Open access • Journal Article • DOI:10.1007/S12190-021-01499-9

Self-dual and LCD double circulant and double negacirculant codes over $\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q$ — Source link

Shikha Yadav, Habibul Islam, Om Prakash, Patrick Solé

Institutions: Indian Institute of Technology Patna, Aix-Marseille University

Published on: 25 Jan 2021 - Journal of Applied Mathematics and Computing (Springer Berlin Heidelberg)

Topics: Circulant matrix

Self-dual and LCD double circulant and double negacirculant codes over $F\_\_q + uF\_\_q + vF\_\_q$

Shikha Yadav, Habibul Islam, Om Prakash, Patrick Solé

J. Appl. Math. Comput. manuscript No.
(will be inserted by the editor)

Self-dual and LCD double circulant and double negacirculant codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$

Shikha Yadav · Habibul Islam · Om Prakash · Patrick Solé

Received: date / Accepted: date

Abstract Let q be an odd prime power, and denote by $\mathbb{F}_q$ the finite field with q elements. In this paper, we consider the ring $R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$, where $u^2 = u, v^2 = v, uv = vu = 0$ and study double circulant and double negacirculant codes over this ring. We first obtain the necessary and sufficient conditions for a double circulant code to be self-dual (resp. LCD). Then we enumerate self-dual and LCD double circulant and double negacirculant codes over R. Last but not the least, we show that the family of Gray images of self-dual and LCD double circulant codes over R are good. Several numerical examples of self-dual and LCD codes over $\mathbb{F}_5$ as the Gray images of these codes over R are given in short lengths.

Keywords Double circulant code · Self-dual code · LCD code · Gray map

Mathematics Subject Classification (2000) 94B05 · 94B15 · 94B35 · 94B60

1 Introduction

Cyclic codes are one of the oldest family of block codes. They have received very intensive attention during the last six decades [6]. In that period, several studies have shown their important uses in and out of mathematics. Many times, they have appeared through their generalized classes [4,14, 15,25] and have produced lots of good codes. Along with some other classes, namely, constacyclic, skew cyclic etc., quasi-cyclic codes have led to record-breaking codes [8,9]. Recall that a linear code is said to be a quasi-cyclic code of index l, if it is invariant under T^l, where T denotes the cyclic shift operator. In particular, a quasi-cyclic code of index 1 is indeed a cyclic code. In 2001, Ling and Solé [17] presented a new approach to study quasi-cyclic codes over finite fields. They regarded quasi-cyclic codes over a finite field F as linear codes of length l over the polynomial ring $R(F, m) = F[x]/(x^m - 1)$ where $m = \frac{n}{l}$. Essential to that approach was the decomposition of $R(F, m)$ into local rings via the Chinese Remainder Theorem for polynomials. Later, in 2003, they extended their study to the case when F is itself a chain ring [18]. In 2016, Guneri et al. [7] have shown that quasi-cyclic codes include families of good LCD codes. Double circulant codes are particular types of quasi-cyclic codes having index 2. In 2018, Alahmadi et al. [2] have shown the self-dual double circulant codes of odd dimension to be dihedral or constadihedral depending upon the characteristic of the field. Meanwhile, self-dual negacirculant codes over finite fields were studied in [1]. To generalize the concept over finite rings, recently, Shi et al. [21] considered the finite commutative semi-local non-chain ring $\mathbb{F}_q + u\mathbb{F}_q$, $u^2 = u$ and studied double circulant self-dual or LCD codes. They first enumerated these codes for self-dual and LCD codes, respectively, and later obtained distance bounds on them. A similar work has been reported over a semi-local non-chain ring $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$, where $u^3 = u$ in [28]. On the other

Shikha Yadav
Habibul Islam
Om Prakash
Department of Mathematics
Indian Institute of Technology Patna, Patna 801 106, India
E-mail: 1821ma10@iitp.ac.in, habibul.pma17@iitp.ac.in,om@iitp.ac.in

Patrick Solé
I2M, (CNRS, Aix-Marseille University, Centrale Marseille)
Marseilles, France
E-mail: sole@enst.fr

side, double circulant LCD codes over $\mathbb{Z}_4$ in [22], $\mathbb{Z}_{p^2}$ in [10] and Galois ring in [23] were studied, respectively. Further, for some related studies on these topics, interested readers can see [20, 24, 26, 27, 29]. Therefore, because of available works on non-chain rings [21, 28], it is logical to investigate these codes over other semi-local non-chain rings. Motivated by the above studies, here we consider the finite commutative semi-local non-chain ring $R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$, where $u^2 = u, v^2 = v, uv = vu = 0$. In fact, we first determine the necessary and sufficient conditions (Lemma 1) of double circulant codes to be self-dual and LCD. Then we enumerate self-dual and LCD double circulant codes of length $2n$ over R when n is odd and double negacirculant codes when n is even, respectively. Finally, by taking Gray images of such codes we show that both families are good in terms of distance bounds (Theorem 2). It is worth mentioning that the ring R has an important interest and several classes of codes were considered over it [3, 12, 13] in the literature.

The paper is organized as follows: Section 2 contains some basic definitions and Gray maps. In Section 3, we study the structure of double circulant and double negacirculant codes over R and enumerate self-dual and LCD double circulant and double negacirculant codes. Section 4 provides the distance bounds and establishes that the families of Gray images of self-dual double circulant codes, and LCD double circulant codes over R are good. In Section 5, we present several non-trivial examples of self-dual and LCD codes over $\mathbb{F}_5$ from the Gray images of these codes over R. Section 6 concludes the paper.

2 Preliminary

Let q be an odd prime power such that there exists $\omega \in \mathbb{F}_q$ with $\omega^2 = -1$ (for the existence of such element see [18]) . Throughout, we fix $R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$, $u^2 = u, v^2 = v, uv = vu = 0$. Now, following [3, 12], we recall that R is a semi-local non-chain ring with three maximal ideals $\langle 1 - u\rangle, \langle 1 - v\rangle$ and $\langle u + v\rangle$. Again, by applying the Chinese Remainder Theorem (CRT) decomposition, we can write $R \cong (1 - u - v)\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$. Hence, an arbitrary element $r \in R$ has a unique representation $r = (1-u-v)r_1 + ur_2 + vr_3$, where $r_1, r_2, r_3 \in \mathbb{F}_q$. Further, R has $(q-1)^3$ units and $q^3 - (q-1)^3$ non-unit elements where the set of units is calculated by the fact that r is a unit in R if and only if r_1, r_2, r_3 are non-zero in $\mathbb{F}_q$. Now, we define a Gray map $\phi_1 : R \to \mathbb{F}_q^3$ by $\phi_1(a + ub + vc) = (-b, 2a + b, c)$, for all $a, b, c \in \mathbb{F}_q$. In addition, we consider another Gray map $\phi_2 : R \to \mathbb{F}_q^3$ defined in [12] by $\phi_2(a + ub + vc) = (a, a + b, a + c)$, for all $a, b, c \in \mathbb{F}_q$. It is evident to check that ϕ_i is an $\mathbb{F}_q$-linear bijective map and can be naturally extended over R^n. In later portion, we show that these Gray maps preserve the orthogonality of a linear code, and hence carry Euclidean LCD and self-dual codes from R to $\mathbb{F}_q$.

A *linear code* C of length n over R is an R-submodule of R^n. The *Hamming weight* $w_H(c)$ of a vector $c = (c_0, c_1, \dots, c_{n-1}) \in R^n$ is the number of non-zero coordinates while the minimum Hamming distance of the code C is

$$d_H(C) = \min\{w_H(c) : 0 \neq c \in C\}.$$

Now, we define the Lee weight $w_L(c)$ of a vector $c = (c_0, c_1, \dots, c_{n-1}) \in R^n$ as $w_L(c) = w_H(\phi_i(c))$ while the minimum Lee distance of C is given by

$$d_L(C) = \min\{w_L(c) : 0 \neq c \in C\}.$$

Therefore, it is checked that ϕ_i is a linear isometric map from (R^n, d_L) to $(\mathbb{F}_q^{3n}, d_H)$ for $i = 1, 2$. For any two elements $s = (s_0, s_1, \dots, s_{n-1})$ and $t = (t_0, t_1, \dots, t_{n-1})$ in R^n, their *Euclidean* (resp. *Hermitian*) *inner product* is defined by

$$s \cdot t = \sum_{i=0}^{n-1} s_i t_i$$

and

$$\langle s, t\rangle_H = \sum_{i=0}^{n-1} s_i \bar{t}_i,$$

respectively, where for $x + uy + vz \in R$ its conjugate is defined by $\overline{x + uy + vz} = x^{\sqrt{q}} + uy^{\sqrt{q}} + vz^{\sqrt{q}}$. In this way, the Euclidean (resp. Hermitian) dual of a linear code C is denoted by $C^{\perp}$ (resp. $C^{\perp_H}$) and defined by

$$C^{\perp} = \{a \in R^n : a \cdot c = 0 \text{ for all } c \text{ in } C\}$$

and

$$C^{\perp_H} = \{a \in R^n : \langle a, c\rangle_H = 0 \text{ for all } c \text{ in } C\},$$

respectively. A linear code C is said to be a *Euclidean* (resp. *Hermitian*) *LCD code* if and only if $C \cap C^{\perp} = \{0\}$ (resp. $C \cap C^{\perp_H} = \{0\}$). Also, C is said to be a *Euclidean* (resp. *Hermitian*) *self-dual code* if $C = C^{\perp}$ (resp. $C = C^{\perp_H}$). Now, the next result shows that ϕ_i preserve the orthogonality of a linear code.

Theorem 1 *Let C be a linear code over R. Then C is a Euclidean LCD (resp. self-dual) code if and only if $\phi_i(C)$ is a Euclidean LCD (resp. self-dual) code over $\mathbb{F}_q$ for $i = 1, 2$.*

Proof The proof depends on the main fact $\phi_i(C^{\perp}) = (\phi_i(C))^{\perp}$, which can be verified by using the similar procedure of [[21], Theorem 2.2].

For solving the nonlinear equations in Theorem 3, we use the concept of norm functions which is defined as $Norm : \mathbb{F}_{q^n} \to \mathbb{F}_q$ given by

$$Norm(x) = x^{\frac{q^n-1}{q-1}}, \quad \text{for } x \in \mathbb{F}_{q^n}.$$

Then $Norm$ is a multiplicative surjective function and $Norm(0) = 0$. Further, each element in $\mathbb{F}_q^*$ is a norm of exactly $\frac{q^n-1}{q-1}$ elements in $\mathbb{F}_{q^n}^*$ (see [16], Theorem 2.28). Now, we recall that a linear code is said to be a *double circulant* (resp. *negacirculant*) *code*, if its generator matrix is of the form

$$G = (I, A)$$

where A is a circulant (resp. negacirculant) matrix, i.e., the matrix whose rows can be obtained by successive circular shifts (resp. negashifts) of the first row. Let $C_{<n>}$ be a family of codes having parameters $[n, k_n, d_n]$ over $\mathbb{F}_q$. Then the *rate* ρ and *relative distance* δ are defined as $\rho = \limsup\limits_{n\to\infty} \frac{k_n}{n}$ and $\delta = \limsup\limits_{n\to\infty} \frac{d_n}{n}$. This family is said to be *good* , if $\rho\delta \neq 0$. To derive the main result which proposes that the Gray images of a subfamily of double circulant (LCD or self dual) codes over R are good (Theorem 2), we will use the entropy function [11] defined by

$$H_q(x) = \begin{cases} 0, & \text{if } x = 0 \\ x\log_q(q-1) - x\log_q(x) - (1-x)\log_q(1-x), & \text{if } 0 < x \le 1 - \frac{1}{q} \end{cases}.$$

Now, we state one of the main result of this paper, and prove it at the end of Section 4.

Theorem 2 *Let q be an odd prime power, and $\delta > 0$ be given. Then there are families of double circulant self-dual (resp. LCD) codes of length $2n$ over R, with code rate $\frac{1}{2}$, and with Gray images of relative distance δ as long as $H_q(\delta) < \frac{1}{12}$ (resp. $H_q(\delta) < \frac{1}{6}$). Moreover, we conclude that both of these families of codes are good.*

Remark: This result shows that for all $\epsilon > 0$ arbitrarily small there are families of the said types of relative distance $\delta_0 - \epsilon$, with $H_q(\delta_0) = \frac{1}{12}$ (resp. $H_q(\delta_0) = \frac{1}{6}$). Unfortunately, the method does not allow us to make $\epsilon = 0$.

3 Double circulant and double negacirculant codes

In this section, we enumerate self-dual and LCD double circulant codes over R. For this, we first obtain the necessary and sufficient conditions of double circulant codes to be self-dual or LCD. Further, the enumeration of self-dual and LCD double negacirculant codes is provided.

3.1 Enumeration of double circulant codes when n is odd

We assume that n is an odd positive integer and the factorization of $x^n - 1$ into distinct irreducible polynomials over R is as follows:

$$x^n - 1 = a(x-1)\prod_{i=2}^{s} g_i(x)\prod_{j=1}^{t} h_j(x)h_j^*(x),$$

where

- $a \in R^*$ where R^* denotes the set of all units in R,
- $g_i(x)$ $(2 \leq i \leq s)$ are self-reciprocal polynomials of even degree $2e_i$, respectively,
- $h_j^*(x)$ $(1 \leq j \leq t)$ are reciprocal polynomials of $h_j(x)$ with degree d_j, respectively.

By the Chinese Remainder Theorem (CRT), we have

$$\begin{aligned}\frac{R[x]}{\langle x^n-1\rangle} \cong & \frac{R[x]}{\langle x-1\rangle} \oplus \left(\oplus_{i=2}^{s} \frac{R[x]}{\langle g_i(x)\rangle}\right) \oplus \left(\oplus_{j=1}^{t} \left(\frac{R[x]}{\langle h_j(x)\rangle}\right) \oplus \left(\frac{R[x]}{\langle h_j^*(x)\rangle}\right)\right)\\ \cong & R \oplus (\oplus_{i=2}^{s} R_{2e_i}) \oplus (\oplus_{j=1}^{t} R_{d_j} \oplus R_{d_j}),\end{aligned}$$

where $R_r = \mathbb{F}_{q^r} + u\mathbb{F}_{q^r} + v\mathbb{F}_{q^r}$, $u^2 = u, v^2 = v, uv = vu = 0$ for $r = 2e_i$ or d_j. The above decomposition can be naturally extended as

$$\left(\frac{R[x]}{\langle x^n-1\rangle}\right)^2 \cong R^2 \oplus \left(\oplus_{i=2}^{s} (R_{2e_i})^2\right) \oplus \left(\oplus_{j=1}^{t} (R_{d_j})^2 \oplus (R_{d_j})^2\right).$$

Now, using this decomposition, any linear code C of length 2 over $\frac{R[x]}{\langle x^n-1\rangle}$ can be decomposed as

$$C \cong C_1 \oplus (\oplus_{i=2}^{s} C_i) \oplus \left(\oplus_{j=1}^{t} (C_j^{'} \oplus C_j^{''})\right) \tag{1}$$

where C_1 is a linear code over R, C_i is a linear code over R_{2e_i}, for $2 \leq i \leq s$ and $C_j^{'}, C_j^{''}$ are linear codes over R_{d_j}, for $1 \leq j \leq t$.

Lemma 1 *Let C be a double circulant code over R given in the CRT decomposition (1) and $\alpha_1 = (1, c_{e_1}), \alpha_i = (1, c_{e_i}), \alpha_j^{'} = (1, c_{d_j}^{'}), \alpha_j^{''} = (1, c_{d_j}^{''})$ be generators of the constituent codes $C_1, C_i, C_j^{'}, C_j^{''}$ over R, R_{2e_i}, R_{d_j} and R_{d_j}, respectively, for $2 \leq i \leq s$, $1 \leq j \leq t$. Then*

(1) C is a self-dual code if and only if $1 + c_{e_1}^2 = 0$, $1 + c_{e_i}^{1+q^{e_i}} = 0$ and $1 + c_{d_j}^{'} c_{d_j}^{''} = 0$.

(2) C is a Euclidean LCD code if and only if $1 + c_{e_1}^2 \in R^*$, $1 + c_{e_i}^{1+q^{e_i}} \in R_{2e_i}^*$ and $1 + c_{d_j}^{'} c_{d_j}^{''} \in R_{d_j}^*$.

Proof Let C be a double circulant code over R given by the CRT decomposition (1). By following the same procedure of [[18], Theorem 4.2], we get that C is a self-dual code if and only if C_1, C_i are self-dual codes with respect to the Euclidean, Hermitian inner product, respectively for $2 \leq i \leq s$ and $C_j^{''}$ is the dual code of $C_j^{'}$ with respect to Euclidean inner product, for $1 \leq j \leq t$. In our case, it further implies that C is a self-dual code if and only if $1 + c_{e_1}^2 = 0$, $1 + c_{e_i}^{1+q^{e_i}} = 0$ and $1 + c_{d_j}^{'} c_{d_j}^{''} = 0$.

Now, following the same method of [[7], Theorem 3.1], we get C is an LCD code if and only if C_1, C_i are LCD codes with respect to the Euclidean, Hermitian inner product, respectively for $2 \leq i \leq s$ and $(C_j^{''})^{\perp} \cap C_j^{'} = \{0\}$, $C_j^{''} \cap (C_j^{'})^{\perp} = \{0\}$, for $1 \leq j \leq t$. In our case, it further implies that C is a Euclidean LCD code if and only if $1 + c_{e_1}^2 \in R^*$, $1 + c_{e_i}^{1+q^{e_i}} \in R_{2e_i}^*$ and $1 + c_{d_j}^{'} c_{d_j}^{''} \in R_{d_j}^*$.

Using the necessary and sufficient conditions given in Lemma 1, we now find the total number of self-dual or LCD double circulant codes over R in the following results.

Theorem 3 *Assume that for an odd integer n, the factorization of $x^n - 1$ over R is*

$$x^n - 1 = a(x-1) \prod_{i=2}^{s} g_i(x) \prod_{j=1}^{t} h_j(x) h_j^*(x),$$

where $a \in R^*$ and $n = 1 + \Sigma_{i=2}^{s} 2e_i + 2\Sigma_{j=1}^{t} d_j$. Then the total number of self-dual double circulant codes over R is

$$8 \prod_{i=2}^{s} (q^{e_i} + 1)^3 \prod_{j=1}^{t} (q^{d_j} - 1)^3.$$

Proof We can obtain the total number of self-dual double circulant codes by just counting the constituent codes. There are 8 choices for C_1 which have the generator polynomials as $(1, \omega)$, $(1, -\omega)$, $(1, \omega(1-2v))$, $(1, \omega(2v-1))$, $(1, \omega(1-2u))$, $(1, \omega(2u-1))$, $(1, \omega(1-2u-2v))$ and $(1, \omega(-1+2u+2v))$, respectively, where $\omega^2 = -1$.

For the second constituent codes, to count self-dual codes with respect to the Hermitian inner product, we need to find the number of solutions of the equation $1 + c_{e_i} c_{e_i}^{q^{e_i}} = 0$. Let $c_{e_i} = x(1-u-v) + yu + zv$, for some $x, y, z \in \mathbb{F}_{q^{2e_i}}$. Then

$$1 + (x(1-u-v) + yu + zv)(x(1-u-v) + yu + zv)^{q^{e_i}} = 0$$

if and only if

$$xx^{q^{e_i}} = -1, yy^{q^{e_i}} = xx^{q^{e_i}} = -1 \text{ and } zz^{q^{e_i}} = xx^{q^{e_i}} = -1$$

i.e., $Norm(x) = -1, Norm(y) = -1$ and $Norm(z) = -1$. There are $q^{e_i} + 1$ solutions for each $Norm(x) = -1$, $Norm(y) = -1$ and $Norm(z) = -1$, respectively. Therefore, the total number of solutions for the above system is $(q^{e_i} + 1)^3$.

Now, we count the dual pairs (w.r.t. Euclidean inner product) of codes. For this, we need to find the number of solutions of the equation $1 + c^{'}_{d_j} c^{''}_{d_j} = 0$. We have the following possibilities:

- If $c^{'}_{d_j} \in R^*_{d_j}$, then $c^{''}_{d_j} = -\frac{1}{c^{'}_{d_j}}$ and we have $|R^*_{d_j}| = (q^{d_j} - 1)^3$ choices for the pair $\{c^{'}_{d_j}, c^{''}_{d_j}\}$.
- If $c^{'}_{d_j} \in R_{d_j} \setminus R^*_{d_j}$, then $c^{'}_{d_j} = x(1 - u - v) + yu + zv$, for some $x, y, z \in \mathbb{F}_{q^{d_j}}$ and at least one of x, y or z is 0. For $c^{''}_{d_j} = \beta_1(1 - u - v) + \beta_2 u + \beta_3 v \in R_{d_j}$, where $\beta_1, \beta_2, \beta_3 \in \mathbb{F}_{q^{d_j}}$, we have

  $$1 + c^{'}_{d_j} c^{''}_{d_j} = (1 + x\beta_1) + (y\beta_2 - x\beta_1)u + (z\beta_3 - x\beta_1)v = 0,$$

  which implies that $x\beta_1 = -1, y\beta_2 = -1, z\beta_3 = -1$. If any one of x, y or z is 0, then we get $-1 = 0$, a contradiction. Therefore, these cases doesn't occur.

Hence, we have $(q^{d_j} - 1)^3$ choices for the dual pairs. Combining above all cases we get the desired result.

With the same notations used in the above theorem, we now count the total number of LCD double circulant codes over R.

Theorem 4 *The total number of LCD double circulant codes over R is*

$$(q-2)^3 \prod_{i=2}^{s} (q^{2e_i} - q^{e_i} - 1)^3 \prod_{j=1}^{t} (q^{6d_j} - 3q^{5d_j} + 6q^{4d_j} - 7q^{3d_j} + 6q^{2d_j} - 3q^{d_j} + 1).$$

Proof We can obtain the total number of LCD double circulant codes by just counting the constituent codes as done for the self-dual codes. If C_1 is an LCD code with respect to the Euclidean inner product, then $1 + c^2_{e_1} \in R^*$ and we have the following possibilities:

- If $c_1 = 0$, then $1 + c_1^2 = 1 \in R^*$.
- If $0 \neq c_1 \in \langle 1-u-v \rangle$ and $c_1 = x(1-u-v)$, for some $x \in \mathbb{F}_q^*$, then $1+c_1^2 = 1+x^2(1-u-v) \in R^*$ if and only if $x \neq \pm\omega$, where $\omega^2 = -1$. Therefore, we have $q-3$ choices. Similarly, when $0 \neq c_1 \in \langle u \rangle$ or $\langle v \rangle$, we have $q - 3$ choices for each.
- If $0 \neq c_1 \in \langle 1 - u - v, u \rangle$ and $c_1 = x(1 - u - v) + yu$, for some $x, y \in \mathbb{F}_q^*$, then $1 + c_1^2 = 1 + x^2(1 - u - v) + y^2 u \in R^*$ if and only if $x \neq \pm\omega$ and $y \neq \pm\omega$, where $\omega^2 = -1$. Therefore, we have $(q-3)^2$ choices. Similarly, when $0 \neq c_1 \in \langle u, v \rangle$ or$\langle 1 - u - v, v \rangle$, we have $(q-3)^2$ choices for each.
- If $0 \neq c_1 \in \langle 1 - u - v, u, v \rangle$ and $c_1 = x(1 - u - v) + yu + zv$, for some $x, y, z \in \mathbb{F}_q^*$, then $1+c_1^2 = 1+x^2(1-u-v)+y^2u+z^2v \in R^*$ if and only if $x, y, z \neq \pm\omega$, where $\omega^2 = -1$. Therefore, we have $(q-3)^3$ choices.

So, we have $1 + 3(q-3) + 3(q-3)^2 + (q-3)^3 = (q-2)^3$ choices for C_1.

Now, we find the choices for C_{e_i} such that it is an LCD code over R_{2e_i} with respect to the Hermitian inner product. The linear code C_{e_i} is Hermitian LCD if $1 + c_{e_i}^{1+q^{e_i}} \in R^*_{2e_i}$ and we have the following possibilities:

- If $c_{e_i} = 0$, then $1 + c_{e_i}^{1+q^{e_i}} = 1 \in R^*_{2e_i}$.
- If $0 \neq c_{e_i} \in \langle 1-u-v \rangle$ and $c_{e_i} = x(1-u-v)$, for some $x \in \mathbb{F}^*_{q^{2e_i}}$, then $1+c_{e_i}^{1+q^{e_i}} = 1+x^{1+q^{e_i}}(1-u-v) \in R^*_{2e_i}$ if and only if $x^{1+q^{e_i}} \neq -1$. Therefore, we have $q^{2e_i} - q^{e_i} - 2$ choices. Similarly, when $0 \neq c_{e_i} \in \langle u \rangle$ or $\langle v \rangle$, we have $q^{2e_i} - q^{e_i} - 2$ choices for each.
- If $0 \neq c_{e_i} \in \langle 1 - u - v, u \rangle$ and $c_{e_i} = x(1 - u - v) + yu$, for some $x, y \in \mathbb{F}^*_{q^{2e_i}}$, then $1 + c_{e_i}^{1+q^{e_i}} = 1 + x^{1+q^{e_i}}(1 - u - v) + y^{1+q^{e_i}} u \in R^*_{2e_i}$ if and only if $x^{1+q^{e_i}} \neq -1$ and $y^{1+q^{e_i}} \neq -1$. Therefore, we have $(q^{2e_i} - q^{e_i} - 2)^2$ choices. Similarly, when $0 \neq c_{e_i} \in \langle u, v \rangle$ or $\langle 1 - u - v, v \rangle$, we have $(q^{2e_i} - q^{e_i} - 2)^2$ choices for each.
- If $0 \neq c_{e_i} \in \langle 1 - u - v, u, v \rangle$ and $c_{e_i} = x(1 - u - v) + yu + zv$, for some $x, y, z \in \mathbb{F}^*_{q^{2e_i}}$, then $1+c_{e_i}^{1+q^{e_i}} = 1+x^{1+q^{e_i}}(1-u-v)+y^{1+q^{e_i}}u+z^{1+q^{e_i}}v \in R^*_{2e_i}$ if and only if $x^{1+q^{e_i}} \neq -1, y^{1+q^{e_i}} \neq -1$ and $z^{1+q^{e_i}} \neq -1$. Therefore, we have $(q^{2e_i} - q^{e_i} - 2)^3$ choices.

So, in this case, we have $1+3(q^{2e_i}-q^{e_i}-2)+3(q^{2e_i}-q^{e_i}-2)^2+(q^{2e_i}-q^{e_i}-2)^3=(q^{2e_i}-q^{e_i}-1)^3$ choices for C_i, where $2 \leq i \leq s$.

Now, for the last case we need to find choices for the pairs $\{c^{'}_{d_j}, c^{''}_{d_j}\}$ such that $1+c^{'}_{d_j}c^{''}_{d_j} \in R^*_{d_j}$ and we have the following possibilities:

- If $c^{'}_{d_j}=0$, then $1+c^{'}_{d_j}c^{''}_{d_j} \in R^*_{d_j}$ for any $c^{''}_{d_j} \in R^*_{d_j}$. So, we have q^{3d_j} choices for $c^{''}_{d_j}$.
- If $c^{'}_{d_j} \in R^*_{d_j}$ then $c^{''}_{d_j} \in R^*_{d_j} - \frac{1}{c^{'}_{d_j}}$ and $|R^*_{d_j} - \frac{1}{c^{'}_{d_j}}| = |R^*_{d_j}|$. We have $|R^*_{d_j}|^2 = (q^{d_j}-1)^6$ choices for the pairs $\{c^{'}_{d_j}, c^{''}_{d_j}\}$.
- If $0 \neq c^{'}_{d_j} \in \langle 1-u-v \rangle$ and $c^{'}_{d_j} = x(1-u-v)$, for some $x \in \mathbb{F}^*_{q^{d_j}}$. Assume that $c^{''}_{d_j} = \beta_1(1-u-v)+\beta_2 u+\beta_3 v$, for some $\beta_1, \beta_2, \beta_3 \in \mathbb{F}_{q^{d_j}}$. Then $1+c^{'}_{d_j}c^{''}_{d_j} = 1+x\beta_1(1-u-v) \in R^*_{d_j}$ if and only if $x\beta_1 \neq -1$. Therefore, we have $(q^{d_j}-1)^2q^{2d_j}$ choices. Similarly, when $0 \neq c_{e_i} \in \langle u \rangle$ or $\langle v \rangle$, we have $(q^{d_j}-1)^2q^{2d_j}$ choices for each.
- If $0 \neq c^{'}_{d_j} \in \langle 1-u-v, u \rangle$ and $c^{'}_{d_j} = x(1-u-v)+yu$, for some $x, y \in \mathbb{F}^*_{q^{d_j}}$. Assume that $c^{''}_{d_j} = \beta_1(1-u-v)+\beta_2 u+\beta_3 v$, for some $\beta_1, \beta_2, \beta_3 \in \mathbb{F}_{q^{d_j}}$ Then $1+c^{'}_{d_j}c^{''}_{d_j} = 1+x\beta_1(1-u-v)+y\beta_2 u \in R^*_{d_j}$ if and only if $x\beta_1 \neq -1$ and $y\beta_2 \neq -1$. Therefore, we have $(q^{d_j}-1)^4q^{d_j}$ choices. Similarly, when $0 \neq c^{'}_{d_j} \in \langle u, v \rangle$ or $\langle 1-u-v, v \rangle$, we have $(q^{d_j}-1)^4q^{d_j}$ choices for each.

In this case, we have $q^{3d_j}+(q^{d_j}-1)^6+3(q^{d_j}-1)^2q^{2d_j}+3(q^{d_j}-1)^4q^{d_j} = (q^{6d_j}-3q^{5d_j}+6q^{4d_j}-7q^{3d_j}+6q^{2d_j}-3q^{d_j}+1)$ choices for the pairs $\{C^{'}_j, C^{''}_j\}$, where $1 \leq j \leq t$. Now, summing all these above choices we get the required result.

3.2 Enumeration of double negacirculant codes when n is even

The present subsection deals with the enumeration of self-dual or LCD double negacirculant codes over R. Here, we take n to be an even positive integer such that $gcd(n,q)=1$. We assume that the factorization of x^n+1 into distinct irreducible polynomials over R is as follows:

$$x^n+1 = a\prod_{i=1}^{s} g_i(x) \prod_{j=1}^{t} h_j(x)h_j^*(x),$$

where $a \in R^*$, $g_i(x)$ $(1 \leq i \leq s)$ are self-reciprocal polynomials of even degree $2e_i$ and $h_j^*(x)$ $(1 \leq j \leq t)$ are reciprocal polynomials of $h_j(x)$ with degree d_j, respectively. Using the arguments similar to double circulant codes, we get

$$\frac{R[x]}{\langle x^n+1 \rangle} \cong (\oplus_{i=1}^{s} R_{2e_i}) \oplus \left(\oplus_{j=1}^{t} R_{d_j} \oplus R_{d_j}\right),$$

where $R_r = \mathbb{F}_{q^r}+u\mathbb{F}_{q^r}+v\mathbb{F}_{q^r}$, $u^2=u, v^2=v, uv=vu=0$ for $r=2e_i$ or d_j. Also, any linear code C of length 2 can be written as

$$C \cong (\oplus_{i=1}^{s} C_i) \oplus \left(\oplus_{j=1}^{t}(C^{'}_j \oplus C^{''}_j)\right), \tag{2}$$

where C_i is a linear code over R_{2e_i}, for $1 \leq i \leq s$ and $C^{'}_j, C^{''}_j$ are linear codes over R_{d_j}, for $1 \leq j \leq t$. To enumerate the self-dual and LCD double negacirculant codes, we need the following result which can be proved using the same procedure of Lemma 1.

Lemma 2 *Let C be a double negacirculant code over R and $\alpha_i = (1, c_{e_i}), \alpha^{'}_j = (1, c^{'}_{d_j}), \alpha^{''}_j = (1, c^{''}_{d_j})$ be generators of the constituent codes $C_i, C^{'}_j, C^{''}_j$ over R_{2e_i}, R_{d_j} and R_{d_j}, respectively, for $1 \leq i \leq s$, $1 \leq j \leq t$. Then*

(1) C is a self-dual code if and only if $1+c_{e_i}^{1+q^{e_i}} = 0$ and $1+c^{'}_{d_j}c^{''}_{d_j} = 0$.
(2) C is a Euclidean LCD code if and only if $1+c_{e_i}^{1+q^{e_i}} \in R^*_{2e_i}$ and $1+c^{'}_{d_j}c^{''}_{d_j} \in R^*_{d_j}$.

Using this lemma, we now enumerate self-dual and LCD double negacirculant codes over R.

Theorem 5 *Assume that for an even integer n, the factorization of x^n+1 over R is*

$$x^n+1 = a\prod_{i=1}^{s} g_i(x) \prod_{j=1}^{t} h_j(x)h_j^*(x),$$

where $a \in R^*$ and $n = \sum_{i=1}^{s} 2e_i + 2\sum_{j=1}^{t} d_j$. The total number of self-dual double negacirculant codes over R is

$$\prod_{i=1}^{s}(q^{e_i}+1)^3 \prod_{j=1}^{t}(q^{d_j}-1)^3.$$

Proof We enumerate self-dual double negacirculant codes by counting the constituent codes. To count the choices for C_i, we need to find the number of solutions of the equation $1 + c_{e_i} c_{e_i}^{q^{e_i}} = 0$. Let $c_{e_i} = x(1-u-v) + yu + zv$, for some $x, y, z \in \mathbb{F}_{q^{2e_i}}$. Then

$$1 + (x(1-u-v) + yu + zv)(x(1-u-v) + yu + zv)^{q^{e_i}} = 0$$

if and only if

$$xx^{q^{e_i}} = -1, yy^{q^{e_i}} = xx^{q^{e_i}} = -1 \text{ and } zz^{q^{e_i}} = xx^{q^{e_i}} = -1$$

i.e., $Norm(x) = -1, Norm(y) = -1$ and $Norm(z) = -1$. There are $q^{e_i} + 1$ solutions for each $Norm(x) = -1$, $Norm(y) = -1$ and $Norm(z) = -1$, respectively. Therefore, the total number of solutions for the above system is $(q^{e_i}+1)^3$.

Now, to count the choices for the dual pairs $\{C_j^{'}, C_j^{''}\}$, we need to find the number of solutions of the equation $1 + c_{d_j}^{'} c_{d_j}^{''} = 0$. There are the following possibilities:

- If $c_{d_j}^{'} \in R_{d_j}^*$, then $c_{d_j}^{''} = -\frac{1}{c_{d_j}^{'}}$, i.e., a unique choice for $c_{d_j}^{''}$ corresponding to each $c_{d_j}^{'}$. Therefore, there are $|R_{d_j}^*| = (q^{d_j}-1)^3$ choices for $c_{d_j}^{'}$ and hence for the pair $\{c_{d_j}^{'}, c_{d_j}^{''}\}$.
- If $c_{d_j}^{'} \in R_{d_j} \setminus R_{d_j}^*$, then $c_{d_j}^{'} = x(1-u-v) + yu + zv$, for some $x, y, z \in \mathbb{F}_{q^{d_j}}$, where not all x, y or z are non-zero. For $c_{d_j}^{''} = \beta_1(1-u-v) + \beta_2 u + \beta_3 v \in R_{d_j}$, where $\beta_1, \beta_2, \beta_3 \in \mathbb{F}_{q^{d_j}}$, we have

$$1 + c_{d_j}^{'} c_{d_j}^{''} = (1 + x\beta_1) + (y\beta_2 - x\beta_1)u + (z\beta_3 - x\beta_1)v = 0,$$

  which implies that $x\beta_1 = -1, y\beta_2 = -1, z\beta_3 = -1$. Any one of x, y or z equal to 0, yields $-1 = 0$, a contradiction. Therefore, these cases are not possible.

From all the above cases, we conclude that there are $\prod_{i=1}^{s}(q^{e_i}+1)^3 \prod_{j=1}^{t}(q^{d_j}-1)^3$ self-dual double negacirculant codes over R.

With the same assumptions and notations of Theorem 5, the following result provides the enumeration of LCD double negacirculant codes over R.

Theorem 6 *The total number of LCD double negacirculant codes over R is*

$$\prod_{i=1}^{s}(q^{2e_i} - q^{e_i} - 1)^3 \prod_{j=1}^{t}(q^{6d_j} - 3q^{5d_j} + 6q^{4d_j} - 7q^{3d_j} + 6q^{2d_j} - 3q^{d_j} + 1).$$

Proof The total number of LCD double negacirculant codes over R can be obtained by counting the constituent codes. To count the choices for C_i, we need to find the number of solutions for the equation $1 + c_{e_i}^{1+q^{e_i}} \in R_{2e_i}^*$. The following cases arise:

- If $c_{e_i} = 0$, then clearly $1 + c_{e_i}^{1+q^{e_i}} \in R_{2e_i}^*$.
- Let $c_{e_i} \in \langle 1-u-v \rangle$ and $c_{e_i} = x(1-u-v)$, for some $x \in \mathbb{F}_{q^{2e_i}}^*$. Then $1 + c_{e_i}^{1+q^{e_i}} = 1 + x^{1+q^{e_i}}(1-u-v) \in R_{2e_i}^*$ if and only if $x^{1+q^{e_i}} \neq -1$. Therefore, we have $q^{2e_i} - q^{e_i} - 2$ choices for x and hence for c_{e_i}. Similarly, there are $q^{2e_i} - q^{e_i} - 2$ choices for each case $0 \neq c_{e_i} \in \langle u \rangle$ or $\langle v \rangle$.
- Let $c_{e_i} \in \langle 1-u-v, u \rangle$ and $c_{e_i} = x(1-u-v) + yu$, for some $x, y \in \mathbb{F}_{q^{2e_i}}^*$. Then $1 + c_{e_i}^{1+q^{e_i}} = 1 + x^{1+q^{e_i}}(1-u-v) + y^{1+q^{e_i}}u \in R_{2e_i}^*$ if and only if $x^{1+q^{e_i}} \neq -1$ and $y^{1+q^{e_i}} \neq -1$. Therefore, we have $q^{2e_i} - q^{e_i} - 2$ choices for each x, y and hence $(q^{2e_i} - q^{e_i} - 2)^2$ choices for c_{e_i}. Similarly, there are $(q^{2e_i} - q^{e_i} - 2)^2$ choices for $0 \neq c_{e_i} \in \langle u, v \rangle$ or $\langle 1-u-v, v \rangle$ each.
- Let $c_{e_i} \in \langle 1-u-v, u, v \rangle$ and $c_{e_i} = x(1-u-v) + yu + zv$, for some $x, y, z \in \mathbb{F}_{q^{2e_i}}^*$. Then $1 + c_{e_i}^{1+q^{e_i}} = 1 + x^{1+q^{e_i}}(1-u-v) + y^{1+q^{e_i}}u + z^{1+q^{e_i}}v \in R_{2e_i}^*$ if and only if $x^{1+q^{e_i}} \neq -1, y^{1+q^{e_i}} \neq -1$ and $z^{1+q^{e_i}} \neq -1$. Therefore, we have $q^{2e_i} - q^{e_i} - 2$ choices for each x, y, z and hence $(q^{2e_i} - q^{e_i} - 2)^3$ choices for c_{e_i}.

Hence, there are $1 + 3(q^{2e_i} - q^{e_i} - 2) + 3(q^{2e_i} - q^{e_i} - 2)^2 + (q^{2e_i} - q^{e_i} - 2)^3 = (q^{2e_i} - q^{e_i} - 1)^3$ choices for C_i, where $1 \leq i \leq s$.

Now, to count the choices for the pairs $\{C_j^{'}, C_j^{''}\}$, we need to find the number of solution pairs $\{c_{d_j}^{'}, c_{d_j}^{''}\}$ for the equation $1 + c_{d_j}^{'} c_{d_j}^{''} \in R_{d_j}^*$. Here the following cases arise:

- If $c_{d_j}=0$, then clearly $1+c^{'}_{d_j}c^{''}_{d_j}\in R^*_{d_j}$ for all $c^{''}_{d_j}\in R^*_{d_j}$. Thus, there are q^{3d_j} choices for $c^{''}_{d_j}$.
- If $c^{'}_{d_j}\in R^*_{d_j}$, then $c^{''}_{d_j}\in R^*_{d_j}-\frac{1}{c^{'}_{d_j}}$ and we have $|R^*_{d_j}-\frac{1}{c^{'}_{d_j}}|=|R^*_{d_j}|$ choices for $c^{''}_{d_j}$ corresponding to each $c^{'}_{d_j}$. Therefore, there are $|R^*_{d_j}|^2=(q^{d_j}-1)^6$ choices for the pair $\{c^{'}_{d_j},c^{''}_{d_j}\}$.
- If $c^{'}_{d_j}\in\langle 1-u-v\rangle\setminus\{0\}$, then $c^{'}_{d_j}=x(1-u-v)$, for some $x\in\mathbb{F}^*_{q^{d_j}}$. Assume that $c^{''}_{d_j}=\beta_1(1-u-v)+\beta_2u+\beta_3v$, for some $\beta_1,\beta_2,\beta_3\in\mathbb{F}_{q^{d_j}}$. Then $1+c^{'}_{d_j}c^{''}_{d_j}=1+x\beta_1(1-u-v)\in R^*_{d_j}$ if and only if $x\beta_1\neq-1$. Once $c^{'}_{d_j}$ is fixed, there are $q^{d_j}-1$ choices for β_1 and q^{d_j} choices for each β_2,β_3. Therefore, there are $(q^{d_j}-1)^2q^{2d_j}$ choices for the pair $\{c^{'}_{d_j},c^{''}_{d_j}\}$. Similarly, if $0\neq c_{e_i}\in\langle u\rangle$ or $\langle v\rangle$, there are $(q^{d_j}-1)^2q^{2d_j}$ choices for each case.
- If $c^{'}_{d_j}\in\langle 1-u-v,u\rangle$ and $c^{'}_{d_j}=x(1-u-v)+yu$, for some $x,y\in\mathbb{F}^*_{q^{d_j}}$. Assume that $c^{''}_{d_j}=\beta_1(1-u-v)+\beta_2u+\beta_3v$, for some $\beta_1,\beta_2,\beta_3\in\mathbb{F}_{q^{d_j}}$ Then $1+c^{'}_{d_j}c^{''}_{d_j}=1+x\beta_1(1-u-v)+y\beta_2u\in R^*_{d_j}$ if and only if $x\beta_1\neq-1$ and $y\beta_2\neq-1$. Once $c^{'}_{d_j}$ is fixed, there are $q^{d_j}-1$ choices for each β_1,β_2 and q^{d_j} choices for β_3. Therefore, there are $(q^{d_j}-1)^4q^{d_j}$ choices for the pair $\{c^{'}_{d_j},c^{''}_{d_j}\}$. Similarly, if $0\neq c^{'}_{d_j}\in\langle u,v\rangle$ or $\langle 1-u-v,v\rangle$, we have $(q^{d_j}-1)^4q^{d_j}$ choices for each pair $\{c^{'}_{d_j},c^{''}_{d_j}\}$.

Summing all these cases, we get that there are $q^{3d_j}+(q^{d_j}-1)^6+3(q^{d_j}-1)^2q^{2d_j}+3(q^{d_j}-1)^4q^{d_j}=(q^{6d_j}-3q^{5d_j}+6q^{4d_j}-7q^{3d_j}+6q^{2d_j}-3q^{d_j}+1)$ choices for the pairs $\{C^{'}_j,C^{"}_j\}$, where $1\leq j\leq t$. Now, combining all the above choices for C_i and the pairs $\{C^{'}_j,C^{''}_j\}$, we get the desired result.

4 Distance bounds for double circulant codes

In this section, we provide distance bounds for self-dual or LCD double circulant codes and show that the families of Gray images of self-dual or LCD double circulant codes are good (which is one of the main results of this paper).

Let n be an odd prime and q be a primitive root modulo n. We assume that the factorization of x^n-1 into distinct irreducible polynomials over R is

$$x^n-1=(x-1)(1+x+\cdots+x^{n-1})=(x-1)h(x), \tag{3}$$

where $h(x)=1+x+\cdots+x^{n-1}$ is an irreducible polynomial over R. By the Chinese Remainder Theorem (CRT), we have

$$\begin{aligned}\frac{R[x]}{\langle x^n-1\rangle}\cong&\frac{R[x]}{\langle x-1\rangle}\oplus\frac{R[x]}{\langle h(x)\rangle}\\ \cong&R\oplus R_1,\end{aligned}$$

where $R_1=\mathbb{F}_{q^{n-1}}+u\mathbb{F}_{q^{n-1}}+v\mathbb{F}_{q^{n-1}}$, $u^2=u,v^2=v,uv=vu=0$. We denote $\mathcal{R}=\frac{R[x]}{\langle h(x)\rangle}$.

Definition 1 Let C be a cyclic code over R of odd length n and $h(x)$ be a polynomial given in the above discussion. Then a non-zero codeword in C is said to be a constant vector if it is generated by $h(x)$.

Now, we provide two lemmas which will be used to prove the main result.

Lemma 3 *Let $z=(e,f)\in R^{2n}$ be a non-zero vector such that e is not a constant vector. Then there are at most q^{2n+1} double circulant codes $C_a=(1,a)$ over R such that $z\in C_a$, where $a\in\mathcal{R}$.*

Proof The vector z can be written as $z=(e,f)\cong(e_1,f_1)\oplus(e_2,f_2)$ by the CRT decomposition. As $z\in C_a$, we have $f=ea,f_1=e_1a_1$ and $f_2=e_2a_2$, where $e_1,f_1,a_1\in R$ and $e_2,f_2,a_2\in\mathcal{R}$. Let $a_1=r_1(1-u-v)+us_1+vt_1$ and $a_2=r_2(1-u-v)+us_2+vt_2$, for some $r_1,s_1,t_1\in\mathbb{F}_q$ and $r_2,s_2,t_2\in\mathbb{F}_{q^{n-1}}$. Now, we discuss the first constituent of the code C_a through e_1.

- If $e_1=0$, then we have q^3 choices for a_1.
- If $0\neq e_1\in\langle 1-u-v\rangle$, then $e_1=(1-u-v)x_1$ and $f_1=(1-u-v)x^{'}_1$, for some $x_1\in\mathbb{F}^*_q,x^{'}_1\in\mathbb{F}_q$. Now,

$$f_1=(1-u-v)x^{'}_1=(1-u-v)x_1a_1=(1-u-v)x_1r_1.$$

This implies that $r_1=\frac{x^{'}_1}{x_1}$ and we have q^2 choices for a_1. Similarly, when $0\neq e_1\in\langle u\rangle$ or $\langle v\rangle$, we have q^2 choices for each case.

- If $0 \neq e_1 \in \langle 1-u-v, u\rangle$ and $e_1 = x_1(1-u-v) + y_1 u$, for some $x_1, y_1 \in \mathbb{F}_q^*$, then $f_1 = x_1^{'}(1-u-v) + y_1^{'}u$, for some $x_1^{'}, y_1^{'} \in \mathbb{F}_q$. Now,
$$f_1 = (1-u-v)x_1^{'} + uy_1^{'} = ((1-u-v)x_1 + uy_1)a_1 = (1-u-v)x_1r_1 + uy_1s_1.$$
This implies that $r_1 = \frac{x_1^{'}}{x_1}, s_1 = \frac{y_1^{'}}{y_1}$ and we have q choices for a_1. Similarly, when $0 \neq c_1 \in \langle u, v\rangle$ or $\langle 1-u-v, v\rangle$, we have q choices for each case.
- If $e_1 \in R^*$, then we have a unique choice for $a_1 = \frac{f_1}{e_1}$.

Therefore, for each case we have at most q^3 choices for a_1.

For the second constituent code of C_a, we discuss choices for a_2 through e_2.

- If $e_2 = 0$, then e is a constant vector, i.e., $e \equiv 0 \pmod{h(x)}$, which is a contradiction to the choice of e.
- If $0 \neq e_2 \in \langle 1-u-v\rangle$, then $e_2 = (1-u-v)x_2$ and $f_2 = (1-u-v)x_2^{'}$, for some $x_2 \in \mathbb{F}_{q^{n-1}}^*, x_2^{'} \in \mathbb{F}_{q^{n-1}}$. Now,
$$f_2 = (1-u-v)x_2^{'} = (1-u-v)x_2a_2 = (1-u-v)x_2r_2.$$
This implies that $r_2 = \frac{x_2^{'}}{x_2}$ and we have q^{2n-2} choices for a_2. Similarly, when $0 \neq e_2 \in \langle u\rangle$ or $\langle v\rangle$, we have q^{2n-2} choices for each case.
- If $0 \neq e_2 \in \langle 1-u-v, u\rangle$ and $e_2 = x_2(1-u-v) + y_2 u$, for some $x_2, y_2 \in \mathbb{F}_{q^{n-1}}^*$, then $f_2 = x_2^{'}(1-u-v) + y_2^{'}u$, for some $x_2^{'}, y_2^{'} \in \mathbb{F}_{q^{n-1}}$. Now,
$$f_2 = (1-u-v)x_2^{'} + uy_2^{'} = ((1-u-v)x_2 + uy_2)a_2 = (1-u-v)x_2r_2 + uy_2s_2.$$
This implies that $r_2 = \frac{x_2^{'}}{x_2}, s_2 = \frac{y_2^{'}}{y_2}$ and we have q^{n-1} choices for a_2. Similarly, when $0 \neq c_2 \in \langle u, v\rangle$ or $\langle 1-u-v, v\rangle$, we have q^{n-1} choices for each case.
- If $e_2 \in \mathcal{R}^*$, then we have a unique choice for $a_2 = \frac{f_2}{e_2}$.

From the above cases, we conclude that the number of choices for a_2 is at most q^{2n-2}. Therefore, there are at most q^{2n+1} choices for a such that $z \in C_a$.

Keeping the same notations, we have the following result.

Lemma 4 *Let $z = (e, f) \in R^{2n}$ be a non-zero vector such that e is not a constant vector. Then there are at most $8(1 + q^{\frac{n-1}{2}})^2$ self-dual codes $C_a = (1, a)$ such that $z \in C_a$, where $a \in \mathcal{R}$.*

Proof Intially, we discuss the first constituent of the code C_a. From Theorem 3, there are at most 8 choices for C_1, a self-dual double circulant code over R.

For the second constituent code of C_a, we discuss choices for a_2 through e_2. Let $a_2 = (1-u-v)r_2 + us_2 + vt_2$, for some $r_2, s_2, t_2 \in \mathbb{F}_{q^{n-1}}$.

- If $e_2 = 0$, then e is a constant vector, i.e., $e \equiv 0 \pmod{h(x)}$, which is a contradiction to the choice of e.
- If $0 \neq e_2 \in \langle 1-u-v\rangle$, then $e_2 = (1-u-v)x_2$ and $f_2 = (1-u-v)x_2^{'}$, for some $x_2 \in \mathbb{F}_{q^{n-1}}^*, x_2^{'} \in \mathbb{F}_{q^{n-1}}$. Now,
$$f_2 = (1-u-v)x_2^{'} = (1-u-v)x_2a_2 = (1-u-v)x_2r_2.$$
This implies that $r_2 = \frac{x_2^{'}}{x_2}$. Further, as C_a is self-dual, $1 + a_2\bar{a}_2 = 1 + a_2a_2^{q^{\frac{n-1}{2}}} = 0$ which implies that $r_2r_2^{q^{\frac{n-1}{2}}} = -1, s_2s_2^{q^{\frac{n-1}{2}}} = -1$ and $t_2t_2^{q^{\frac{n-1}{2}}} = -1$, i.e., $Norm(r_2) = -1, Norm(s_2) = -1$ and $Norm(t_2) = -1$. Therefore, we have $(1 + q^{\frac{n-1}{2}})^2$ choices for a_2. Similarly, when $0 \neq e_2 \in \langle u\rangle$ or $\langle v\rangle$, we have $(1 + q^{\frac{n-1}{2}})^2$ choices for each case.
- If $0 \neq e_2 \in \langle 1-u-v, u\rangle$ and $e_2 = x_2(1-u-v) + y_2 u$, for some $x_2, y_2 \in \mathbb{F}_{q^{n-1}}^*$, then $f_2 = x_2^{'}(1-u-v) + y_2^{'}u$, for some $x_2^{'}, y_2^{'} \in \mathbb{F}_{q^{n-1}}$. Now,
$$f_2 = (1-u-v)x_2^{'} + uy_2^{'} = ((1-u-v)x_2 + uy_2)a_2 = (1-u-v)x_2r_2 + uy_2s_2.$$
This implies that $r_2 = \frac{x_2^{'}}{x_2}, s_2 = \frac{y_2^{'}}{y_2}$. Further, as C_a is self-dual, $1 + a_2\bar{a}_2 = 1 + a_2a_2^{q^{\frac{n-1}{2}}} = 0$, which implies that $r_2r_2^{q^{\frac{n-1}{2}}} = -1, s_2s_2^{q^{\frac{n-1}{2}}} = -1$ and $t_2t_2^{q^{\frac{n-1}{2}}} = -1$, i.e., $Norm(r_2) = -1, Norm(s_2) = -1$ and $Norm(t_2) = -1$. Therefore, we have at most $(1 + q^{\frac{n-1}{2}})$ choices for a_2. Similarly, when $0 \neq c_2 \in \langle u, v\rangle$ or $\langle 1-u-v, v\rangle$, we have at most $(1 + q^{\frac{n-1}{2}})$ choices for each case.

– If $e_2 \in \mathcal{R}^*$, then we have a unique choice for $a_2 = \frac{f_2}{e_2}$.

From the above cases, we conclude that the number of choices for a_2 is at most $(1+q^{\frac{n-1}{2}})^2$. Therefore, there are at most $8(1+q^{\frac{n-1}{2}})^2$ choices for a such that $z \in C_a$.

Using the Artin's conjecture for primitive roots, we see that for a fixed q which is not a square, there are infinitely many primes n such that q is primitive root modulo n. In that situation, the factorization given in (3) of $x^n - 1$ into two irreducible factors holds. Thus, we get an infinite family of double circulant codes over R. (Note that Artin's conjecture is known to be true for all non-square q's except at most two unspecified exceptions [19]). Now, we are in a position to prove Theorem 2.

Proof We denote the size of the family by A_n. Then using Theorem 3 and Theorem 4 for n tending to infinity, we can approximate A_n to $8q^{\frac{3n-1}{2}}$, for self-dual and q^{3n}, for LCD double circulant codes. Let $B(d_n)$ be the number of elements in R^{2n}, whose image under ϕ_i have Hamming weight less than d_n. Assume that we have

$$A_n > a_n B(d_n), \tag{4}$$

(see [21,28]) where $a_n = 8(1+q^{(n-1)/2})^2$ for self-dual and q^{2n+1}, for LCD codes. Therefore, by Lemma 3 and Lemma 4 we conclude that in the family, there exist codes of length $2n$ over R whose images under ϕ_i have Hamming distance $\geq d_n$.

To enforce inequality (4) for large n, we make the following argument. We consider δ to be the relative distance of the above family and assume that d_n is the largest such that $A_n > a_n B(d_n)$. Also, we assume that the growth is of the form $d_n = 6\delta n$. Then by [[11], Lemma 2.10.3], we get that $B(d_n)$ is approximately equal to $q^{6nH_q(\delta)}$. From this, we can see that if $H_q(\delta_0) < \frac{1}{6}$, for LCD and $< \frac{1}{12}$, for self-dual codes, then inequality (4) holds for n large enough.

5 Numerics

Here, we present several examples of double circulant LCD and self-dual codes under the map ϕ_i, for $i = 1, 2$. To determine their parameters we need a result as below.

Lemma 5 *Assume that C has the generator matrix $G = (I, A)$, where $A = A_1 + uA_2 + vA_3$, A_i is an $n \times n$ matrix over $\mathbb{F}_q$, for $i = 1, 2, 3$ and I is the identity matrix of order n. Then $\phi_i(C)$ has a generator matrix*

$$M_1 = \begin{pmatrix} 0 & 2I & 0 & -A_2 & 2A_1 + A_2 & A_3 \\ -I & I & 0 & -A_1 - A_2 & A_1 + A_2 & 0 \\ 0 & 0 & I & 0 & 0 & A_1 + A_3 \end{pmatrix}_{3n \times 6n}.$$

and

$$M_2 = \begin{pmatrix} I & I & I & A_1 & A_1 + A_2 & A_1 + A_3 \\ 0 & I & 0 & 0 & A_1 + A_2 & 0 \\ 0 & 0 & I & 0 & 0 & A_1 + A_3 \end{pmatrix}_{3n \times 6n}.$$

for $i = 1, 2$, respectively.

Proof The matrix M_i is constructed by applying Gray map ϕ_i on $G = (I, A)$, uG and vG, for $i = 1, 2$, respectively.

Now, by using the generator matrices given by Lemma 5 and the Magma computation system [5], we calculate the minimum distances d in Table 1 for the double circulant codes of length $2n$ over $R = \mathbb{F}_5 + u\mathbb{F}_5 + v\mathbb{F}_5$. In this way, we obtain their $\mathbb{F}_5$ parameters $[6n, 3n, d]$ (sixth-column). Note that second to fourth columns include the generator polynomials $a_i(x)$, for $i = 1, 2, 3$, respectively. Also, we write the coefficients of these polynomials in decreasing powers of x, for instance, we write 3242 to represent the polynomial $3x^3 + 2x^2 + 4x + 2$. In last column, we also mention their nature in terms of LCD or self-dual.

6 Conclusion

In this paper , we have calculated the total number of self-dual and LCD double circulant and double negacirculant codes over the semi-local ring R. Further, we study the distance bounds for the family of Gray images of self-dual and LCD double circulant codes over R and show that these families are good. It would be a worthy study to investigate these codes for other semi-local non-chain rings in the future.

Table 1: $\mathbb{F}_5$-images of double circulant codes of length $2n$ over $\mathbb{F}_5 + u\mathbb{F}_5 + v\mathbb{F}_5$

n	$a_1(x)$	$a_2(x)$	$a_3(x)$	Map	Parameters	Remark
2	30	23	22	ϕ_2	$[12, 6, 2]_5$	Self-dual
3	133	114	344	ϕ_2	$[18, 9, 4]_5$	Self-dual
3	121	402	121	ϕ_1	$[18, 9, 4]_5$	LCD
4	0334	3242	4234	ϕ_1	$[24, 12, 4]_5$	LCD
4	1114	3332	3332	ϕ_2	$[24, 12, 4]_5$	Self-dual
5	43030	04131	33303	ϕ_1	$[30, 15, 5]_5$	LCD
6	010044	132202	142241	ϕ_1	$[36, 18, 5]_5$	LCD
7	1402124	2113424	1402124	ϕ_1	$[42, 21, 6]_5$	LCD
8	34430110	24023121	31231143	ϕ_1	$[48, 24, 6]_5$	LCD
9	033302122	314321000	342123122	ϕ_1	$[54, 27, 7]_5$	LCD

Acknowledgement

The authors are thankful to the University Grants Commission (UGC), Govt. of India for financial support and Indian Institute of Technology Patna for research facilities. Also, authors would like to thank the anonymous referee(s) and the Editor for their valuable comments to improve the presentation of the manuscript.

References

1. Alahmadi, A., Güneri, C., Ozkaya, B., Shoaib, H., Solé, P.: On self-dual double negacirculant codes. Discret. Appl. Math. **222**, 205-212 (2017).
2. Alahmadi, A., Özdemir, F., Solé, P.: On self-dual double circulant codes. Des. Codes Cryptogr. **86**(6), 1257-1265 (2018).
3. Ashraf, M., Mohammad, G.: Skew cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$. Asian-Eur. J. Math. **11**(5), 1850072 (2018).
4. Aydin, N., Cengellenmis, Y., Dertli, A.: On some constacyclic codes over $\mathbb{Z}_4[u]/\langle u^2 - 1\rangle$, their $\mathbb{Z}_4$ images, and new codes. Des. Codes Cryptogr. **86**(6), 1249-1255 (2018).
5. Bosma, W., Cannon, J.: Handbook of Magma Functions. Univ. of Sydney (1995).
6. Blake, I. F.: Codes over certain rings. Inform. Contr. **20**, 396-404 (1972).
7. Guneri, C., Ozkaya, B., Solé, P.: Quasi-cyclic complementary dual codes. Finite Fields Their Appl. **42**, 67-80 (2016).
8. Gulliver, T. A., Bhargava, V. K.: Some best rate $\frac{1}{p}$ and rate $\frac{p-1}{p}$ systematic quasi-cyclic codes. IEEE Trans. Inf. Theory. **37**, 552-555 (1991).
9. Gulliver, T. A., Bhargava, V. K.: Twelve good rate $\frac{(m-r)}{pm}$ binary quasi-cyclic codes. IEEE Trans. Inf. Theory **39**, 1750-1751 (1993).
10. Huang, D., Shi, M., Solé, P.: Double Circulant Self-Dual and LCD Codes Over $\mathbb{Z}_{p^2}$. Int. J. Found. Comput. Sci. **30**(3), 407-416 (2019).
11. Huffman, W. C., Pless, V.: Fundamentals of Error Correcting Codes. Cambridge University Press, (2003).
12. Islam, H., Prakash, O.: A note on skew constacyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$. Discrete Math. Algorithms Appl. **11**(3), 1950030 (2019).
13. Islam, H., Prakash, O.: New quantum codes from constacyclic and additive constacyclic codes. Quantum Inf. Process **19**(9), 1-17 (2020).
14. Islam, H., Bag, T., Prakash, O.: A class of constacyclic codes over $\mathbb{Z}_4[u]/\langle u^k\rangle$. J. Appl. Math. Comput. **60**(1-2), 237-251 (2019).
15. Islam, H., Prakash, O.: A class of constacyclic codes over the ring $\mathbb{Z}_4[u, v]/\langle u^2, u^2, uv - vu\rangle$ and their Gray images. Filomat **33**(8), 2237-2248 (2019).
16. Lidl, R., Niederreiter, H.: Finite Fields. Addison-Wesley, Reading (1983).
17. Ling, S., Solé, P.: On the algebraic structure of quasi-cyclic codes I: Finite fields. IEEE Trans. Inf. Theory **47**(7), 2751-2760 (2001).
18. Ling, S., Solé, P.: On the algebraic structure of quasi-cyclic codes II: Chain rings. Des. Codes Cryptogr. **30**(1), 113-130 (2003).
19. Moree, P.: Artin's primitive root conjecture a survey. Integers **10**(6), 1305-1416 (2012).
20. Qian, L., Shi, M., Solé, P.: On self-dual and LCD quasi-twisted codes of index two over a special chain ring. Cryptogr. Commun. **11**(4), 717-734 (2019).
21. Shi, M., Zhu, H., Qian, L., Sok, L., Solé, P.: On self-dual and LCD double circulant and double negacirculant codes over $\mathbb{F}_q + u\mathbb{F}_q$. Cryptogr. Commun. **12**(1), 53-70 (2020).
22. Shi, M., Huang, D., Sok, L., Solé, P.: Double circulant LCD codes over $\mathbb{Z}_4$. Finite Fields Appl. **58**, 133-144 (2019).
23. Shi, M., Huang, D., Sok, L., Solé, P.: Double circulant self-dual and LCD codes over Galois ring. Adv. Math. Commun. **13**(1), 171-183 (2019).

24. Shi, M., Zhu, H., Qian, L., Solé, P.: On self-dual four circulant codes. Int. J. Found. Comput. Sci. **29**(07), 1143-1150 (2018).
25. Shi, M., Sok, L., Aydin, N., Sole, P.: On constacyclic codes over $\mathbb{Z}_4[u]/\langle u^2-1\rangle$. Finite Fields Appl. **45**, 86-95 (2015).
26. Shi, M., Zhang, Y.: Quasi-twisted codes with constacyclic constituent codes. Finite Fields Their Appl. **39**, 159-178 (2016).
27. Shi, M., Qian, L., Solé, P.: On self-dual negacirculant codes of index two and four. Des. Codes Cryptogr. **11**, 2485-2494 (2018).
28. Yao, T., Zhu, S., Kai, X.: On self-dual and LCD double circulant codes over a non-chain ring. Chinese Journal of Electronics **28**(5), 1018-1024 (2019).
29. Zhu, H., Shi, M.: On linear complementary dual four circulant codes. Bull. Aust. Math. Soc. **98**(1), 159-166 (2018).