \nmid k(q+1) + q^2 - 2q + 2$, then C is an LCD code over $GF(l)$.*

Proof. Note that

$$Q_q(0,1,0)Q_q(0,1,0)^{'} = (k+1)I + kJ$$

and

$$Q_q(0,1,1)Q_q(0,1,1)^{'} = I + (q-2)J.$$

Then $GG' = (k+2)I + (k+q-2)J$ and $det(GG') = (k+2)^{q-1}(k(q+1) + q^2 - 2q + 2)$. The result now follows using Lemma 3.1. □

Example 3.16. *Take $q = 3$ and $k = 1$, i.e., $l = p = 7$. Then $p \nmid k+2$ and $p \nmid k(q+1) + q^2 - 2q + 2$. Therefore, the linear code with the generator matrix $G = [Q_q(0,1,0)|Q_q(0,1,1)]$ is an LCD code over $GF(l)$ with the parameters $[6,3,3]$.*

Now, we generalize the construction (2) to provide a new construction (4) of linear codes over a finite field of characteristic 2 and characterize LCD codes. Consider a linear code with the generator matrix of the form

$$G = \left[\begin{array}{c|c|c|c} \beta_1 & \beta_2 \cdots \beta_2 & \beta_3 & \beta_4 \cdots \beta_4 \\ \hline \beta_5 & & \beta_6 & \\ \vdots & Q_q(a,b,c) & \vdots & I \\ \beta_5 & & \beta_6 & \end{array}\right], \tag{4}$$

where $a, b, c, \beta_i \in GF(l)$ for $1 \leq i \leq 6$ and $l = 2^m$, $m \geq 1$. The linear code obtained from this construction is called *bordered quadratic double circulant code.*

Theorem 3.17. *Let C be a linear code over a finite field of characteristic 2, with the generator matrix G given in the construction (4). If*

1. $\Sigma_{i=1}^{4}\beta_i^2 = 1$,
2. $(\beta_5^2 + \beta_6^2)J + Q_q(a,b,c)Q_q(a,b,c)^{'} = O$ *and*
3. $\beta_1\beta_5 + \beta_2(a + b\lambda_q + c\lambda_q) + \beta_3\beta_6 + \beta_4 = 0$,

where $\lambda_q = \frac{q-1}{2}$, then C is a Euclidean LCD code of length $2q+2$. In particular, if $\beta_1 = 1$ and $\beta_4 = 0$ then C is a $[2q+2, q+1]$ code.

Proof. Let $B_1 = (\beta_1)$, $B_2 = (\beta_2\ \beta_2 \ldots \beta_2)$, $B_3 = (\beta_3)$, $B_4 = (\beta_4\ \beta_4 \ldots \beta_4)$, $B_5 = (\beta_5\ \beta_5 \ldots \beta_5)$ and $B_6 = (\beta_6\ \beta_6 \ldots \beta_6)$. Then G can be written as

$$G = \begin{bmatrix} B_1 & B_2 & B_3 & B_4 \\ B_5^{'} & Q_q(a,b,c) & B_6^{'} & I \end{bmatrix}$$

and $GG^{'}$ is

$$\begin{bmatrix} B_1B_1^{'} + B_2B_2^{'} + B_3B_3^{'} + B_4B_4^{'} & B_1B_5 + B_2Q_q(a,b,c)^{'} + B_3B_6 + B_4I \\ B_5^{'}B_1^{'} + Q_q(a,b,c)B_2^{'} + B_6^{'}B_3^{'} + IB_4^{'} & B_5^{'}B_5 + Q_q(a,b,c)Q_q(a,b,c)^{'} + B_6^{'}B_6 + I \end{bmatrix}.$$

Also,

$$B_1B_1^{'} + B_2B_2^{'} + B_3B_3^{'} + B_4B_4^{'} = \beta_1^2 + q\beta_2^2 + \beta_3^2 + q\beta_4^2,$$

$$B_5^{'}B_5 + Q_q(a,b,c)Q_q(a,b,c)^{'} + B_6^{'}B_6 + I = (\beta_5^2 + \beta_6^2)J + Q_q(a,b,c)Q_q(a,b,c)^{'} + I,$$

$$B_1B_5 + B_2Q_q(a,b,c)^{'} + B_3B_6 + B_4I = \begin{bmatrix} \beta_1\beta_5 + \beta_2(a + b\lambda_q + c\lambda_q) + \beta_3\beta_6 + \beta_4 \\ \vdots \\ \beta_1\beta_5 + \beta_2(a + b\lambda_q + c\lambda_q) + \beta_3\beta_6 + \beta_4 \end{bmatrix}^{'},$$

$$B_5^{'}B_1^{'} + Q_q(a,b,c)B_2^{'} + B_6^{'}B_3^{'} + IB_4^{'} = \begin{bmatrix} \beta_1\beta_5 + \beta_2(a + b\lambda_q + c\lambda_q) + \beta_3\beta_6 + \beta_4 \\ \vdots \\ \beta_1\beta_5 + \beta_2(a + b\lambda_q + c\lambda_q) + \beta_3\beta_6 + \beta_4 \end{bmatrix}.$$

Now, substituting the given conditions $(1-3)$ and using Lemma 3.1, we conclude that C is a Euclidean LCD code. □

Example 3.18. *Take $\beta_1 = \beta_6 = 1, \beta_2 = \beta_3 = \beta_4 = \beta_5 = 0$, $q = 5$ and $l = 4$. Then the linear code C with generator matrix given by construction (4) using $Q_q(1,1,1)$ is a $[12,6,1]$ Euclidean LCD code over $GF(4)$. Also, the dual of C is an LCD code with the parameters $[12,6,2]$.*

Example 3.19. *Take $\beta_1 = \beta_6 = 1, \beta_2 = \beta_3 = \beta_4 = \beta_5 = 0$, $q = 3$, $l = 4$ and $GF(l) = \mathbb{F}_2[w]$. Then the linear code C with generator matrix given by construction (4) using $Q_q(0, w, w^2)$ is a $[8,4,3]$ Euclidean LCD code over $GF(4)$. Moreover, it is a near to optimal code.*

Example 3.20. *Take* $\beta_1 = \beta_2 = \beta_5 = \beta_6 = 0, \beta_3 = \beta_4 = 1$, $q = 3$, $l = 2$ *and* $GF(2)$. *Then the linear code* C *with generator matrix given by construction* (4) *using* $Q_q(1,1,1)$ *is a* $[8,4,2]$ *Euclidean LCD code over* $GF(2)$.

Now, we characterize Hermitian LCD codes over $GF(l)$ (where $l = p^m$ such that m is even) from the linear codes associated with the three constructions (1), (3) and (4) provided earlier. We proceed with the assumption that m is an even positive integer whenever the Hermitian inner product is taken under consideration. It can be seen that a linear code over $GF(l)$ with the generator matrix $G = [I|Q_q(a,b,c)]$ given by construction (1) is a Hermitian LCD code if and only if $det(I + Q_q(a,b,c)Q_q(a,b,c)^*) \neq 0$. For the modified construction (3), we have the following result in which we consider A to be a matrix satisfying $AA^* = \delta_1 I$, for some $\delta_1 \in GF(l)$.

Theorem 3.21. *Let* C *be a linear code over a finite field* $GF(l)$ *with the generator matrix* $G = [A|Q_q(a,b,c)]$. *If* $Q_q(a,b,c)Q_q(a,b,c)^* = \delta_2 I$ *for some* $\delta_2 \in GF(l)$ *and* $\delta_1 \neq -\delta_2$, *then* C *is a Hermitian LCD code over* $GF(l)$.

Proof. Since $GG^* = AA^* + Q_q(a,b,c)Q_q(a,b,c)^* = (\delta_1 + \delta_2)I$, the result follows by Lemma 3.2. □

The following result provides some conditions under which linear code associated with construction (4) is a Hermitian LCD code.

Theorem 3.22. *Let* C *be a linear code over a finite field of characteristic* 2, *with the generator matrix* G *given in the construction* (4). *If*

1. $\Sigma_{i=1}^{4} \beta_i^{1+\sqrt{l}} = 1$,
2. $(\beta_5^{1+\sqrt{l}} + \beta_6^{1+\sqrt{l}})J + Q_q(a,b,c)Q_q(a,b,c)^* = O$,
3. $\beta_1\beta_5^{\sqrt{l}} + \beta_2(a^{\sqrt{l}} + \lambda_q b^{\sqrt{l}} + \lambda_q c^{\sqrt{l}}) + \beta_3\beta_6^{\sqrt{l}} + \beta_4 = 0$ *and*
4. $\beta_5\beta_1^{\sqrt{l}} + \beta_2^{\sqrt{l}}(a + \lambda_q b + \lambda_q c) + \beta_6\beta_3^{\sqrt{l}} + \beta_4^{\sqrt{l}} = 0$,

where $\lambda_q = \frac{q-1}{2}$, *then* C *is a Hermitian LCD code of length* $2q+2$. *In particular, if* $\beta_1 = 1$ *and* $\beta_4 = 0$, *then* C *is a* $[2q+2, q+1]$ *code.*

Proof. Let $B_1 = (\beta_1)$, $B_2 = (\beta_2\beta_2 \dots \beta_2)$, $B_3 = (\beta_3)$, $B_4 = (\beta_4 \dots \beta_4)$, $B_5 = (\beta_5 \dots \beta_5)$ and $B_6 = (\beta_6 \dots \beta_6)$. Then G can be written as

$$G = \begin{bmatrix} B_1 & B_2 & B_3 & B_4 \\ B_5' & Q_q(a,b,c) & B_6' & I \end{bmatrix}$$

and GG^* is

$$\begin{bmatrix} B_1B_1^* + B_2B_2^* + B_3B_3^* + B_4B_4^* & B_1(B_5')^* + B_2Q_q(a,b,c)^* + B_3(B_6')^* + B_4I \\ B_5'B_1^* + Q_q(a,b,c)B_2^* + B_6'B_3^* + IB_4^* & B_5'(B_5')^* + Q_q(a,b,c)Q_q(a,b,c)^* + B_6'(B_6')^* + I \end{bmatrix},$$

where

$$B_1B_1^* + B_2B_2^* + B_3B_3^* + B_4B_4^* = \beta_1^{1+\sqrt{l}} + q\beta_2^{1+\sqrt{l}} + \beta_3^{1+\sqrt{l}} + q\beta_4^{1+\sqrt{l}},$$

$$B_5'(B_5')^* + Q_q(a,b,c)Q_q(a,b,c)^* + B_6'(B_6')^* + I = (\beta_5^{1+\sqrt{l}} + \beta_6^{1+\sqrt{l}})J + Q_q(a,b,c)Q_q(a,b,c)^* + I,$$

$$B_1(B_5')^* + B_2Q_q(a,b,c)^* + B_3(B_6')^* + B_4I$$
$$= \begin{bmatrix} \beta_1\beta_5^{\sqrt{l}} + \beta_2(a^{\sqrt{l}} + \lambda_q b^{\sqrt{l}} + \lambda_q c^{\sqrt{l}}) + \beta_3\beta_6^{\sqrt{l}} + \beta_4 \\ \vdots \\ \beta_1\beta_5^{\sqrt{l}} + \beta_2(a^{\sqrt{l}} + \lambda_q b^{\sqrt{l}} + \lambda_q c^{\sqrt{l}}) + \beta_3\beta_6^{\sqrt{l}} + \beta_4 \end{bmatrix}'$$

and

$$B_5'B_1^* + Q_q(a,b,c)B_2^* + B_6'B_3^* + IB_4^* = \begin{bmatrix} \beta_5\beta_1^{\sqrt{l}} + \beta_2^{\sqrt{l}}(a + \lambda_q b + \lambda_q c) + \beta_6\beta_3^{\sqrt{l}} + \beta_4^{\sqrt{l}} \\ \vdots \\ \beta_5\beta_1^{\sqrt{l}} + \beta_2^{\sqrt{l}}(a + \lambda_q b + \lambda_q c) + \beta_6\beta_3^{\sqrt{l}} + \beta_4^{\sqrt{l}} \end{bmatrix}.$$

Now, substituting the given conditions $(1-4)$ and using Lemma 3.2, we conclude that C is a Hermitian LCD code. □

Example 3.23. *Take $\beta_1 = \beta_2 = \beta_3 = 1, \beta_4 = 2, \beta_5 = 1, \beta_6 = 2$. Then the linear code C with generator matrix given by construction (4) using $Q_5(1,1,2)$ is a Hermitian LCD code over $GF(4)$ with parameters $[12,6,4]$.*

Example 3.24. *Take $\beta_1 = 1, \beta_2 = 2, \beta_3 = 1, \beta_4 = 3, \beta_5 = 1, \beta_6 = 2$. Then the linear code C with generator matrix given by construction (4) using $Q_3(1,1,3)$ is a Hermitian LCD code over $GF(4)$ with parameters $[8,4,2]$.*

Using the generator matrices provided in construction (1), we obtain several double circulant codes (with the help of Magma computation system [3]) of length $2q$ over $GF(l)$ in Table 1. This way, we obtain double circulant codes over $GF(l)$ with the parameters $[2q, q, d]$. We denote the primitive element of the finite field $GF(l)$ by ω. In the fourth column, we represent a code with the maximum possible distance for a given length and dimension, i.e., optimal code (according to the Grassl table [12] available online) by $*$ and the code having distance one less than the maximum possible (i.e., near to optimal code) by $\#$. In the last column, we also mention their nature in terms of Euclidean or Hermitian LCD codes.

4. Conclusion

In this paper, we have studied LCD codes in terms of their generator matrices and presented several conditions for double circulant codes obtained from the constructions (1), (3) to be LCD. Moreover, we have provided a new modified construction for quadratic double circulant codes (bordered case) and characterized Euclidean and Hermitian LCD codes from them. Towards this, we have used the quadratic residue approach to obtain conditions for these codes derived from modified construction to be Euclidean and Hermitian LCD. Further, several optimal and near to optimal Euclidean and Hermitian LCD codes have been obtained from these constructions. The concepts of strongly regular graphs (SRGs) and doubly regular tournaments (DRTs) used in [8] to study LCD codes are very interesting. These can be used to obtain conditions for the linear codes obtained from our constructions to be LCD. Presently we leave it as an open problem for interested readers of this topic to explore in future.

Acknowledgment: The authors would like to thank the Indian Institute of Technology Patna for providing research facilities. We thank Prof. Patrick Solé (University Aix-Marseille, Marseille, France) for his careful reading and suggestions to improve results of this manuscript. Also, the authors would like to thank the anonymous referees and the Editor for their valuable comments to improve the presentation of the paper.

Table 1. Double circulant LCD codes with generator matrix $[I|Q_q(a,b,c)]$ of length $2q$ over $GF(l)$.

q	l	$Q_q(a,b,c)$	Parameters of C	Remark
7	2	$Q_7(1,1,0)$	$[14,7,3]_2^{\#}$	Euclidean LCD
5	2	$Q_5(0,0,1)$	$[10,5,3]_2^{\#}$	Euclidean LCD
7	3	$Q_7(0,2,1)$	$[14,7,5]_3^{\#}$	Euclidean LCD
5	3	$Q_5(1,2,2)$	$[10,5,4]_3^{\#}$	Euclidean LCD
3	3	$Q_3(0,1,1)$	$[6,3,3]_3^{*}$	Euclidean LCD
5	4	$Q_5(0,0,1)$	$[10,5,3]_4$	Hermitian LCD
7	4	$Q_7(1,\omega,\omega^2)$	$[14,7,5]_4^{\#}$	Hermitian LCD
7	4	$Q_7(0,1,\omega)$	$[14,7,6]_4^{*}$	Euclidean LCD
5	4	$Q_5(\omega,0,\omega^2)$	$[10,5,4]_4^{\#}$	Euclidean LCD
3	4	$Q_3(1,1,\omega)$	$[6,3,4]_4^{*}$	Euclidean LCD
7	5	$Q_7(0,1,4)$	$[14,7,6]_5^{*}$	Euclidean LCD
5	5	$Q_5(1,2,3)$	$[10,5,5]_5^{*}$	Euclidean LCD
3	5	$Q_3(1,1,2)$	$[6,3,4]_5^{*}$	Euclidean LCD
3	9	$Q_3(0,0,\omega^2)$	$[6,3,2]_9$	Hermitian LCD
5	9	$Q_5(0,0,2)$	$[10,5,3]_9$	Hermitian LCD
7	9	$Q_7(0,0,\omega)$	$[14,7,4]_9$	Hermitian LCD

References

[1] A. Alahmadi, A. Altassan, A. AlKenani, S. Çalkavur, H. Shoaib, P. Solé, A multisecret-sharing scheme based on LCD codes, Mathematics 8(2) (2020) 272–282.

[2] A. Alahmadi, F. Özdemir, P. Solé, On self-dual double circulant codes, Designs, Codes and Cryptography 86(6) (2018) 1257–1265.

[3] W. Bosma, J. Cannon, Handbook of magma functions, University of Sydney, Sydney, (1995).

[4] C. Carlet, S. Guilley, Complementary dual codes for counter-measures to side-channel attacks, Advances in Mathematics of Communications 10(1) (2016) 131–150.

[5] C. Carlet, S. Mesnager, C. Tang, Y. Qi, R. Pellikaan, Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$, IEEE Transactions on Information Theory 64(4) (2018) 3010–3017.

[6] J. Conan, G. Séguin, Structural properties and enumeration of quasi-cyclic codes, Applicable Algebra in Engineering, Communication and Computing 4(1) (1993) 25–39.

[7] D. Crnković, R. Egan, B. G. Rodrigues, A. Švob, LCD codes from weighing matrices, Applicable Algebra in Engineering, Communication and Computing 32(2) (2021) 175–189.

[8] D. Crnković, A. Grbac, A. Švob, Formally self-dual LCD codes from two-class association schemes, Applicable Algebra in Engineering, Communication and Computing 34 (2023) 183–200.

[9] S. T. Dougherty, J. L. Kim, P. Solé, Double circulant codes from two class association schemes, Advances in Mathematics of Communications 1(1) (2007) 45–64.

[10] P. Gaborit, Quadratic double circulant codes over fields, Journal of Combinatorial Theory, Series A 97(1) (2002) 85–107.

[11] J. Gildea, H. Hamilton, A. Kaya, B. Yildiz, Modified quadratic residue constructions and new extremal binary self-dual codes of length 64, 66 and 68, Information Processing Letters 157 (2020)

105927.
[12] M. Grassl, Table of bounds on linear codes, Online resource, available at: http://www.codetables.de/.
[13] C. Güneri, B. Özkaya, P. Solé, Quasi-cyclic complementary dual codes, Finite Fields and Their Applications 42 (2016) 67–80.
[14] D. Huang, M. Shi, P. Solé, Double circulant self-dual and LCD codes over $\mathbb{Z}_{p^2}$, International Journal of Foundations of Computer Science 30(03) (2019) 407–416.
[15] H. Islam, E. Martínez-Moro, O. Prakash, Cyclic codes over a non-chain ring $R_{e,q}$ and their application to LCD codes, Discrete Mathematics 344(10) (2021) 112545.
[16] K. Lally, P. Fitzpatrick, Algebraic structure of quasi-cyclic codes, Discrete Applied Mathematics 111(1-2) (2001) 157–175.
[17] C. Li, Hermitian LCD codes from cyclic codes, Designs, Codes and Cryptography 86(10) (2018) 2261–2278.
[18] S. Ling, P. Solé, On the algebraic structure of quasi-cyclic codes I: finite fields, IEEE Transactions on Information Theory 47(7) (2001) 2751–2760.
[19] S. Ling, P. Solé, On the algebraic structure of quasi-cyclic codes II: chain rings, Designs, Codes and Cryptography 30(1) (2003) 113–130.
[20] X. Liu, H. Liu, LCD codes over finite chain rings, Finite Fields and Their Applications 34 (2015) 1–19.
[21] Z. Liu, J. Wang, Further results on Euclidean and Hermitian linear complementary dual codes, Finite Fields and Their Applications 59 (2019) 104–133.
[22] Z. Liu, J. Wang, Linear complementary dual codes over rings, Designs, Codes and Cryptography 87(12) (2019) 3077–3086.
[23] J. L. Massey, Linear codes with complementary duals, Discrete Mathematics 106-107 (1992) 337–342.
[24] O. Prakash, S. Yadav, H. Islam, P. Solé, Self-dual and LCD double circulant codes over a class of non-local rings, Computational and Applied Mathematics 41(6) (2022) 1–16.
[25] O. Prakash, S. Yadav, R. K. Verma, Constacyclic and linear complementary dual codes over $\mathbb{F}_q+u\mathbb{F}_q$, Defence Science Journal 70(6) (2020) 626–632.
[26] N. Sendrier, Linear codes with complementary duals meet the Gilbert-Varshamov bound, Discrete Mathematics 285(1–3) (2004) 345–347.
[27] M. Shi, D. Huang, L. Sok, P. Solé, Double circulant LCD codes over $\mathbb{Z}_4$, Finite Fields and Their Applications 58 (2019) 133–144.
[28] M. Shi, D. Huang, L. Sok, P. Solé, Double circulant self-dual and LCD codes over Galois rings, Advances in Mathematics of Communications 13(1) (2019) 171–183.
[29] M. Shi, H. Zhu, L. Qian, L. Sok, P. Solé, On self-dual and LCD double circulant and double negacirculant codes over $\mathbb{F}_q + u\mathbb{F}_q$, Cryptography and Communications 12(1) (2020) 53–70.
[30] L. Sok, On Hermitian LCD codes and their Gray image, Finite Fields and Their Applications 62 (2020) 101623.
[31] S. Yadav, H. Islam, O. Prakash, P. Solé, Self-dual and LCD double circulant and double negacirculant codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$, Journal of Applied Mathematics and Computing 67(1–2) (2021) 689–705.
[32] X. Yang, J. L. Massey, The condition for a cyclic code to have a complementary dual, Discrete Mathematics 126(1–3) (1994) 391–393.
[33] T. Yao, S. Zhu, X. Kai, On self-dual and LCD double circulant codes over a non-chain ring, Chinese Journal of Electronics 28(5) (2019) 1018–1024.
[34] H. Zhu, M. Shi, On linear complementary dual four circulant codes, Bulletin of the Australian Mathematical Society 98(1) (2018) 159–166.