International Journal of Informatics and Applied Mathematics
e-ISSN:2667-6990 Vol. 6, No. 2, 8-19

A Class of LCD Codes Through Cyclic Codes Over $\mathbb{Z}_p R$

Zineb Hebbache[1,2] and Amit Sharma[3]

[1] National School of Built and Ground Works Engineering NSBGWE (ENSTP), Street of Sidi Garidi, B.P. 32, Kouba, 16051, Algiers, Algeria
[2] Laboratory of Algebra and number theory, Faculty of Mathematics, U.S.T.H.B., B.P. 32, 16111 El-Alia, Algiers, Algeria.
z.hebbache@enstp.edu.dz
[3] Department of Mathematics and Humanities, S.V. National Institute of Technology Surat, Surat, India.
apsharmaiitr@gmail.com

Abstract. In recent time, some mixed types of alphabets have been considered for constructing error correcting codes. These constructions include $\mathbb{Z}_2\mathbb{Z}_4-$additive codes, $\mathbb{Z}_2\mathbb{Z}_2[u]-$linear codes et cetera. In this paper, we studied a class of codes over a mixed ring $\mathbb{Z}_pR$ where $R = \mathbb{Z}_p + v\mathbb{Z}_p + v^2\mathbb{Z}_p, v^3 = v$. We determined an algebraic structure of these codes under certain conditions. We have also constructed a class of LCD cyclic codes over $\mathbb{Z}_pR$. A necessary and sufficient condition for a cyclic code to be a complementary dual (LCD) code has been obtained.

Keywords: Linear Cyclic Codes · Codes Over Mixed Alphabets · Gray Map · LCD Codes.

Received: 03 December 2022 | Revised: 03 August 2023 | Accepted: 10 September 2023

1 Introduction

As we know, cyclic codes possess a nice algebraic structures as they are easy to understand and implement. In recent time, linear codes, or in particular cyclic codes, have been studied over mixed alphabets. In 1973, Delsarte [1] introduced additive codes which can be viewed as subgroups of the underlying abelian group of the form $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. Later, many scholars paid more attention to additive codes. Abualrub *et al.* [2] and Borges *et al.* [3] introduced $\mathbb{Z}_2\mathbb{Z}_4-$additive cyclic codes. They investigated the generator matrix and the duality of the family of codes. Aydogdu *et al.* [4],[5] generalized $\mathbb{Z}_2\mathbb{Z}_4-$additive codes to $\mathbb{Z}_2\mathbb{Z}_{2^s}-$additive codes and $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}-$additive codes. Afterwards, some papers focused on additive codes appeared, such as [6],[7],[8], [9].

LCD codes were first introduced by Massey [10]. This family of codes have shown effectiveness against side-channel attacks(SCA) and fault injection attacks(FIA) to improve the security related information on sensitive devices [11]. Authors have explored properties of LCD codes with various conditions and structures in [12], [13], [14]. To the best of our knowledge, there is no study yet on linear cyclic codes over $\mathbb{Z}_p \times (\mathbb{Z}_p + v\mathbb{Z}_p + v^2\mathbb{Z}_p)$ with $v^3 = v$. Unlike the finite chain ring $\mathbb{Z}_p + u\mathbb{Z}_p + u^2\mathbb{Z}_p$ with $u^3 = 0$, the ring $\mathbb{Z}_p + v\mathbb{Z}_p + v^2\mathbb{Z}_p$ with $v^3 = v$ is a non-chain ring, and hence many algebraic properties of $\mathbb{Z}_p(\mathbb{Z}_p + u\mathbb{Z}_p + u^2\mathbb{Z}_p)$ and $\mathbb{Z}_p(\mathbb{Z}_p + v\mathbb{Z}_p + v^2\mathbb{Z}_p$ vary. We have chosen an other approach to define this class in this paper and then a class of LCD codes have been constructed.

The paper is organized as follows. In Section 2, we give some basic results about the ring $R = \mathbb{Z}_p + v\mathbb{Z}_p + v^2\mathbb{Z}_p, v^3 = v$, and linear codes over $\mathbb{Z}_pR$. In Section 3, we study some structural properties of cyclic codes over R. In Section 4, cyclic codes over $\mathbb{Z}_pR$ are studied. In Section 5, necessary and sufficient conditions for cyclic codes to be LCD codes over $\mathbb{Z}_p$ are given. Finally, we construct some LCD codes from $\mathbb{Z}_pR-$linear cyclic codes.

2 Preliminaries

Let R be a commutative ring with characteristic p defined as $\mathbb{Z}_p+v\mathbb{Z}_p+v^3\mathbb{Z}_p = \{a+vb+v^2c \mid a, b, c \in \mathbb{Z}_p\}$, $v^3 = v$. The ring R can be considered as the quotient ring $\mathbb{Z}_p[v]/\langle v^3 - v\rangle$. It can be easily checked that R is a principal ideal ring but not a finite chain ring.

Define $\epsilon_1 = 1 - v^2, \epsilon_2 = \frac{v+v^2}{2}$ and $\epsilon_3 = \frac{v^2-v}{2}$. Then $\epsilon_i^2 = \epsilon_i, \epsilon_i\epsilon_j = 0$ and $\sum_{i=1}^{3} \epsilon_i = 1$ for $i \neq j$ and $i, j \in \{1, 2, 3\}$. By Chinese remainder theorem, we have $R = \epsilon_1\mathbb{Z}_p \oplus \epsilon_2\mathbb{Z}_p \oplus \epsilon_3\mathbb{Z}_p$.

We define a Gray map on R as follows:

$$\phi : R \to \mathbb{Z}_p^3$$

$$a + vb + v^2c \mapsto (a, a + b + c, a - b + c);$$

Recall the following definitions.

Definition 1. *[15] Let* $\mathbf{x} = (x \mid r) \in \mathbb{Z}_p^\alpha \times R^\beta$*, where* $x = (x_0, \ldots, x_{\alpha-1}) \in \mathbb{Z}_p^\alpha$ *and* $r = (r_0, \ldots, r_{\beta-1}) \in R^\beta$*. Then the Lee weight of* $\mathbf{x}$ *is defined as*

$$w_L(\mathbf{x}) = w_H(\phi(\mathbf{x})),$$

where w_H *denotes the Hamming weight.*

Definition 2. *Let* $(\mathbf{x}, \mathbf{w}) \in \mathbb{Z}_p^\alpha \times R^\beta$*. Then the Lee distance of* $\mathbf{x}$ *and* $\mathbf{w}$ *is defined as*

$$d_L(\mathbf{x}, \mathbf{w}) = w_L(\mathbf{x} - \mathbf{w}).$$

For any element $r \in R, r$ can be expressed uniquely as $r = a + vb + v^2c$, where $a, b, c \in \mathbb{Z}_p$. We define the set

$$\mathbb{Z}_pR = \{(x, r) \mid x \in \mathbb{Z}_p, r \in R\}.$$

The ring $\mathbb{Z}_pR$ is not an $R-$module under standard multiplication , but to make it an $R-$module, we define the following map:

$$\begin{gathered} \eta : R \to \mathbb{Z}_p \\ r = a + vb + v^2c \mapsto a. \end{gathered} \tag{1}$$

Clearly the mapping η is a ring homomorphism. For any $l \in R$, we define the multiplication $\star$ as

$$l \star (x, r) = (\eta(l)x, lr).$$

And the map $\star$ can be naturally generalized to the ring $\mathbb{Z}_p^\gamma R^\beta$ as follows.
For any $l \in R$ and $w = (x_0, x_1, \ldots, x_{\alpha-1} \mid r_0, r_1, \ldots, r_{\beta-1}) \in \mathbb{Z}_p^\alpha R^\beta$ define

$$l \star w = (\eta(l)x_0, \eta(l)x_1, \ldots, \eta(l)x_{\alpha-1} \mid lr_0, lr_1, \ldots, lr_{\beta-1}),$$

where $(x_0, x_1, \ldots, x_{\alpha-1}) \in \mathbb{Z}_p^\alpha$ and $(r_0, r_1, \ldots, r_{\beta-1}) \in R^\beta$.

Thus we conclude that the ring $\mathbb{Z}_p^\alpha R^\beta$ is an R-module under the usual addition and the multiplication just defined above.

Definition 3. *A non-empty subset* C *of* $\mathbb{Z}_p^\alpha R^\beta$ *is called a* $\mathbb{Z}_pR$*-linear code if it is an* $R-$*submodule of* $\mathbb{Z}_p^\alpha R^\beta$*.*

Let C be a $\mathbb{Z}_pR$-linear code and let C_α (respectively, C_β) be the canonical projection of C on the first α (respectively, on the last β) coordinates. Since the canonical projection is a linear map, C_α and C_β are linear codes of lengths α and β (over $\mathbb{Z}_p$ and over R), respectively.

The Euclidean inner product on $\mathbb{Z}_p^\alpha R^\beta$ is calculated as follows. For any two vectors

$$\mathbf{t} = (x_0, \ldots, x_{\alpha-1} \mid r_0, \ldots, r_{\beta-1}), \mathbf{t}' = (x'_0, \ldots, x'_{\alpha-1} \mid r'_0, \ldots, r'_{\beta-1}) \in \mathbb{Z}_p^\alpha \times R^\beta,$$

we have

$$\langle \mathbf{t}, \mathbf{t}' \rangle = (1+v) \sum_{i=0}^{\alpha-1} x_i \acute{x}_i + \sum_{j=0}^{\beta-1} r_j \acute{r}_j.$$

Let C be a $\mathbb{Z}_pR$-linear code. The dual of C is defined by

$$C^{\perp} = \{\mathbf{t}' \in \mathbb{Z}_p^{\alpha} \times R^{\beta},\ \langle \mathbf{t}, \mathbf{t}' \rangle = 0 \text{ for all } \mathbf{t} \in C\}.$$

A linear code is called an Euclidean LCD (linear complementary dual) code if $C \cap C^{\perp} = \{0\}$.

Note that the Euclidean dual of a linear code C of length α over $\mathbb{Z}_p$ is defined as $C^{\perp} = \{x \in \mathbb{Z}_p^{\alpha} \mid \forall y \in C, \langle x, y \rangle = 0\}$ where for x, y in $\mathbb{Z}_p^{\alpha}$, $\langle x, y \rangle = \sum_{i=1}^{\alpha} x_i y_i$ is the scalar product of x and y.

3 Cyclic codes over R

This section deals with some structural properties of cyclic codes over R. All codes are assumed to be linear unless otherwise stated.

A code of length β over R is a nonempty subset of R^{β}. A code C_{β} is said to be linear if it is a submodule of the $R-$module R^{β}.

Let C_{β} be a linear code over R, define:

$$\begin{aligned} C_{\beta,1} &= \{a \in \mathbb{Z}_p^{\beta} \mid \epsilon_1 a + \epsilon_2 b + \epsilon_3 c, \forall a, b, c \in C_{\beta}\} \\ C_{\beta,2} &= \{b \in \mathbb{Z}_p^{\beta} \mid \epsilon_1 a + \epsilon_2 b + \epsilon_3 c, \forall a, b, c \in C_{\beta}\} \\ C_{\beta,3} &= \{c \in \mathbb{Z}_p^{\beta} \mid \epsilon_1 a + \epsilon_2 b + \epsilon_3 c, \forall a, b, c \in C_{\beta}\}. \end{aligned} \quad (2)$$

Then $C_{\beta,1}, C_{\beta,2}$ and $C_{\beta,3}$ are linear codes of length β over $\mathbb{Z}_p$. Moreover C_{β} can be uniquely expressed as $C_{\beta} = \epsilon_1 C_{\beta,1} \oplus \epsilon_2 C_{\beta,2} \oplus \epsilon_3 C_{\beta,3}$ with $|C_{\beta}| = |C_{\beta,1}||C_{\beta,2}||C_{\beta,3}|$ and $d_L(C_{\beta}) = \min\ \{d_H(C_{\beta,i}), i = 1,2,3\}$.

Let G_j be generator matrices of linear codes $C_{\beta,j}, j = 1,2,3$ respectively, then the generator matrix of C_{β} is

$$G = \begin{pmatrix} \epsilon_1 G_1 \\ \epsilon_2 G_2 \\ \epsilon_3 G_3 \end{pmatrix}$$

and the generator matrix of $\phi(C_{\beta})$ is

$$\phi(G) = \begin{pmatrix} \phi(\epsilon_1 G_1) \\ \phi(\epsilon_2 G_2) \\ \phi(\epsilon_3 G_3) \end{pmatrix}.$$

The following proposition is straightforward from the definition of the Gray map ϕ.

Proposition 1. *Let C_β be a linear code of length β over R with $|C_\beta| = M$ and minimum Lee distance $d_L(C_\beta) = d$. Then $\phi(C_\beta)$ is a linear code with parameters $(3\beta, M, d)$.*

A code C_β is said to be a cyclic, if C_β is closed under the cyclic shift defined as:

$$\rho : R^\beta \to R^\beta,$$

$$\rho(a_0, a_1, \ldots, a_{\beta-1}) = (a_{\beta-1}, a_0, \ldots, a_{\beta-2}).$$

Lemma 1. *A linear code C_β of length β over R is cyclic code if and only if C_β is a $R[x]-$submodule of $R[x]/\langle x^\beta - 1\rangle$.*

Proof. Straightforward.

Now we present some results on cyclic codes over R that are necessary to further study the cyclic codes over over $\mathbb{Z}_pR$.

Theorem 1. *Let $C_\beta = \epsilon_1 C_{\beta,1} \oplus \epsilon_2 C_{\beta,2} \oplus \epsilon_3 C_{\beta,3}$ be a linear code of length β over R. Then C_β is a cyclic code of length β over R if and only if $C_{\beta,j}$ are cyclic codes of length β over $\mathbb{Z}_p$ for $j = 1, 2, 3$.*

Proof. For any $s = (s_0, s_1, \ldots, s_{\beta-1}) \in C_\beta$, we can write its components as $s_i = \epsilon_1 a_i + \epsilon_2 b_i + \epsilon_3 c_i$, where $a_i, b_i, c_i \in \mathbb{Z}_p, 0 \le i \le \beta - 1$. Let $a = (a_0, a_1, \ldots, a_{\beta-1})$, $b = (b_0, b_1, \ldots, b_{\beta-1})$, $c = (c_0, c_1, \ldots, c_{\beta-1})$. Then $a \in C_{\beta,1}, b \in C_{\beta,2}$ and $c \in C_{\beta,3}$. If $C_{\beta,j}$ is a cyclic code for $j = 1, 2, 3$. This implies that

$$\begin{aligned} \rho(a) &= (a_{\beta-1}, a_0, \ldots, a_{\beta-2}) \in C_{\beta,1}, \\ \rho(b) &= (b_{\beta-1}, b_0, \ldots, b_{\beta-2}) \in C_{\beta,2}, \\ \rho(c) &= (c_{\beta-1}, c_0, \ldots, c_{\beta-2}) \in C_{\beta,3}. \end{aligned} \tag{3}$$

Thus $\epsilon_1\rho(a) + \epsilon_2\rho(b) + \epsilon_3\rho(c) = \rho(s) \in C_\beta$, i.e., C_β is a cyclic code of length β over R.

Conversely, suppose that C_β is a cyclic code of length β over R. Let $s_i = \epsilon_1 a_i + \epsilon_2 b_i + \epsilon_3 c_i$, where $a = (a_0, a_1, \ldots, a_{\beta-1}), b = (b_0, b_1, \ldots, b_{\beta-1})$ and $c = (c_0, c_1, \ldots, c_{\beta-1})$. Then $a \in C_{\beta,1}, b \in C_{\beta,2}$ and $c \in C_{\beta,3}$. Now for $s = (s_0, s_1, \ldots, s_{\beta-1}) \in C_\beta$, we have

$$\rho(s) = (s_{\beta-1}, s_0, \ldots, s_{\beta-2}) \in C_\beta.$$

This gives

$\rho(a) \in C_{\beta,1}, \rho(b) \in C_{\beta,2}, \rho(c) \in C_{\beta,3}$, i.e., $C_{\beta,j}$ is a cyclic code of length β over $\mathbb{Z}_p$ for all $j = 1, 2, 3$.

Theorem 2. *Let $C_\beta = \epsilon_1 C_{\beta,1} \oplus \epsilon_2 C_{\beta,2} \oplus \epsilon_3 C_{\beta,3}$ be a cyclic code of length β over R. Suppose $g_j(x)$ are the monic generator polynomials of cyclic code $C_{\beta,j}$ such that $g_j(x)$ divides $x^\beta - 1$ for all $j = 1, 2, 3$. Then*

(i)

$$C_\beta = \langle \epsilon_1 g_1(x), \epsilon_2 g_2(x), \epsilon_3 g_3(x)\rangle$$

and $|C_\beta| = p^{3\beta-(deg\ (g_1(x))+deg\ (g_2(x))+deg\ (g_3(x)))}$.

(ii) There exists a polynomial $g(x) \in R[x]$ such that $C_\beta = \langle g(x) \rangle$, where $g(x) = \langle \epsilon_1 g_1(x) + \epsilon_2 g_2(x) + \epsilon_3 g_3(x) \rangle$ which is a divisor of $x^\beta - 1$.

Proof. (i) Let $C_\beta = \epsilon_1 C_{\beta,1} \oplus \epsilon_2 C_{\beta,2} \oplus \epsilon_3 C_{\beta,3}$ be a cyclic code of length β over R. Then by Theorem 1, $C_{\beta,j}$ is cyclic code of length β over $\mathbb{Z}_p$ for all $j = 1, 2, 3$. Since $g_j(x)$ is the monic generator polynomial of $C_{\beta,j}$, we have $C_{\beta,j} = \langle g_j(x) \rangle \subseteq \mathbb{Z}_p[x]/\langle x^\beta - 1 \rangle$ for all $j = 1, 2, 3$. Therefore C_β has the following form:

$$C_\beta = \langle \epsilon_1 g_1(x), \epsilon_2 g_2(x), \epsilon_3 g_3(x) \rangle.$$

Also, since $|C_\beta| = |\phi(C_\beta)| = |C_{\beta,1}||C_{\beta,2}|C_{\beta,3}|$, we have

$$|C_\beta| = p^{3\beta - (\deg\ (g_1(x)) + \deg\ (g_2(x)) + \deg\ (g_3(x))}.$$

(ii) The first part gives,

$$C_\beta = \langle \epsilon_1 g_1(x), \epsilon_2 g_2(x), \epsilon_3 g_3(x) \rangle.$$

Let $g(x) = \epsilon_1 g_1(x) + \epsilon_2 g_2(x) + \epsilon_3 g_3(x)$. Then it can easily be seen that $\langle g(x) \rangle \subseteq C_\beta$. Moreover, $\epsilon_1 g_1(x) = \epsilon_1 g(x), \epsilon_2 g_2(x) = \epsilon_2 g(x)$ and $\epsilon_3 g_3(x) = \epsilon_3 g(x)$, which concludes $C_\beta \subseteq \langle g(x) \rangle$ and hence $C_\beta = \langle g(x) \rangle$.
Now for all $j = 1, 2, 3$, suppose $g_j(x)$ is the monic generator polynomials of $C_{\beta,j}$. Thus $g_j(x)$ divides $x^\beta - 1$ such that $x^\beta - 1 = h_j(x) g_j(x)$, which further implies that $\epsilon_j(x^\beta - 1) = \epsilon_j h_j(x) g_j(x)$. So that,
$x^\beta - 1 = (\epsilon_1 + \epsilon_2 + \epsilon_3)x^\beta - (\epsilon_1 + \epsilon_2 + \epsilon_3).$
$= \epsilon_1(x^\beta - 1) + \epsilon_2(x^\beta - 1) + \epsilon_3(x^\beta - 1)$
$= \epsilon_1 h_1(x) g_1(x) + \epsilon_2 h_2(x) g_2(x) + \epsilon_3 h_3(x) g_3(x)$
$= (\epsilon_1 h_1(x) + \epsilon_2 h_2(x) + \epsilon_3 h_3(x))(\epsilon_1 g_1(x) + \epsilon_2 g_2(x) + \epsilon_3 g_3(x))$ (because $\epsilon_i^2 = \epsilon_i, \epsilon_i \epsilon_j = 0$ where $i = 1, 2, 3$ and $i \neq j$).
$= (\epsilon_1 h_1(x) + \epsilon_2 h_2(x) + \epsilon_3 h_3(x)) g(x).$
Therefore, $g(x)$ is a divisor of $x^\beta - 1$.

Corollary 1. *Let $C_\beta = \epsilon_1 C_{\beta,1} \oplus \epsilon_2 C_{\beta,2} \oplus \epsilon_3 C_{\beta,3}$ be a cyclic code of length β over R. Then $C_\beta^\perp = \epsilon_1 C_{\beta,1}^\perp \oplus \epsilon_2 C_{\beta,2}^\perp \oplus \epsilon_3 C_{\beta,3}^\perp$ is also a cyclic code of length β over R, where $C_{\beta,j}^\perp$ is a cyclic code of length β over $\mathbb{Z}_p$ for all $j = 1, 2, 3$.*

Corollary 2. *Let $C_\beta = \epsilon_1 C_{\beta,1} \oplus \epsilon_2 C_{\beta,2} \oplus \epsilon_3 C_{\beta,3}$ be a cyclic code of length β over R. Suppose $g_j(x)$ is the monic generator polynomial of the cyclic code $C_{\beta,j}$, which divides $x^\beta - 1$ for all $j = 1, 2, 3$. Then*

1. *$C_\beta^\perp = \langle \epsilon_1 h_1^*(x), \epsilon_2 h_2^*(x), \epsilon_3 h_3^*(x) \rangle$ and $|C_\beta^\perp| = p^{\sum_{j=1}^{3} (deg\ (g_j(x)))}$.*
2. *$C_\beta^\perp = \langle h^*(x) \rangle$, where $h^*(x) = \langle \epsilon_1 h_1^*(x) + \epsilon_2 h_2^*(x) + \epsilon_3 h_3^*(x) \rangle$,*

where $x^\beta - 1 = h_j(x) g_j(x)$ for some $h_j(x) \in \mathbb{Z}_p[x]$, and $h_j^*(x)$ are the reciprocal polynomials of $h_j(x)$, that is, $h_j^*(x) = x^{\deg(h_j(x))} h_j(x^{-1})$ for $j = 1, 2, 3$.

4 Cyclic codes over $\mathbb{Z}_pR$

In this section, we study some structural properties of cyclic codes over $\mathbb{Z}_pR$. Recall that a linear code of length (α, β) over $\mathbb{Z}_pR$, we mean a submodule of R-module $\mathbb{Z}_p^\alpha \times R^\beta$.

Definition 4. *A linear code C over $\mathbb{Z}_p^\alpha R^\beta$ is called cyclic code if C satisfies the following two conditions.*

(i) C is an $R-$submodule of $\mathbb{Z}_p^\alpha R^\beta$, and
(ii)

$$\left(c_{\alpha-1}, c_0, \dots, c_{\alpha-2} \mid c'_{\beta-1}, c'_0, \dots, c'_{\beta-2}\right) \in C,$$

whenever

$$\left(c_0, c_1, \dots, c_{\alpha-1} \mid c'_0, c'_1, \dots, c'_{\beta-1}\right) \in C.$$

Let $R_{\alpha,\beta} = \frac{\mathbb{Z}_p[x]}{\langle x^\alpha - 1\rangle} \times \frac{R[x]}{\langle x^\beta - 1\rangle}$. In polynomial form, each codeword $a = (c_0, c_1, \dots, c_{\alpha-1} \mid c'_0, c'_1, \dots, c'_{\beta-1})$ of a cyclic code can be represented by a pair of polynomials as:

$$\begin{aligned} a(x) &= \left(c_0 + c_1 x + \cdots + c_{\alpha-1}x^{\alpha-1} \mid c'_0 + c'_1 x + \cdots + c'_{\beta-1}x^{\beta-1}\right) \\ &= (c(x) \mid c'(x)) \in R_{\alpha,\beta}. \end{aligned}$$

Let $f(x) = f_0 + f_1 x + \cdots + f_t x^t \in R\,[x]$ and let $(c(x) \mid c'(x)) \in R_{\alpha,\beta}$. Then the multiplication is defined by the basic rule

$$f(x) \star (c(x) \mid c'(x)) = (\eta(f(x))c(x) \mid f(x)c'(x)),$$

where $\eta(f(x)) = \eta(f_0) + \eta(f_1)x + \cdots + \eta(f_t)x^t$.

Lemma 2. *A code C of length (α, β) over $\mathbb{Z}_pR$ is a cyclic code if and only if C is left $R[x]-$submodule of $R_{\alpha,\beta}$.*

Proof. Since $xa(x)$, in $R_{\alpha,\beta}$, represents the cyclic shift of the codeword $a \in C$ whose polynomial form is $a(x) = (c(x) \mid c'(x))$, the remaining part of the proof is straightforward.

We now extend the result of Theorem 2 to the ring $\mathbb{Z}_pR$ as follows.

Theorem 3. *Let C be a cyclic code of length (α, β) over $\mathbb{Z}_pR$. Then*

$$C = \langle (f(x) \mid 0), (\ell(x) \mid g(x))\rangle,$$

where $f(x), \ell(x) \in \mathbb{Z}_p[x]/\langle x^\alpha - 1\rangle, f(x)$ is a divisor of $x^\alpha - 1$ and $g(x)$ is a divisor of $x^\beta - 1$.

A $\mathbb{Z}_pR-$linear code C of length (α, β) is called a separable code if $C = C'_\alpha \otimes C'_\beta$, while considering C'_α and C'_β as punctured codes of C by deleting the coordinates outside the α and β components, respectively.

Proposition 2. *Let $C = \langle (f(x) \mid 0), (\ell(x) \mid g(x)) \rangle$ be a linear cyclic code of length (α, β) over $\mathbb{Z}_pR$. Then,*

1. *$deg\ (\ell(x)) < deg\ (f(x))$ and $f(x) \mid g_3(x)\ell(x)$.*
2. *$C'_\alpha = \langle gcd(f(x), \ell(x)) \rangle$ and $C'_\beta = \langle g(x) \rangle$.*

Lemma 3. *Let $C = \langle (f(x) \mid 0), (\ell(x) \mid g(x)) \rangle$ be a linear cyclic code of length (α, β) over $\mathbb{Z}_pR$. Then, $f(x) \mid \ell(x)$ if and only if $\ell(x) = 0$.*

The following Lemma is a direct consequence of Lemma 3.

Lemma 4. *Let $C = \langle (f(x) \mid 0), (\ell(x) \mid g(x)) \rangle$ be a linear cyclic code. Then the following assertions are equivalent:*

(i) C is a separable,
(ii) $f(x) \mid \ell(x)$,
(iii) $C = \langle (f(x) \mid 0), (0 \mid g(x)) \rangle$. Thus, for a separable code, we obtain

$$C'_\alpha = \langle gcd(f(x), 0) \rangle = \langle f(x) \rangle = C_\alpha, \text{ and } C'_\beta = \langle g(x) \rangle = C_\beta.$$

Theorem 4. *Let $C = C_\alpha \otimes C_\beta$ be a linear code over $\mathbb{Z}_pR$ of length (α, β), where C_α is linear code over $\mathbb{Z}_p$ of length α and C_β is linear code over R of length β. Then C is a cyclic code if and only if C_α is a cyclic code over $\mathbb{Z}_p$ and C_β is a cyclic code over R.*

Proof. Let $(c_0, c_1, \ldots, c_{\alpha-1}) \in C_\alpha$ and let $(c'_0, c'_1, \ldots, c'_{\beta-1}) \in C_\beta$. If $C = C_\alpha \otimes C_\beta$ is a cyclic code over $\mathbb{Z}_pR$, then

$$\left(c_{\alpha-1}, c_0, \ldots, c_{\alpha-2}, c'_{\beta-1}, c'_0, \ldots, c'_{\beta-2}\right) \in C,$$

which implies that

$$(c_{\alpha-1}, c_0, \ldots, c_{\alpha-2}) \in C_\alpha$$

and

$$(c'_{\beta-1}, c'_0, \ldots, c'_{\beta-2}) \in C_\beta.$$

Hence, C_α is a cyclic code over $\mathbb{Z}_p$ and C_β is a cyclic code over R.

On the other hand, suppose that C_α is a cyclic code over $\mathbb{Z}_p$ and C_β is a cyclic code over R. Note that

$$(c_{\alpha-1}, c_0, \ldots, c_{\alpha-2}) \in C_\alpha$$

and

$$\left(c'_{\beta-1}, c'_0, \ldots, c'_{\beta-2}\right) \in C_\beta.$$

Since $C = C_\alpha \otimes C_\beta$, then

$$\left(c_{\alpha-1}, c_0, \ldots, c_{\alpha-2}, c'_{\beta-1}, c'_0, \ldots, c'_{\beta-2}\right) \in C,$$

so C is a cyclic code over $\mathbb{Z}_pR$.

By Theorems 1 and 4, we have the following corollary.

Corollary 3. *Let $C = C_\alpha \otimes C_\beta$ be a linear code over $\mathbb{Z}_pR$ of length (α, β), where C_α is linear code over $\mathbb{Z}_p$ of length α and C_β is linear code over R of length β. Then C is a cyclic code if and only if C_α is a cyclic code over $\mathbb{Z}_p$ and $C_{\beta,j}$ is a cyclic code over $\mathbb{Z}_p$, where $j = 1, 2, 3$.*

In Theorem 3, we have studied the generator polynomial for a cyclic code over $\mathbb{Z}_pR$ of length (α, β). Now here we study the generator polynomial for a separable cyclic code over $\mathbb{Z}_pR$ of length (α, β) as follows.

Theorem 5. *Let $C = C_\alpha \otimes C_\beta$ be a cyclic code over $\mathbb{Z}_pR$ of length (α, β), where $C_\alpha = \langle f(x) \rangle$ and $C_\beta = \langle g(x) \rangle$. Then $C = \langle f(x) \rangle \otimes \langle g(x) \rangle$.*

5 Conditions for complementary duality

A linear complementary dual (LCD) code is a linear code C whose dual $C^\perp$ satisfies the condition $C \cap C^\perp = \{0\}$. In this section, we obtain some conditions on cyclic codes and negacyclic codes over $\mathbb{Z}_pR$ to be LCD codes.

It is proved in paper [16] that if $gcd(\beta, p) = 1$, then $x^\beta - 1$ factorizes uniquely into distinct monic pairwise co-prime basic irreducible polynomials over $\mathbb{Z}_p$. Let

$$x^\beta - 1 = f_1(x), f_2(x), \dots f_l(x). \tag{4}$$

By setting $g_i = f_i$ for $i = \{1, 2, \dots, m\}$ and $h_j h_j^* = f_{s+j}$ for $j = \{1, 2, \dots, r\}$ in (4), we obtain the following factorization

$$x^\beta - 1 = g_1(x) \dots g_m(x) \left(h_1(x)(h_1^*)(x) \dots h_r(x)(h_r^*)(x) \right). \tag{5}$$

Lemma 5. *Let β be an integer such that $\gcd(\beta, p) = 1$. Then if $g(x)$ is a generator polynomial for a cyclic code of length β over R, C is an LCD code if and only if $gcd(g(x), h^*(x)) = 1$, where h^* is the monic reciprocal polynomial of $h(x) = \frac{x^\beta - 1}{g(x)}$.*

Proof. Let h^* be the generator polynomial of $C^\perp$. Therefore, the polynomial $\tilde{g} = \operatorname{lclm}(g(x), h^*(x))$ is the generator polynomial of the cyclic code $C \cap C^\perp$. Now $C \cap C^\perp = \{0\}$ if and only if $\tilde{g}(x)$ has degree β and $x^\beta - 1$ is divisible by $g(x)$ and $h^*(x)$, $\deg(g(x)) = \beta - k$ and $\deg(h^*(x)) = k$. This implies that $\deg(\tilde{g}(x)) = \beta$ if and only if $gcd(g(x), h^*(x)) = 1$.

Theorem 6. *If $g(x)$ is the generator polynomial of a q-ary cyclic code C of length β, then C is an LCD code if and only if $g(x)$ is self-reciprocal and all the monic irreducible factors of $g(x)$ have the same multiplicity in $g(x)$ and in $x^\beta - 1$.*

Proof. Let $\gcd(\beta, p) = 1$. Now suppose that C is an LCD code by Lemma 5. Then we have that $\gcd(g(x), h^*(x)) = 1$. Since

$$x^\beta - 1 = g(x)h(x) = g^*(x)h^*(x), \tag{6}$$

then we must have that $g(x)$ divides $g^*(x)$. Hence $g(x) = g^*(x)$; which means that $g(x)$ is self-reciprocal. Thus $\gcd(g(x), h^*(x)) = 1$ implies that $\gcd(g^*(x), h^*(x)) = 1$, and hence $\gcd(g(x), h(x)) = 1$. As

$$x^\beta - 1 = g(x)h(x), \tag{7}$$

we have that all the irreducible factors of $g(x)$ must have multiplicity p^s.

Conversely, suppose that $g(x)$ is not self-reciprocal so then $g(x)$ does not divide $g^*(x)$. From (6), $\gcd(g(x), h^*(x)) \neq 1$ and by Lemma 5, we have that C is not an LCD code. Finally, suppose that $g(x)$ is self-reciprocal, so is $h(x) = \frac{x^\beta - 1}{g(x)}$. Now suppose that some monic irreducible factor of $g(x)$ has multiplicity less than p^s. From (7), it follows that $1 \neq \gcd(g(x), h(x)) = \gcd(g(x), h^*(x))$, so then by Lemma 5, C is not an LCD code.

Theorem 7. *Consider* $\gcd(\beta, p) = 1$. *Then the cyclic LCD code C of length β over R is generated by*

$$g(x) = g_1^{a_1}(x) \dots g_m^{a_m}(x) \left(h_1^{b_1}(x) h_1^{*b_1}(x) \dots h_r^{b_r}(x) h_r^{*b_r}(x) \right), \tag{8}$$

where $a_i, b_i \in \{0, p^s\}$ *for all* $1 \leq i \leq m, 1 \leq j \leq r$.

Proof. Let C be an LCD cyclic code with generator polynomial $g(x)$, so then $g(x)$ divide $x^\beta - 1$. Furthermore, suppose that

$$g(x) = g_1^{a_1}(x) \dots g_m^{a_m}(x) \left(h_1^{b_1}(x) h_1^{*c_1}(x) \dots h_r^{b_r}(x) h_r^{*c_r}(x) \right), \tag{9}$$

where for $1 \leq i \leq m, a_i \leq p^s$, for $1 \leq i \leq r, b_i, c_i \leq p^s$. From Theorem 6, C is an LCD code if it satisfies

$$g(x) = g^*(x) = g_1^{*a_1}(x) \dots g_m^{*a_m}(x) \left(h_1^{*b_1}(x) h_1^{c_1}(x) \dots h_r^{*b_r}(x) h_r^{c_r}(x) \right). \tag{10}$$

Since all the factors g_i are self-reciprocal, then the equality (10) is true if and only if $b_i = c_i$ for all $1 \leq i \leq r$.

6 Linear complementary dual cyclic codes over $\mathbb{Z}_pR$

In this section, we briefly discuss the cyclic codes to be LCD codes over $\mathbb{F}_qR$, and give some examples for better understanding of our study.

Proposition 3. *Let C_α be a cyclic code over $\mathbb{Z}_p$. Then C_α is an LCD code if and only if $g(x)$ is a self-reciprocal polynomial, i.e., $g^*(x) = g(x)$.*

Proof. Suppose that C_α is an LCD code. Then by Lemma 3, we have $gcd(g, h^*) = 1$, which further implies that $g(x)$ must divide g^* since

$$x^\alpha - 1 = g(x)h(x) = g^*(x)h^*(x). \tag{11}$$

Conversely, suppose that $g(x)$ is not a self-reciprocal polynomial, i.e., $g(x)$ does not divides $g^*(x)$. It follow from (11) that $gcd(g, h^*) \neq 1$, and hence by Lemma 3, C is not LCD code over $\mathbb{Z}_p$.

Theorem 8. *Let $C_\beta = \langle \epsilon_1 g_1(x), \epsilon_2 g_2(x), \epsilon_3 g_3(x)\rangle$ be a cyclic code over R. Then C_β is a LCD code over R if and only if $g_j(x)$ is a self-reciprocal polynomial over $\mathbb{Z}_p$ for all $j = 1, 2, 3$.*

Proof. Let $g_j(x)$ is the monic generator polynomial of $C_{\beta,j}$ for $j = 1, 2, 3$, respectively. Then by Proposition 3, $C_{\beta,j}$ is an LCD code over $\mathbb{Z}_p$, i.e., $C_{\beta,j} \cap C_{\beta,j}^\perp = \{0\}$. Thus, as $C_\beta = \epsilon_1 C_{\beta,1} \oplus \epsilon_2 C_{\beta,2} \oplus \epsilon_3 C_{\beta,3}$, we have

$$\begin{aligned} C_\beta \cap C_\beta^\perp &= (\epsilon_1 C_{\beta,1} \oplus \epsilon_2 C_{\beta,2} \oplus \epsilon_3 C_{\beta,3}) \\ &\quad \cap \left(\epsilon_1 C_{\beta,1}^\perp \oplus \epsilon_2 C_{\beta,2}^\perp \oplus \epsilon_3 C_{\beta,3}^\perp\right) \\ &= \epsilon_1 (C_{\beta,1} \cap C_{\beta,1}^\perp) \oplus \epsilon_2 (C_{\beta,2} \cap C_{\beta,2}^\perp) \oplus \epsilon_3 (C_{\beta,3} \cap C_{\beta,3}^\perp) \\ &= \{0\}. \text{ Hence } C_\beta \text{ is LCD code over } R. \end{aligned}$$

Conversely, assume that C_β is LCD code over R, i.e., $C_\beta \cap C_\beta^\perp = \{0\}$. Also

$$C_\beta \cap C_\beta^\perp = \epsilon_1 (C_{\beta,1} \cap C_{\beta,1}^\perp) \oplus \epsilon_2 (C_{\beta,2} \cap C_{\beta,2}^\perp) \oplus \epsilon_3 (C_{\beta,3} \cap C_{\beta,3}^\perp).$$

Therefore $C_{\beta,j} \cap C_{\beta,j}^\perp = \{0\}$ only if $C_\beta \cap C_\beta^\perp = \{0\}$. Hence $C_{\beta,j}$ is an LCD code over $\mathbb{Z}_p$ for all $j = 1, 2, 3$.

Proposition 4. *Let C be a cyclic code of length (α, β) over $\mathbb{Z}_p R$. Then $C = C_\alpha \otimes C_{\beta,j}$ is an LCD code of length (α, β) if and only if C_α and $C_{\beta,j}$ are LCD codes of length α and β over $\mathbb{Z}_p$, for $j = 1, 2, 3$.*

Proof. By noting that $C \cap C^\perp = (C_\alpha \otimes C_{\beta,j}) \cap (C_\alpha^\perp \otimes C_{\beta,j}^\perp) = (C_\alpha \cap C_\alpha^\perp) \otimes (C_{\beta,j} \cap C_{\beta,j}^\perp)$, we have $C \cap C^\perp = \{0\}$ if and only if $C_\alpha \cap C_\alpha^\perp = \{0\}$, and $C_{\beta,j} \cap C_{\beta,j}^\perp = \{0\}$. Hence C is an LCD codes if and only if C_α and $C_{\beta,j}$ are LCD codes over $\mathbb{Z}_p$ for all $j = 1, 2, 3$.

7 Conclusion

In this paper, we have given the new structure of cyclic codes over a new mixed alphabet ring $\mathbb{Z}_p R$ where $R = \mathbb{Z}_p + v\mathbb{Z}_p + v^2\mathbb{Z}_p, v^3 = v$. We have also constructed a class of LCD cyclic codes over $\mathbb{Z}_p R$. A necessary and sufficient condition for a cyclic code to be a complementary dual (LCD) code has been obtained.

References

1. P. Delsarte. *An algebraic approach to the association schemes of coding theory.* PhD thesis, Universite Catholique de Louvain, 1973.
2. T. Abualrub, I. Siap, and N. Aydin. $\mathbb{Z}_2\mathbb{Z}_4-$additive cyclic codes. *IEEE Trans. Inf. Theory*, 3:1508–1514, 2014.
3. J. Borges, C. Fernández-Córdoba, and R. Ten-Valls. $\mathbb{Z}_2\mathbb{Z}_4-$additive cyclic codes, generator polynomials and dual codes. *IEEE Trans. Inf. Theory*, 11:6348–6354, 2016.
4. I. Aydogdu and T. Abualrub. The structure of $\mathbb{Z}_2\mathbb{Z}_{2^s}-$additive cyclic codes. *Discrete Math. Algorithms Appl.*, 4:1850048–1850060, 2018.
5. I. Aydogdu and I. Siap. On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}-$additive codes. *Linear Multilinear Algebra*, 10:2089–2102, 2014.

6. I. Aydogdu and T. Abualrub. The structure of $\mathbb{Z}_2\mathbb{Z}_2[u]-$cyclic and constacyclic codes. *IEEE Trans. Inf. Theory*, 63(8):4883–4893, 2017.
7. L. Diao and J. Gao. $\mathbb{Z}_p\mathbb{Z}_p[u]-$additive cyclic codes. *Int. J. Inf. Coding Theory*, 1:1–17, 2018.
8. B. Srinivasulu and B. Maheshanand. $\mathbb{Z}_2(\mathbb{Z}_2 + u\mathbb{Z}_2)-$additive cyclic codes and their duals. *Discrete Math. Algorithms Appl.*, 2:1650027–1650045, 2016.
9. Z. Hebbache, A. Kaya, N. Aydin, and K. Guenda. On some skew codes over $\mathbb{Z}_q + u\mathbb{Z}_q$. *Discrete Mathematics Algorithms and Applications*, 2022.
10. J-L. Massey. Linear codes with complementary duals. *Discrete Math.*, 106-107:337–342, 1992.
11. C. Carlet. *Boolean Functions for Cryptography and Error Correcting Codes*. Cambridge University Press, Cambridge, U.K., 2010.
12. X. Liu and H. Liu. Lcd codes over finite chain rings. *Finite Fields Appl.*, 34:1–19, 2015.
13. C. Li, C. Ding, and S. Li. Lcd cyclic codes over finite fields. *IEEE Trans. Inf. Theory*, 63:4344–4356, 2017.
14. X. Yang and J-L. Massey. The condition for a cyclic code to have a complementary dual. *Discrete Math.*, 126:391–393, 1994.
15. L. Diao, J. Gao, and J. Lu. Some results on $\mathbb{Z}_p\mathbb{Z}_p[v]-$additive cyclic codes. *Adv. Math. Commun.*, 4:555–572, 2020.
16. M. Bhaintwal and S-K. Wasan. On quasi-cyclic codes over $\mathbb{Z}_p$.. *Appl. Algebra Engrg. Comm. Comput.*, 20:459–480, 2009.