Self-dual and LCD double circulant codes over a class of non-local rings

Om Prakash, Shikha Yadav, Habibul Islam, Patrick Solé

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

Self-dual and LCD double circulant codes over a class of non-local rings

Om Prakash[*1] · **Shikha Yadav**[1] · **Habibul Islam**[1] · **Patrick Solé**[2]

Received: date / Accepted: date

Abstract Let $\mathbb{F}_q$ be a finite field of order $q = p^m$ where p is an odd prime. This paper presents the study of self-dual and LCD double circulant codes over a class of finite commutative non-chain rings $R_q = \mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q + \cdots + u^{q-1}\mathbb{F}_q$ where $u^q = u$. Here, the whole contribution is two-folded. Firstly, we enumerate self-dual and LCD double circulant codes of length $2n$ over R_q, where n is an odd integer. Then by considering a dual-preserving Gray map ϕ, we show that Gray images of such codes are asymptotically good. Secondly, we investigate the algebraic structure of 1-generator quasi-cyclic (QC) codes over R_q for $q = 3$. In that context, we present their generator polynomials along with their minimal generating sets and minimum distance bounds. Here, it is proved that $\phi(C)$ is an sq-QC code of length nq over $\mathbb{F}_q$ if C is an s-QC code of length n over R_q.

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

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

1 Introduction

Self-dual double circulant codes over finite fields have remained worthy of study for more than three decades [34]. Recently, their enumeration and asymptotic performance over finite fields have been presented in [2]. However, there is a scope to extend this study over finite commutative rings where -1 is a square. Towards this end, the Chinese Remainder Theorem (CRT) approach, which was introduced in [18] for quasi-cyclic codes, can be employed.
On the other hand, a special kind of linear code, namely, linear complementary dual (shortly, LCD), was introduced in 1992 [23]. They have defined LCD codes as linear codes having trivial intersections with their dual. These codes play an important role in preventing side-channel attacks (SCA), fault-injection attacks (FIA) in embarked cryptosystems [5], and in multi-secret sharing schemes [26]. These codes are worth studying over different alphabets (finite fields and rings) [16, 17,20,21]. In the last three years, both self-dual and LCD double circulant codes experienced intense attention over finite commutative rings, like $\mathbb{Z}_{p^2}$ (p is prime) in [13], $\mathbb{Z}_4$ in [29], and Galois rings in [30]. In 2020, self-dual and LCD double circulant and double negacirculant codes over the non-chain ring $\mathbb{F}_q + u\mathbb{F}_q$, where $u^2 = u$ are studied in [28]. The enumeration and performance of such codes have explicitly been presented there.Further, these codes are investigated over another non-chain rings $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, $v^3 = v$ in [37] and $\mathbb{F}_q[v]/\langle v^2 - 1\rangle$ in [36]. Recently, we [35] investigated self-dual and LCD double circulant and double negacirculant codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$ where $u^2 = u, v^2 = v, uv = vu = 0$. In continuation, here we consider a class of non-chain rings $R_q = \mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q + \cdots + u^{q-1}\mathbb{F}_q$, $u^q = u$ of size q^q, where $q = p^m$ and p is an odd prime. The ring R_q has a special interest and was explored in several studies [8,9]. This paper enumerates

[1] Department of Mathematics
Indian Institute of Technology Patna, Patna 801 106, India
E-mail: om@iitp.ac.in(*corresponding author), 1821ma10@iitp.ac.in, habibul.pma17@iitp.ac.in

[2] I2M, (CNRS, Aix-Marseille University, Centrale Marseille) Marseille, France
E-mail: sole@enst.fr

both self-dual and LCD double circulant codes over R_q. In addition, using a Gray map ϕ which carries self-dual (resp. LCD) codes over R_q to self-dual (resp. LCD) codes over $\mathbb{F}_q$, we show that the Gray images of such codes constitute an asymptotically good family of codes.

In the second part of the paper, we investigate 1-generator quasi-cyclic (QC) codes over R_q for $q = 3$. It is well known that quasi-cyclic code is one of the most remarkable and studied generalizations of cyclic codes and hence consists of several record-breaking codes [11,12]. By using the Chinese Remainder Theorem (CRT) approach, Ling and Solé investigated the algebraic structure of these codes over finite fields [18], and over chain rings [19], respectively. Further, when a quasi-cyclic code is generated by a single element as a module over some auxiliary ring, then it is called a 1-generator quasi-cyclic code. Such codes have been studied in several series of papers [4,6,7,25,27,33]. Here, we obtain the algebraic structure of 1-generator quasi-cyclic codes over R_3 by using their generators and minimal spanning sets. In short, three major contributions of the paper are:

1. The paper enumerates both self-dual (Theorem 4) and LCD (Theorem 5) double circulant codes over R_q of length $2n$ where n is an odd integer.
2. It contains asymptotically good families of codes (Theorem 6).
3. It also presents the algebraic structure of 1-generator quasi-cyclic codes of length n over R_q for $q = 3$ (Section 6). Further, it is proved that the Gray image of an s-QC code of length n is an sq-QC code of length nq over $\mathbb{F}_q$ (Theorem 7).

The presentation of this paper is as follows: Section 2 recalls basic facts and definitions of the ring R_q and double circulant codes. Section 3 enumerates double circulant self-dual codes of length $2n$. In section 4, we discuss the asymptotic results for the families of LCD and self-dual double circulant codes. Next, section 5 contains numerical examples of double circulant LCD codes over R_3. Section 6 focuses on 1-generator codes, while section 7 concludes the paper.

2 Preliminary

Let $R_q = \mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q + \cdots + u^{q-1}\mathbb{F}_q$, $u^q = u$. Thus, following [8,9], R_q is a finite commutative non-chain semi-local ring with unity. Also, the ring R_q is isomorphic to the ambient ring $\mathbb{F}_q[u]/\langle u^q - u\rangle$, and every element $r \in R_q$ has a representation $r = a_0 + ua_1 + \cdots + a_{q-1}u^{q-1}$ where $a_i \in \mathbb{F}_q$ for $0 \le i \le q-1$. Let α be a primitive element of $\mathbb{F}_q$ and

$$\begin{aligned}
\eta_1 &= 1 - u^{q-1},\\
\eta_2 &= \frac{1}{q-1}(u + u^2 + \cdots + u^{q-2} + u^{q-1}),\\
\eta_3 &= \frac{1}{q-1}(\alpha u + \alpha^2 u^2 + \cdots + \alpha^{q-2}u^{q-2} + u^{q-1}),\\
\eta_4 &= \frac{1}{q-1}(\alpha^2 u + (\alpha^2)^2 u^2 + \cdots + (\alpha^2)^{q-2}u^{q-2} + u^{q-1}),\\
&\vdots\\
\eta_q &= \frac{1}{q-1}(\alpha^{q-2} u + (\alpha^{q-2})^2 u^2 + \cdots + (\alpha^{q-2})^{q-2}u^{q-2} + u^{q-1}).
\end{aligned}$$

Then it is checked that $\eta_i^2 = \eta_i, \eta_i\eta_j = 0$ for $i \neq j, 1 \le i, j \le q$ and $\sum_{i=1}^{q} \eta_i = 1$. In other words, $\{\eta_i : 1 \le i \le q\}$ is a set of pairwise orthogonal idempotent elements. Therefore, by using the Chinese Remainder Theorem, we have $R_q \cong \bigoplus_{i=1}^{q} \eta_i\mathbb{F}_q$. Consequently, every element $r \in R_q$ can be expressed uniquely as $r = \sum_{i=1}^{q} \eta_i r_i$, where $r_i \in \mathbb{F}_q$ for all i. Moreover, $r \in R_q$ is a unit if and only if r_i is a unit in $\mathbb{F}_q$ for $1 \le i \le q$.

Now, we recall that a non-empty subset C of R_q^n is said to be a *linear code* of length n over R_q if it is an R_q-submodule of R_q^n and elements of C are called *codewords*. For any two vectors $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n)$, the *Euclidean* inner product is defined by $x \cdot y = \sum_{i=1}^{n} x_i y_i$. In this way, the Euclidean dual of a linear code C is given by $C^\perp = \{x \in R_q^n : x \cdot y = 0, \text{ for all } y \in C\}$. In addition, C is said to be *self-dual* if $C = C^\perp$, *self-orthogonal* if $C \subseteq C^\perp$ and *linear complementary dual* (shortly, LCD) if $C \cap C^\perp = \{0\}$. It has been shown in [19] that a double

circulant self-dual code over a commutative ring can only exist if a square root of -1 exists in that ring. The following theorem provides the conditions for the existence of the square root of -1 in the ring R_q.

Theorem 1 *In the ring R_q with characteristic p, i.e., $q = p^s$ for $s \geq 1$, a square root of -1 exists if and only if one of the following cases occurs:*

1. $p = 2$,
2. $p \equiv 3 \pmod 4$, *and s is even*
3. $p \equiv 1 \pmod 4$

Proof We already have that an square root of -1 exists in $\mathbb{F}_q$ if and only if any one of the above cases occurs (see [19]). Therefore, if any one of the above cases occurs then an square root of -1 exists in R_q (since $\mathbb{F}_q \subseteq R_q$). Conversely, assume that $r = \sum_{i=1}^{q} \eta_i r_i$, where $r_i \in \mathbb{F}_q$ for all i, be an square root of -1 in R_q, i.e., $r^2 = -1$ or equivalently $r^2 + 1 = 0$. Then

$$r^2 + 1 = 1 + \eta_1 r_1^2 + \eta_2 r_2^2 + \cdots + \eta_i r_q^2 = \eta_1(1 + r_1^2) + \eta_2(1 + r_2^2) + \cdots + \eta_q(1 + r_q^2) = 0$$

if and only if $r_i^2 = -1$ for all i. That is, an square root of -1 exists in $\mathbb{F}_q$. Therefore, q is any one of the form given in above three cases. □

For a linear code C of length n over R_q, we define

$$C_1 = \{y_1 \in \mathbb{F}_q^n | \text{ there exists } y_i (i \neq 1) \in \mathbb{F}_q^n \text{ such that } \sum_{i=1}^{q} y_i \eta_i \in C\},$$

$$C_2 = \{y_2 \in \mathbb{F}_q^n | \text{ there exists } y_i (i \neq 2) \in \mathbb{F}_q^n \text{ such that } \sum_{i=1}^{q} y_i \eta_i \in C\},$$

$$\vdots$$

$$C_q = \{y_q \in \mathbb{F}_q^n | \text{ there exists } y_i (i \neq q) \in \mathbb{F}_q^n \text{ such that } \sum_{i=1}^{q} y_i \eta_i \in C\}.$$

Then C_i is a linear code of length n over $\mathbb{F}_q$ for $1 \leq i \leq q$ and $C = \bigoplus_{i=1}^{q} \eta_i C_i$.

Proposition 1 *Let $C = \bigoplus_{i=1}^{q} \eta_i C_i$ be a linear code of length n, where C_i is a linear code of length n over $\mathbb{F}_q$ for $1 \leq i \leq q$. Then $C^\perp = \bigoplus_{i=1}^{q} \eta_i C_i^\perp$. Moreover, C is self-dual if and only if C_i is self-dual for $1 \leq i \leq q$.*

Proof Same as the proof of [[15], Theorem 3.5]. □

Again, we recall a linear code C is said to be a cyclic code if for any codeword $(c_0, c_1, \ldots, c_{n-1}) \in C$, we have $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$. In addition, a cyclic code C can be described as an ideal of the ring $R_q[x]/\langle x^n - 1\rangle$ by the correspondence $(c_0, c_1, \ldots, c_{n-1}) \in C \longmapsto c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in R_q[x]/\langle x^n - 1\rangle$. Here, the structural properties of cyclic codes over R_q are already available in the literature [8] and we enlist them in the next result.

Theorem 2 *Let $C = \bigoplus_{i=1}^{q} \eta_i C_i$ be a linear code of length n over R_q. Then C is cyclic if and only if C_i is a cyclic code for $1 \leq i \leq q$. Further, C is principally generated by a polynomial $g(x) = \eta_1 g_1(x) + \eta_2 g_2(x) + \cdots + \eta_q g_q(x)$, a factor of $x^n - 1$, where $g_i(x)$ is the generator of C_i for $1 \leq i \leq q$.*

Now, we define a Gray map $\phi : R_q \longrightarrow \mathbb{F}_q^q$ by $\phi(r) = (r_1, r_2, \ldots, r_q)$ where $r = \sum_{i=1}^{q} \eta_i r_i \in R_q$. Then ϕ is an $\mathbb{F}_q$-linear bijective map and can be extended to R_q^n componentwise. The *Lee weight* of $x \in R_q^n$ is defined as $w_L(x) = w_H(\phi(x))$ and the Lee distance between $x, y \in R_q^n$ is $d_L(x, y) = d_H(\phi(x), \phi(y))$, where w_H, d_H are Hamming weight and distance in $\mathbb{F}_q^{nq}$, respectively. Therefore, $\phi : R_q^n \longrightarrow \mathbb{F}_q^{nq}$ is a distance preserving linear map.

Lemma 1 *Let C be a linear code of length n over R_q. Then $\phi(C^{\perp}) = \phi(C)^{\perp}$ and $\phi(C \cap C^{\perp}) = \phi(C) \cap \phi(C)^{\perp}$.*

Proof By the definition of Gray map ϕ, it is easily followed. □

In the light of Lemma 1, we immediately get the following result.

Theorem 3 *Let C be a linear code of length n over R_q. Then C is a self-dual (resp. LCD) code if and only if $\phi(C)$ is a self-dual (resp. LCD) code of length nq over $\mathbb{F}_q$.*

Now, we define the norm function $Norm : \mathbb{F}_{q^n} \to \mathbb{F}_q$ by

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

It is a multiplicative, surjective function with $Norm(0) = 0$ and every non-zero element of $\mathbb{F}_q$ is a norm of exactly $\frac{q^n-1}{q-1}$ elements in $\mathbb{F}_{q^n}$ (see [24, Theorem 2.28]). We will use $Norm$ to find the number of solutions of certain algebraic equations. Recall that a *double circulant code* is a linear code having a generator matrix of the form

$$G = (I, A)$$

where A is a circulant matrix (i.e., the matrix whose rows can be obtained by successive circular shifts of the first row). For a family $C_{\langle n \rangle}$ of codes over $\mathbb{F}_q$ with parameters $[n, k_n, d_n]$, the *rate* ρ and *relative distance* δ are defined as $\rho = \limsup_{n\to\infty} \frac{k_n}{n}$ and $\delta = \limsup_{n\to\infty} \frac{d_n}{n}$. We say that this family of codes is *good* if $\rho\delta \neq 0$. Further, we recall the entropy function from [14] defined as

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

and we will use it to show that the Gray images of family of self-dual (resp. LCD) double circulant codes over R_q are good in subsequent portion.

3 Enumeration of double circulant codes

Let n be an odd integer and factorization of $x^n - 1$ into distinct irreducible factors over R_q be given by

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

where $a \in R_q^*$ (set of units in R_q), $g_i(x)$ are self-reciprocal polynomials of even degree $2e_i$ and $h_j^*(x)$ are reciprocal polynomials of $h_j(x)$ with $\deg(h_j(x)) = d_j$, for $2 \leq i \leq s$ and $1 \leq j \leq t$. Now, by the Chinese Remainder Theorem, we have

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

where $R_{q,r} = \mathbb{F}_{q^r} + u\mathbb{F}_{q^r} + u^2\mathbb{F}_{q^r} + \cdots + u^{q-1}\mathbb{F}_{q^r}$, $u^q = u$ for $r = 2e_i$ or d_j. From the natural extension of the above decomposition, we have

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

Following this, any linear code C of length 2 over $\frac{R_q[x]}{\langle x^n-1\rangle}$ 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 of length 2 over R_q, C_i is a linear code of length 2 over $R_{q,2e_i}$, for $2 \leq i \leq s$ and $C_j^{'}, C_j^{''}$ are linear codes of length 2 over R_{q,d_j}, for $1 \leq j \leq t$. The following lemma is useful to enumerate self-dual and LCD double circulant codes over R_q.

Lemma 2 *Let C be a double circulant code of length $2n$ over R_q given in the CRT decomposition (1) with $\alpha_1 = (1, c_{e_1}), \alpha_i = (1, c_{e_i}), \alpha_j^{'} = (1, c_{d_j}^{'}), \alpha_j^{''} = (1, c_{d_j}^{''})$ be generators of the constituent codes C_1, C_i over $R_q, R_{q,2e_i}$ and $C_j^{'}, C_j^{''}$ over R_{q,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 $1 + c_{e_1}^2 \in R_q^*$, $1 + c_{e_i}^{1+q^{e_i}} \in R_{q,2e_i}^*$ and $1 + c_{d_j}^{'} c_{d_j}^{''} \in R_{q,d_j}^*$.

Proof The proof is similar to [28, Lemma 3.1]. □

Now, by using Lemma 2, we count self-dual and LCD double circulant codes over R_q in Theorem 4 and Theorem 5, respectively.

Theorem 4 *Let n be an odd integer and the factorisation of $x^n - 1$ over R_q be*

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

where $a \in R_q^*$ and $n = 1 + \sum_{i=2}^{s} 2e_i + 2\sum_{j=1}^{t} d_j$. Then there are

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

self-dual double circulant codes of length $2n$ over R_q.

Proof To obtain the total number of self-dual double circulant codes, we count the constituent codes. Let $c_{e_1} \in R_q$. Then $c_{e_1} = a_1\eta_1 + a_2\eta_2 + \cdots + a_q\eta_q$ for some $a_i \in \mathbb{F}_q$, $1 \leq i \leq q$. From Lemma 2, for the first constituent code C_1, we need to find choices for $c_{e_1} \in R_q$ such that $1 + c_{e_1}^2 = 0$. Consider

$$1 + c_{e_1}^2 = 1 + a_1^2\eta_1 + \cdots + a_q^2\eta_q = (1 + a_1^2)\eta_1 + (1 + a_2^2)\eta_2 + \cdots + (1 + a_q^2)\eta_q = 0,$$

if and only if $1 + a_i^2 = 0$ for $1 \leq i \leq q$. So there are 2 choices ($\pm\omega$, where $\omega^2 = -1$) for each a_i. Therefore, we have 2^q choices for c_{e_1} and hence for C_1.

For the second constituent code, we have to find choices for $c_{e_i} \in R_{q,2e_i}$ such that $1 + c_{e_i} c_{e_i}^{q^{e_i}} = 0$ where i is fixed. Let $c_{e_i} = a_1\eta_1 + a_2\eta_2 + \cdots + a_q\eta_q$ for some $a_j \in \mathbb{F}_{q^{2e_i}}$, $1 \leq j \leq q$. Then

$$1 + c_{e_i} c_{e_i}^{q^{e_i}} = 1 + a_1^{q^{e_i}+1}\eta_1 + \cdots + a_q^{q^{e_i}+1}\eta_q = (1 + a_1^{q^{e_i}+1})\eta_1 + \cdots + (1 + a_q^{q^{e_i}+1})\eta_q = 0,$$

if and only if $a_j^{q^{e_i}+1} = -1$, i.e., $Norm(a_j) = -1$ for $1 \leq j \leq q$. There are $q^{e_i} + 1$ solutions for each $Norm(a_j) = -1$, $1 \leq j \leq q$. Thus, there are $(q^{e_i} + 1)^q$ choices for c_{e_i}.

In order to count the dual pairs (w.r.t. Euclidean inner product) of codes for fixed j, we have to find the choices for the pairs $\{c_{d_j}^{'}, c_{d_j}{''}\}$ in R_{q,d_j} such that $1 + c_{d_j}^{'} c_{d_j}^{''} = 0$. Let $c_{d_j}^{'} = a_1\eta_1 + a_2\eta_2 + \cdots + a_q\eta_q$ for some $a_i \in \mathbb{F}_{q^{d_j}}$, $1 \leq i \leq q$. Then, for $c_{d_j}^{''} = b_1\eta_1 + b_2\eta_2 + \cdots + b_q\eta_q$ where $b_i \in \mathbb{F}_{q^{d_j}}$, $1 \leq i \leq q$, we have

$$1 + c_{d_j}^{'} c_{d_j}^{''} = (1 + a_1b_1)\eta_1 + (1 + a_2b_2)\eta_2 + \cdots + (1 + a_qb_q)\eta_q = 0,$$

if and only if $1 + a_ib_i = 0$, for all $1 \leq i \leq q$. If $a_i \in \mathbb{F}_{q^{d_j}}^*$ for $1 \leq i \leq q$, then we have a unique choice $b_i = -\frac{1}{a_i}$, and if $a_i = 0$, then we get $1 = 0$, a contradiction. Therefore, $a_i \in \mathbb{F}_{q^{d_j}}^*$ for each $1 \leq i \leq q$ and corresponding to each a_i there is a unique choice for b_i. Hence, there are $(q^{d_j} - 1)^q$ choices for the dual pairs. Now, combining all the above cases, we get the desired result. □

Theorem 5 *We assume the condition of Theorem 4. Then the total number of LCD double circulant codes of length $2n$ over R_q is*

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

Proof As for the self-dual codes, the total number of LCD double circulant codes can be obtained by counting the constituent codes. For C_1, we need to find the choices for $c_{e_1} \in R_q$ such that $1 + c_{e_1}^2 \in R_q^*$. If $c_{e_1} \in R_q$, then $c_{e_1} = a_1\eta_1 + a_2\eta_2 + \cdots + a_q\eta_q$ for some $a_i \in \mathbb{F}_q$, $1 \leq i \leq q$. Now,

$$1 + c_{e_1}^2 = 1 + a_1^2\eta_1 + \cdots + a_q^2\eta_q = (1 + a_1^2)\eta_1 + (1 + a_2^2)\eta_2 + \cdots + (1 + a_q^2)\eta_q \in R_q^*,$$

if and only if $1 + a_i^2 \neq 0$, for all $1 \leq i \leq q$. That is, there are $q - 2$ choices for each a_i ($\neq \pm\omega$, where $\omega^2 = -1$). Therefore, we have $(q-2)^q$ choices for c_{e_1}.

For a fixed $2 \leq i \leq s$, to count second constituent codes C_i, we need to find choices for $c_{e_i} \in R_{q,2e_i}$ such that $1 + c_{e_i}^{1+q^{e_i}} \in R_{q,2e_i}^*$. If $c_{e_i} \in R_{q,2e_i}$, then $c_{e_i} = a_1\eta_1 + a_2\eta_2 + \cdots + a_q\eta_q$, for some $a_j \in \mathbb{F}_{q^{2e_i}}$, $1 \leq j \leq q$. Now,

$$1 + c_{e_i}^{1+q^{e_i}} = 1 + a_1^{1+q^{e_i}}\eta_1 + \cdots + a_q^{1+q^{e_i}}\eta_q = (1 + a_1^{1+q^{e_i}})\eta_1 + \cdots + (1 + a_q^{1+q^{e_i}})\eta_q \in R_{q,2e_i}^*,$$

if and only if $1 + a_j^{1+q^{e_i}} \neq 0$, for all $1 \leq j \leq q$. That is, there are $q^{2e_i} - q^{e_i} - 1$ choices for each a_j, as we have $q^{e_i} + 1$ solutions for $1 + a_j^{q^{e_i}+1} = 0$. Therefore, we have $(q^{2e_i} - q^{e_i} - 1)^q$ choices for c_{e_i}.

Now, for a fixed $1 \leq j \leq t$, to count dual pairs $\{C_j^{'}, C_j^{''}\}$, we need to find choices for $c_{d_j}^{'}, c_{d_j}^{''} \in R_{q,d_j}$ such that $1 + c_{d_j}^{'}c_{d_j}^{''} \in R_{q,d_j}^*$. If $c_{d_j}^{'} \in R_{q,d_j}$, then $c_{d_j}^{'} = a_1\eta_1 + a_2\eta_2 + \cdots + a_q\eta_q$, for some $a_i \in \mathbb{F}_{q^{d_j}}$, $1 \leq i \leq q$. Now, for any $c_{d_j}^{''} = b_1\eta_1 + b_2\eta_2 + \cdots + b_q\eta_q$ where $b_i \in \mathbb{F}_{q^{d_j}}$, $1 \leq i \leq q$, we have

$$1 + c_{d_j}^{'}c_{d_j}^{''} = (1 + a_1b_1)\eta_1 + (1 + a_2b_2)\eta_2 + \cdots + (1 + a_qb_q)\eta_q \in R_{q,d_j}^*,$$

if and only if $1 + a_ib_i \neq 0$, for all $1 \leq i \leq q$. We have the following possibilities for each a_i, $1 \leq i \leq q$

- If $a_i = 0$, then $1 + a_ib_i = 1 \neq 0$, for each $b_i \in \mathbb{F}_{q^{d_j}}$. Therefore, there are q^{d_j} choices for b_i.
- If $a_i \in \mathbb{F}_{q^{d_j}}^*$, then $1 + a_ib_i \neq 0$ implies that $b_i \neq -\frac{1}{a_i}$ and we have $q^{d_j} - 1$ choices for b_i corresponding to the given a_i. In this case, there are $q^{d_j} - 1$ choices for a_i, so we have $(q^{d_j} - 1)^2$ choices for the pair $\{a_i, b_i\}$ such that $1 + a_ib_i \neq 0$.

Combining the above two possibilities, we have $(q^{d_j} + (q^{d_j} - 1)^2)^q$ choices for the pairs $\{c_{d_j}^{'}, c_{d_j}^{''}\}$ in R_{q,d_j} and hence for $\{C_j^{'}, C_j^{''}\}$. Now, from all the above discussion, we obtain the desired result. □

4 Distance bounds

Let n be an odd prime and q be a power of an odd prime such that it is a primitive root $\pmod{n}$. Then the factorization of $x^n - 1$ into distinct irreducible factors over R_q is as follows:

$$x^n - 1 = (x - 1)(1 + x + \cdots + x^{n-1}) = (x - 1)h(x), \tag{2}$$

where $h(x) = 1 + x + \cdots + x^{n-1}$ is an irreducible polynomial over R_q. Hence, by the Chinese Remainder Theorem (CRT), we know that

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

where $R^{'} = \mathbb{F}_{q^{n-1}} + u\mathbb{F}_{q^{n-1}} + u^2\mathbb{F}_{q^{n-1}} + \cdots + u^{q-1}\mathbb{F}_{q^{n-1}}$, $u^q = u$. We denote $\mathcal{R} = \frac{R_q[x]}{\langle h(x)\rangle}$. Any non-zero codeword of a cyclic code of length n 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 related to distance bound (Theorem 6).

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

Proof Using the CRT decomposition, we can write $z = (e_1, f_1) \oplus (e_2, f_2)$. Since $z \in C_a$, we have $f = ea$, $f_1 = e_1a_1$ and $f_2 = e_2a_2$, where $e_1, f_1, a_1 \in R_q$ and $e_2, f_2, a_2 \in \mathcal{R}$. Let $a_1 = r_1\eta_1 + r_2\eta_2 + \cdots + r_q\eta_q$ and $a_2 = s_1\eta_1 + s_2\eta_2 + \cdots + s_q\eta_q$, for some $r_i \in \mathbb{F}_q$ and $s_i \in \mathbb{F}_{q^{n-1}}$, $1 \leq i \leq q$. Firstly, we discuss the choices for a_1 through e_1.

If $e_1 \in R_q$, then $e_1 = b_1\eta_1 + b_2\eta_2 + \cdots + b_q\eta_q$ and $f_1 = \beta_1\eta_1 + \beta_2\eta_2 + \cdots + \beta_q\eta_q$ for some $\beta_i, b_i \in \mathbb{F}_q$, $1 \leq i \leq q$. Now, $f_1 = e_1a_1$ implies that

$$\beta_1\eta_1 + \beta_2\eta_2 + \cdots + \beta_q\eta_q = r_1b_1\eta_1 + r_2b_2\eta_2 + \cdots + r_qb_q\eta_q.$$

If $b_i = 0$, then we have q choices for r_i, otherwise $r_i = \frac{\beta_i}{b_i}$, i.e., a unique choice for r_i. Therefore, there are at most q choices for each r_i and hence at most q^q choices for a_1.

Now, we discuss the choices for a_2 through e_2. The following cases arise:

- If $e_2 = 0$, then e is a constant vector, i.e., $e \equiv 0 \pmod{h(x)}$ and we get a contradiction to the choice of e.
- If $0 \neq e_2 \in R_q$, then $e_2 = b_1\eta_1 + b_2\eta_2 + \cdots + b_q\eta_q$ and $f_2 = \beta_1\eta_1 + \beta_2\eta_2 + \cdots + \beta_q\eta_q$ for some $\beta_i, b_i \in \mathbb{F}_{q^{n-1}}$, $1 \leq i \leq q$ and $b_i \neq 0$ for at least one i. Now, $f_2 = e_2a_2$ implies that

$$\beta_1\eta_1 + \beta_2\eta_2 + \cdots + \beta_q\eta_q = s_1b_1\eta_1 + s_2b_2\eta_2 + \cdots + s_qb_q\eta_q.$$

  If $b_i = 0$, then we have q^{n-1} choices for s_i, otherwise $s_i = \frac{\beta_i}{b_i}$, i.e., a unique choice for s_i. Also, not all b_i are zero. Therefore, we can conclude that there are at most q^{n-1} choices for each s_i and at most $q^{(n-1)(q-1)}$ choices for a_2.

Combining both the cases (for a_1 and a_2), we conclude that there are at most $q^{n(q-1)+1}$ double circulant codes C_a which contains z. □

Lemma 4 *For any non-zero vector $z = (e, f) \in R_q^{2n}$ such that e is not a constant vector, there are at most $2^q(1 + q^{\frac{n-1}{2}})^{(q-1)}$ self-dual double circulant codes $C_a = (1, a)$ such that $z \in C_a$.*

Proof Using Theorem 4, we have at most q^q choices for the first constituent code C_1 of C_a.

Now, we discuss the choices for the second constituent code, i.e., choices for a_2 through e_2. Let $a_2 = s_1\eta_1 + s_2\eta_2 + \cdots + s_q\eta_q$, for some $s_i \in \mathbb{F}_{q^{n-1}}$, $1 \leq i \leq q$.

- If $e_2 = 0$, then e is a constant vector, i.e., $e \equiv 0 \pmod{h(x)}$ and we get a contradiction to the choice of e.
- If $0 \neq e_2 \in R_q$, then $e_2 = b_1\eta_1 + b_2\eta_2 + \cdots + b_q\eta_q$ and $f_2 = \beta_1\eta_1 + \beta_2\eta_2 + \cdots + \beta_q\eta_q$ for some $\beta_i, b_i \in \mathbb{F}_{q^{n-1}}$, $1 \leq i \leq q$ and $b_i \neq 0$ for at least one i. Now, $f_2 = e_2a_2$ implies that

$$\beta_1\eta_1 + \beta_2\eta_2 + \cdots + \beta_q\eta_q = s_1b_1\eta_1 + s_2b_2\eta_2 + \cdots + s_qb_q\eta_q.$$

  If $b_i = 0$, then we have q^{n-1} choices for s_i, otherwise $s_i = \frac{\beta_i}{b_i}$, i.e., a unique choice for s_i. Also, we have $1 + a_2\bar{a}_2 = 1 + a_2a_2^{q^{\frac{n-1}{2}}} = 0$ (since C_a is self-dual). This implies that $s_is_i^{q^{\frac{n-1}{2}}} = -1$, i.e., $Norm(s_i) = -1$ for $1 \leq i \leq q$. Therefore, we have at most $1 + q^{\frac{n-1}{2}}$ choices for each s_i and hence $(1 + q^{\frac{n-1}{2}})^{q-1}$ choices for each a_2.

Combining these cases (for a_1 and a_2), we conclude that there are at most $2^q(1 + q^{\frac{n-1}{2}})^{q-1}$ double circulant codes C_a which contains z. □

Using the Artin's conjecture [22] for primitive roots, we have that for a fixed non-square q, there are infinitely many primes n for which $x^n - 1$ factors into two irreducible polynomials given in (2) (since q is a primitive root modulo n). Therefore, we get an infinite family of double circulant codes over R and the following result can be derived.

Theorem 6 *Let q be a power of an odd prime, and $\delta > 0$ be given. Then there are families of double circulant self-dual (resp. LCD) codes of length $2n$ over R_q, with code rate $\frac{1}{2}$, and with Gray images of relative distance δ as long as $H_q(\delta) < \frac{1}{4q}$ (resp. $H_q(\delta) < \frac{1}{2q}$). Moreover, we conclude that both of these families of codes are good.*

Proof Let A_n denote the size of the family. Then for large enough n (near infinity), by using Theorem 4 and Theorem 5, $A_n \approx 2^q q^{\frac{(n-1)q}{2}}$ for self-dual and $A_n \approx q^{nq}$ for LCD double circulant codes. Let $B(d_n)$ be the number of elements in R_q^{2n} whose image under ϕ have Hamming weight less than d_n. We assume that the inequality

$$A_n > a_nB(d_n), \tag{3}$$

where $a_n = 2^q(1+q^{\frac{n-1}{2}})^{(q-1)}$ for self-dual and $q^{n(q-1)+1}$, for LCD codes, is satisfied. Therefore, by Lemma 3 and Lemma 4, we conclude that in the family, there exist codes of length $2n$ over R_q whose images under ϕ have Hamming distance $\geq d_n$.
To enforce inequality (3) for large n, we make the following argument. We consider δ as 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 $d_n = 2q\delta n$. Then by [14, Lemma 2.10.3], we get $B(d_n)$ is approximately equal to $q^{2qnH_q(\delta)}$. If $H_q(\delta) = \frac{1}{2q}$ for LCD, and $= \frac{1}{4q}$ for self-dual codes, then

$$a_n B(d_n) \approx q^{n(q-1)+1} q^{2qnH_q(\delta)} = q^{nq+1} \approx q^{nq}$$
$$a_n B(d_n) \approx 2^q(1+q^{\frac{n-1}{2}})^{(q-1)} q^{2qnH_q(\delta)} \approx 2^q q^{\frac{(n-1)(q-1)}{2}} q^{\frac{n}{2}} \approx 2^q q^{\frac{(n-1)q}{2}}$$

for LCD and self-dual codes, respectively. From this, we can see that if $H_q(\delta) < \frac{1}{2q}$ for LCD, and $< \frac{1}{4q}$ for self-dual codes, then inequality (3) holds for n large enough. □

5 Examples

In this section, we construct some examples of LCD double circulant codes over R_q for $q = 3$ to validate our results.
Let $G = (I, A)$ be the generator matrix of a double circulant code C over $R_q = \mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{q-1}\mathbb{F}_q, u^q = u$, where I is the identity matrix of order n and $A = A_1 + uA_2 + \cdots + u^{q-1}A_q$, for $n \times n$ matrices $A_1, A_2, \ldots, A_q$ over $\mathbb{F}_q$. Then the generator matrix of $\phi(C)$ is of order $nq \times 2nq$ whose rows are $\phi(G)$, $\phi(uG), \ldots, \phi(u^{q-2}G)$ and $\phi(u^{q-1}G)$, respectively.

In particular for $q = 3$ here we explicitly discuss its Gray map and generator matrix. In fact, for $q = 3$ we have $\eta_1 = 1 - u^2, \eta_2 = \frac{u^2+u}{2}, \eta_3 = \frac{u^2-u}{2}$. Also, any element of R_3 can be written as

$$a + bu + cu^2 = a\eta_1 + (a + b + c)\eta_2 + (a - b + c)\eta_3.$$

Therefore, the Gray map $\phi : R_3 \longrightarrow \mathbb{F}_3^3$ is defined by

$$\phi(a + bu + cu^2) = (a, a + b + c, a - b + c).$$

Now, let C be a double circulant code over $R_3 = \mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$ with generator matrix of the form $G = (I, A)$, where I is the identity matrix of order n and $A = A_1 + uA_2 + u^2A_3$, for $n \times n$ matrices A_1, A_2 and A_3 over $\mathbb{F}_3$. Then the generator matrix of $\phi(C)$ is given by

$$\hat{G} = \begin{pmatrix} \phi(G) \\ \phi(uG) \\ \phi(u^2G) \end{pmatrix} = \begin{pmatrix} I & I & I & A_1 & A_1 + A_2 + A_3 & A_1 + 2A_2 + A_3 \\ 0 & I & 2I & 0 & A_1 + A_2 + A_3 & 2A_1 + A_2 + 2A_3 \\ 0 & I & I & 0 & A_1 + A_2 + A_3 & A_1 + 2A_2 + A_3 \end{pmatrix}_{3n \times 6n}.$$

By using this generator matrix and the Magma computation system [3], we now construct some LCD codes as $\mathbb{F}_3$-images of double circulant codes of length $2n$ over R_3 in Table 1. In second to fourth columns we have provided polynomials $a_i(x)$, for $i = 1, 2, 3$, respectively such that the generator polynomial of C over R_3 is $(1, a(x))$ where $a(x) = a_1(x) + ua_2(x) + u^2a_3(x)$. Also, these polynomials are given (in Table 1) by their coefficients in decreasing powers of x. For example, 1234 represents the polynomial $x^3 + 2x^2 + 3x + 4$.

Example 1 Take $\alpha = 2$, a primitive element of $\mathbb{F}_5$. Then $\eta_1 = 1 - u^4, \eta_2 = \frac{u+u^2+u^3+u^4}{4}, \eta_3 = \frac{\alpha u+\alpha^2u^2+\alpha^3u^3+u^4}{4}, \eta_4 = \frac{\alpha^2u+u^2+\alpha^2u^3+u^4}{4}$ and $\eta_5 = \frac{\alpha^3u+\alpha^2u^2+\alpha u^3+u^4}{4}$ are pairwise orthogonal idempotent elements of R_5. Also, an element $r = a + bu + cu^2 + du^3 + eu^4 \in R_5$ can be written as

$$r = a\eta_1 + (a+b+c+d+e)\eta_2 + (a+3b+4c+2d+e)\eta_3 + (a+4b+c+4d+e)\eta_4 + (a+2b+4c+3d+e)\eta_5.$$

In that case, the Gray map $\phi : R_5 \longrightarrow \mathbb{F}_5^5$ is defined by

$$\phi(r) = (a, a + b + c + d + e, a + 3b + 4c + 2d + e, a + 4b + c + 4d + e, a + 2b + 4c + 3d + e).$$

Now, let $C = (1, a(x))$ be a double circulant code of length $2n$ over R_5, where $a(x) = a_1(x) + ua_2(x) + u^2a_3(x) + u^3a_4(x) + u^4a_5(x)$. Then, $\phi(C)$ is a $[10n, 5n]$- code over $\mathbb{F}_5$. Moreover, duality is preserved under this map, i.e., the Gray image of self-dual (resp. LCD) code is a self-dual (resp. LCD) code.

Table 1: LCD codes from Gray images of double circulant codes of length $2n$ over R_3

n	$a_1(x)$	$a_2(x)$	$a_3(x)$	$\phi(C)$ (LCD)
7	1021112	1101200	21011211	$[42, 21, 5]_3$
8	21121012	02120112	12100222	$[48, 24, 5]_3$
11	12101202112	12122221212	01222022111	$[66, 33, 6]_3$
12	121012221120	202222100221	220222112012	$[72, 36, 6]_3$
13	1210122011212	2122221002212	2222221120122	$[78, 39, 7]_3$
14	12101220112122	21222210022122	22222211201222	$[84, 42, 7]_3$
16	1210222021222022	2212202210201121	2022202221120102	$[96, 48, 8]_3$
17	12121222211212220	02122022102021202	20222222211201002	$[102, 51, 8]_3$

1. If $n = 2$, take $a_1(x) = 2x, a_2(x) = x + 2, a_3(x) = 2x + 3, a_4(x) = 4x$ and $a_5(x) = x + 2$, then C is a self-dual code and its Gray image $\phi(C)$ is also a self-dual code over $\mathbb{F}_5$ with parameters $[20, 10, 2]$.
2. If $n = 3$, take $a_1(x) = x^2 + 3x + 3, a_2(x) = x^2 + x + 2, a_3(x) = 2x^2 + x + 1, a_4(x) = x^2 + x + 2$ and $a_5(x) = 2x^2 + x + 1$, then C is a self-dual code and its Gray image $\phi(C)$ is also a self-dual code over $\mathbb{F}_5$ with parameters $[30, 15, 4]$.

6 1-generator quasi-cyclic (QC) codes

In the present section, we discuss the algebraic structure of 1-generator quasi-cyclic (QC) code over R_q for $q = 3$. It is worth mentioning that 1-generator quasi-cyclic codes for $q = 2$ are extensively studied in [25]. They obtained their minimal spanning sets and binary Gray images. The 1-generator QC codes over R_q for any $q > 3$ can be obtained but for the sake of calculation, here we restrict to $q = 3$. Now, we start our discussion with the definition of QC codes.

Definition 1 Let C be a linear code over R_q of length $n = sl$ and σ be the cyclic shift operator on R_q^n. Then C is said to be a quasi-cyclic (QC) code with index s (or s-QC code), if $\sigma^s(C) = C$. Evidently, if $s = 1$, then C is a cyclic code.

Definition 2 A quasi-cyclic (QC) code over R_q generated by a single element is called a 1-generator quasi-cyclic code.

Note that any two polynomials $p(x)$ and $q(x)$ in $R_q[x]$ are said to be relatively prime if there exist two polynomials $m_1(x), m_2(x) \in R_q[x]$ such that $p(x)m_1(x) + q(x)m_2(x) = 1$. Based on this, we provide a result which will be used to study 1-generator quasi-cyclic (QC) codes.

Lemma 5 *[25, Lemma 2.4] Let $C = \langle g(x) \rangle$ be a cyclic code of length n over R_q with generator polynomial $g(x)$. Then $C = \langle g(x)f(x) \rangle$ for any polynomial $f(x)$ such that $f(x)$ and $\frac{x^n-1}{g(x)}$ are relatively prime.*

Theorem 7 *Let C be an s-QC code of length $n = sl$ over R_q. Then $\phi(C)$ is an sq-QC code of length nq over $\mathbb{F}_q$.*

Proof Let C be an s-QC code over R_q and $v = (v_{11}, v_{12}, \ldots, v_{1s}, v_{21}, v_{22}, \ldots, v_{2s}, \ldots, v_{l1}, v_{l2}, \ldots, v_{ls}) \in C$, where $v_{ij} = \sum_{k=1}^{q} \eta_k r_{ij}^{(k)}$ for $1 \leq i \leq l, 1 \leq j \leq s$. Then $\sigma^s(v) \in C$ and

$$\begin{aligned}\phi(v) =&(r_{11}^{(1)}, r_{11}^{(2)}, \ldots, r_{11}^{(q)}, \ldots, r_{1s}^{(1)}, r_{1s}^{(2)}, \ldots, r_{1s}^{(q)}, r_{21}^{(1)}, r_{21}^{(2)}, \ldots, r_{21}^{(q)}, \ldots,\\ & r_{2s}^{(1)}, r_{2s}^{(2)}, \ldots, r_{2s}^{(q)}, \ldots, r_{l1}^{(1)}, r_{l1}^{(2)}, \ldots, r_{l1}^{(q)}, \ldots, r_{ls}^{(1)}, r_{ls}^{(2)}, \ldots, r_{ls}^{(q)}).\end{aligned}$$

Therefore,

$$\begin{aligned}\sigma^{sq}(\phi(v)) =&(r_{l1}^{(1)}, r_{l1}^{(2)}, \ldots, r_{l1}^{(q)}, \ldots, r_{ls}^{(1)}, r_{ls}^{(2)}, \ldots, r_{ls}^{(q)}, r_{11}^{(1)}, r_{11}^{(2)}, \ldots, r_{11}^{(q)}, \ldots, r_{1s}^{(1)},\\ & r_{1s}^{(2)}, \ldots, r_{1s}^{(q)}, \ldots, r_{l-11}^{(1)}, r_{l-11}^{(2)}, \ldots, r_{l-11}^{(q)}, \ldots, r_{l-1s}^{(1)}, r_{l-1s}^{(2)}, \ldots, r_{l-1s}^{(q)})\\ =&\phi(v_{l1}, v_{l2}, \ldots, v_{ls}, v_{11}, v_{12}, \ldots, v_{1s}, \ldots, v_{l-11}, v_{l-12}, \ldots, v_{l-1s})\\ =&\phi\sigma^s(v) \in \phi(C).\end{aligned}$$

Thus, $\phi(C)$ is an sq-QC code of length nq over $\mathbb{F}_q$. □

Let C be an s-QC code of length $n = sl$ over R_q. Then we can define a one-one correspondence

$$\Gamma : R_q^n \to R_{q,l}^s$$

by

$$\Gamma(v_{11}, v_{12}, \ldots, v_{1s}, v_{21}, v_{22}, \ldots, v_{2s}, \ldots, v_{l1}, v_{l2}, \ldots, v_{ls}) = (v_1(x), v_2(x), \ldots, v_s(x)),$$

where $v_j(x) = \sum_{i=1}^{l} v_{ij} x^{i-1}$ and $R_{q,l} = \frac{R_q[x]}{\langle x^l - 1 \rangle}$. It can be easily seen that an s-QC code of length $n = sl$ over R_q corresponds to an $R_{q,l}$-submodule of $R_{q,l}^s$.

Theorem 8 *Let C be a 1-generator s-QC code of length $n = sl$ over $R_3 = \mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$, where $u^3 = u$. If C is generated by $G(x) = (G_1(x), G_2(x), \ldots, G_s(x))$ where $G_i(x) \in R_{3,l} = R_3[x]/\langle x^\ell - 1 \rangle$, then $G_i(x) \in B_i$ for some cyclic codes B_i in $R_{3,l}$, $1 \le i \le s$ and there exist polynomials $f_i(x) \in R_3[x]$, $r_i^{(j)}(x) \in \mathbb{F}_3[x]$, $1 \le i \le s$, $j = 1, 2, 3$ such that $G_i(x) = f_i(x)(\eta_1 r_i^{(1)}(x) + \eta_2 r_i^{(2)}(x) + \eta_3 r_i^{(3)}(x))$.*

Proof Let C be a 1-generator s-QC code of length $n = sl$ over R_3 generated by $G(x) = (G_1(x), G_2(x), \ldots, G_s(x))$. Then $\Gamma_i(C)$ is a cyclic code where Γ_i is the i-th projection defined as $\Gamma_i(G_1(x), G_2(x), \ldots, G_s(x)) = G_i(x)$. Therefore, using Theorem 2 and Lemma 5 we get that a generator $G_i(x)$ of $\Gamma_i(C)$ is of the form $G_i(x) = f_i(x)(\eta_1 r_i^{(1)}(x) + \eta_2 r_i^{(2)}(x) + \eta_3 r_i^{(3)}(x))$ for some polynomials $f_i(x) \in R_3[x]$, $r_i^{(j)}(x) \in \mathbb{F}_3[x]$, $1 \le i \le s$, $j = 1, 2, 3$. □

Note that $G_i(x)$ can also be written in the form $G_i(x) = a_i(x)\eta_1 + b_i(x)\eta_2 + c_i(x)\eta_3$ for some polynomials $a_i(x), b_i(x), c_i(x) \in \mathbb{F}_3[x]$, $1 \le i \le s$. The following theorem provides a minimal generating set for a 1-generator s-QC code C over R_3.

Theorem 9 *Let C be a 1-generator s-QC code over R_3 of length $n = sl$ and the generator*

$$G(x) = (a_1(x)\eta_1 + b_1(x)\eta_2 + c_1(x)\eta_3, \ldots, a_s(x)\eta_1 + b_s(x)\eta_2 + c_s(x)\eta_3)$$

where $a_i(x), b_i(x), c_i(x) \in \mathbb{F}_3[x]$, for all $1 \le i \le s$. Let

$$g(x) = \gcd(a_1(x)\eta_1 + b_1(x)\eta_2 + c_1(x)\eta_3, \ldots, a_s(x)\eta_1 + b_s(x)\eta_2 + c_s(x)\eta_3, x^l - 1),$$

and $h(x)$ be a polynomial such that

$$g(x)h(x) = x^l - 1.$$

Then C is free R_3-submodule with basis $B = \bigcup_{i=0}^{\deg(h)-1} \{x^i G(x)\}$ and $rank(C) = \deg(h(x))$.

Proof Any codeword $c(x) \in C$ is of the form $c(x) = f(x)G(x)$, where $f(x) \in R_3[x]$. If $\deg(f(x)) \le \deg(h(x)) - 1$, then $c(x) = f(x)G(x) \in span(B)$. Otherwise, by division algorithm $f(x) = h(x)q_1(x) + s_1(x)$ for some $q_1(x), s_1(x) \in R_3[x]$ where $\deg(s_1(x)) \le \deg(h(x)) - 1$. Then

$$\begin{aligned} f(x)G(x) =& (h(x)q_1(x) + s_1(x))G(x) \\ =& q_1(x)h(x)G(x) + s_1(x)G(x), \text{ where } s_1(x)G(x) \in span(B). \end{aligned}$$

Since $h(x)(a_i(x)\eta_1 + b_i(x)\eta_2 + c_i(x)\eta_3) = 0$ for all $1 \le i \le s$, we have $q_1(x)h(x)G(x) = (0, 0, \ldots, 0) \in span(B)$. Therefore, B spans C. Now, we show that none of the element of B can be written as the linearly combination of other elements of B. Let $\alpha_0, \alpha_1, \ldots, \alpha_{t-1} \in R_3$ where $t = \deg(h(x))$ be such that

$$\sum_{j=0}^{t-1} \alpha_j x^j G(x) = 0,$$

i.e.,

$$\sum_{j=0}^{t-1} \alpha_j x^j (a_i(x)\eta_1 + b_i(x)\eta_2 + c_i(x)\eta_3) = 0, \text{ for all } 1 \le i \le s. \tag{4}$$

Comparing the constant term on both sides of the above equation, we get $\alpha_0(a_i\eta_1 + b_i\eta_2 + c_i\eta_3)(0) = 0$, where $(a_i\eta_1 + b_i\eta_2 + c_i\eta_3)(0)$ is invertible (since each of $a_i(0), b_i(0), c_i(0)$ are non-zero). This implies $\alpha_0 = 0$. Substituting the value of α_0 and comparing the coefficients of x in (4), we get $\alpha_1 = 0$. Similarly, $\alpha_j = 0$ for all $0 \le j \le t - 1$. That is, B is linearly independent and hence none of the element of B belongs to the span of remaining elements of B. □

Theorem 10 *Let C be a 1-generator s-QC code of length $n = sl$ over R_3 generated by $G(x) = (g(x)f_1(x), g(x)f_2(x), \ldots, g(x)f_s(x))$ for some divisor $g(x)$ of $x^l - 1$ and $\gcd(f_i(x), \frac{x^l-1}{g(x)}) = 1$ for each $1 \leq i \leq s$. Then $B' = \{G(x), xG(x), \ldots, x^{l-t-1}G(x)\}$, where $\deg(g(x)) = t$ is a basis for C and $\frac{d_L(C)}{s} \geq d_L(C')$, where $C' = (g(x))$ is a cyclic code of length l over R_3.*

Proof The proof is similar to [25, Theorem 3.7]. □

Now, we present an example as suggested by Theorem 10 and obtain a ternary 6-QC code as below.

Example 2 Let $l = 10$ and

$$g_1(x) = g_2(x) = (x+2)(x^4 + 2x^3 + x^2 + 2x + 1) = x^5 + x^4 + 2x^3 + x^2 + 2x + 2,$$
$$g_3(x) = (x+1)(x^4 + x^3 + x^2 + x + 1) = x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 1.$$

Then $g_1(x), g_2(x), g_3(x)$ are factors of $x^{10} - 1$ in $\mathbb{F}_3[x]$. Therefore $C' = \langle g(x) \rangle$ is a cyclic code of length 10 over $R_3 = \mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$, where $g(x) = \sum_{i=1}^{3} \eta_i g_i(x)$. Hence, C' has $9^5 = 59049$ codewords and minimum Lee distance 4. Also, by Theorem 10, C is a 2-QC code given by $G(x) = \langle g(x)f_1(x), g(x)f_2(x) \rangle$, where $f_1(x), f_2(x)$ satisfying the conditions mentioned in Theorem 10. In this way, C has the parameters $[20, 5, \geq 8]$ and its ternary image $[60, 15, \geq 8]$ is a 6-QC code.

7 Conclusion

The main purpose of the article is to enumerate self-dual and LCD double circulant codes over R_q whose Gray images (both self-dual and LCD) are proved to be good enough. In addition, algebraic properties of 1-generator QC codes are obtained. Besides, we have also provided several examples of LCD double circulant codes over R_3. It is worth mentioning that self-dual double circulant codes do not exist over R_3 due to Theorem 1. Therefore, like Table 1, it would be worthwhile to compute numerical examples of self-dual double circulant codes over R_q for the q's meeting the hypotheses of Theorem 1. Further, one can derive similar results for more general ring $\mathbb{F}_q[u]/\langle f(u) \rangle$ (appeared in [10]), where $f(u)$ splits into linear factors over $\mathbb{F}_q$.

References

1. Alahmadi, A., Guneri, C., Ozkaya, B., Shoaib, H., Solé. P.: On self-dual double negacirculant codes. Discret. Appl. Math. **222**, 205-212 (2017).
2. Alahmadi, A., Ozdemir, F., Solé, P.: On self-dual double circulant codes. Des. Codes Cryptogr. **86**(6), 1257-1265 (2018).
3. Bosma, W., Cannon, J.: *Handbook of Magma Functions*. Univ. of Sydney (1995).
4. Cao, Y.: 1-generator quasi-cyclic codes over finite chain rings. Appl. Algebra Engrg. Comm. Comput. **24**, 53-72 (2013).
5. Carlet, C., Guilley, S.: Complementary dual codes for counter-measures to side-channel attacks. Adv. Math. Commun. **10**(1), 131-150 (2016).
6. Cui. J., Pei, J.: Quaternary 1-generator quasi cyclic codes. Des. Codes Cryptogr. **58**, 23-33 (2011).
7. Gao, Y., Gao, J., Wu, T., Fu, F. W.: 1-Generator quasi-cyclic and generalized quasi-cyclic codes over the ring $\mathbb{Z}_4[u]/\langle u^2 - 1 \rangle$. Appl. Algebra Engrg. Comm. Comput. **28**(6), 457-467 (2017).
8. Goyal, M., Raka, M.: Duadic codes over the ring $\mathbb{F}_q[u]/\langle u^m - u \rangle$ and their Gray images. J. Comp. Comm. **4**(12), 50-62 (2016).
9. Goyal, M., Raka, M.: Quadratic residue codes over the ring $\mathbb{F}_p[u]/\langle u^m - u \rangle$ and their Gray images. Cryptogr. Commun. **10**, 343-355 (2018).
10. Goyal, M., Raka, M.: Duadic negacyclic codes over a finite non-chain ring. Discrete Math. Algorithms Appl. 10(06), 1850080 (2018).
11. Gulliver, T. A., Bhargava, V. K.: Some best rate $\frac{1}{p}$ and rate $\frac{p-1}{p}$ systematic quasi-cyclic codes. IEEE Trans. Inform. Theory. **37**, 552-555 (1991).
12. Gulliver, T. A., Bhargava, V. K.: Twelve good rate $\frac{(m-r)}{pm}$ binary quasi-cyclic codes. IEEE Trans. Inform. Theory **39**, 1750-1751 (1993).
13. 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).
14. Huffman, W. C., Pless, V.: Fundamentals of Error Correcting Codes, Cambridge University Press (2003).
15. 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).
16. Islam, H., Martínez-Moro, E., Prakash, O. Cyclic codes over a non-chain ring $R_{e,q}$ and their application to LCD codes. Discrete Math. **344**(10), 112545 (2021).
17. Islam, H., Prakash, O.: Construction of LCD and new quantum codes from cyclic codes over a finite non-chain ring. Cryptogr. Commun. **14**, 59-73 (2022).

18. Ling, S., Solé, P.: On the algebraic structure of quasi-cyclic codes I: Finite fields, IEEE Trans. Inform. Theory **47**(7), 2751-2760 (2001).
19. Ling, S., Solé, P.: On the algebraic structure of quasi-cyclic codes II: Chain rings. Des. Codes Cryptogr. **30**(1), 113-130 (2003).
20. Li, C., Ding, C., Li, S.: LCD cyclic codes over finite fields. IEEE Trans. Inform. Theory **63**(7), 4344-4356 (2017).
21. Liu, X., Liu, H.: LCD codes over finite chain rings. Finite Fields Appl. **34**, 1-19 (2015).
22. Moree, P.: Artin's primitive root conjecture a survey. Integers **10**(6), 1305-1416 (2012).
23. Massey, J. L.: Linear codes with complementary duals. Discrete Math. **106/107**, 337-342 (1992).
24. Lidl, R., Niederreiter, H.: Finite Fields. Addison-Wesley, Reading (1983).
25. Ozen, M., Ozzaim, N. T., Aydin, N.: One generator quasi-cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$. J. Appl. Math. Inform. **36**(5-6), 359-368 (2018).
26. Prakash, O., Yadav, S., Verma, R. K.: Constacyclic and Linear Complementary Dual codes over $\mathbb{F}_q + u\mathbb{F}_q$. Defence Sci. J. **70**(06), 626-632 (2020).
27. Seguin, G. E.: A class of 1-generator quasi-cyclic codes. IEEE Trans. Inform. Theory **50**, 1745-1753 (2004).
28. 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).
29. Shi, M., Huang, D., Sok, L., Solé, P.: Double circulant LCD codes over $\mathbb{Z}_4$. Finite Fields Appl. **58**, 133-144 (2019).
30. Shi, M., Huang, D., Sok, L., Solé, P.: Double circulant self-dual and LCD codes over Galois ring. arXiv:1801.06624 (2018).
31. Shi, M., Zhu, H., Qian, L., Solé, P.: On self-dual four circulant codes. Int. J. Found. Comput. Sci. **29**(07), 1143-1150 (2018).
32. Shi, M., Sok, L., Aydin, N., Solé, P.: On constacyclic codes over $\mathbb{Z}_4[u]/\langle u^2 - 1\rangle$. Finite Fields Appl. **45**, 86-95 (2015).
33. Siap, I., Abualrub, T., Yildiz, B.: One generator quasi-cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$. J. Frank. Inst. **349**, 284-291 (2012).
34. Ventou, M., Rigoni, C.: Self-dual double circulant codes. Discrete Math. **56**(2-3), 291-298 (1985).
35. Yadav, S., Islam, H., Prakash, O., Solé. P.: Self-dual and LCD double circulant and double negacirculant codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$. J. Appl. Math. Comput. https://doi.org/10.1007/s12190-021-01499-9 (2021).
36. Yadav, S., Prakash, O.: Enumeration of LCD and Self-dual Double Circulant Codes Over $\mathbb{F}_q[v]/\langle v^2 - 1\rangle$. Proceedings of Seventh International Congress on Information and Communication Technology https://doi.org/10.1007/978-981-19-1607-6_21 (2022).
37. Yao, T., Zhu, S., Kai, X.: On self-dual and LCD double circulant codes over a non-chain ring. Chinese J. Electron. **28**(5), 1018-1024 (2019).
38. Zhu, H., Shi, M.: On linear complementary dual four circulant codes. Bull. Aust. Math. Soc. **98**(1), 159-166 (2018).