Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 9(5): 11076–11091.
DOI: 10.3934/math.2024543
Received: 14 January 2024
Revised: 07 March 2024
Accepted: 11 March 2024
Published: 21 March 2024

Research article

On double cyclic codes over $\mathbb{Z}_2 + u\mathbb{Z}_2$

Ismail Aydogdu[*]

Department of Mathematics, Yildiz Technical University, 34210, Istanbul, Turkey

* **Correspondence:** Email: iaydogdu@yildiz.edu.tr.

Abstract: In this paper, we introduced double cyclic codes over $R^r \times R^s$, where $R = \mathbb{Z}_2 + u\mathbb{Z}_2 = \{0, 1, u, 1 + u\}$ is the ring with four elements and $u^2 = 0$. We first determined the generator polynomials of R-double cyclic codes for odd integers r and s, then gave the generators of duals of free double cyclic codes over $R^r \times R^s$. By defining a linear Gray map, we looked at the binary images of R-double cyclic codes and gave several examples of optimal parameter binary linear codes obtained from R-double cyclic codes. Moreover, we studied self-dual R-double cyclic codes and presented an example of a self-dual R-double cyclic code.

Keywords: double cyclic codes; $\mathbb{Z}_2 + u\mathbb{Z}_2$; self-dual cyclic codes; optimal codes
Mathematics Subject Classification: 94B05, 94B60

1. Introduction

Let S be a commutative ring. A linear code C of length n over S is a sub-module of S^n. Any linear code C over S, with the property that any right cyclic shift of the coordinates of a codeword is also a codeword, is called a cyclic code. A subfamily of linear codes is known as double cyclic codes and was introduced by Borges et al. in 2018 in [9]. A linear code is said to be a double cyclic code if its coordinates can be partitioned into two subsets, the first r coordinates and the last s coordinates, such that any simultaneous cyclic shift of the coordinates of the subsets leaves the code invariant. In [9], Borges et al. conducted a study on the algebraic structure of $\mathbb{Z}_2$-double cyclic codes. The research involved the determination of generator polynomials for both this family of codes and their duals. Additionally, the paper established a connection between $\mathbb{Z}_2$-double cyclic codes and $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, as initially introduced in [8]. Actually, double cyclic codes are generalized quasi-cyclic (GQC) codes with index 2, introduced in [13] by Siap and Kulhan. However, there is a difference between the papers [13] and [9]. Siap and Kulhan studied the structure of GQC codes giving the minimal spanning sets, weight enumerators, and minimum Hamming distance bounds of these codes. In [9], the authors discussed the generators and gave the explicit generator polynomials of $\mathbb{Z}_2$-double cyclic codes. Moreover, in [10], Gao et al. introduced the structure of double cyclic codes over the finite ring $\mathbb{Z}_4$.

Now, consider the ring $R = \mathbb{Z}_2 + u\mathbb{Z}_2 = \{0, 1, u, 1 + u\}$ where $u^2 = 0$. The ring R is an important ring with four elements other than the well-known ring $\mathbb{Z}_4$. There are many studies about the cyclic codes over R, such as [2–4, 6, 7, 12]. It has been shown that studying linear and cyclic codes over R has advantages compared to the ring $\mathbb{Z}_4$. First of all, since the finite field $\mathbb{F}_2$ is a subring of the ring R, the factorization of polynomials over $\mathbb{F}_2$ is still valid over R. Additionally, the binary images of linear codes over R are always linear codes, which is not always the case for $\mathbb{Z}_4$. Moreover, decoding algorithms of cyclic codes over R are easier than that over $\mathbb{Z}_4$.

In this paper, we are interested in studying double cyclic codes over $R^r \times R^s$, where r and s are two odd positive integers. We determine both the generators of R-double cyclic code C and its dual $C^\perp$. We show that $C^\perp$ is also an R-double cyclic code. As an application of our study, we give examples of binary linear codes with good parameters according to the database [11], which are binary images of R-double cyclic codes. We also construct an example of a self-dual R-double cyclic code and, furthermore, we show that the binary images of R-double cyclic codes are either binary QC (quasi-cyclic) or GQC codes.

2. Preliminaries

Let $R = \mathbb{Z}_2 + u\mathbb{Z}_2 = \{0, 1, u, 1 + u\}$, with $u^2 = 0$. A nonempty subset C of R^n is called a linear code over R if C is an R-sub-module of R^n. It is well known that a linear code C over R is permutation equivalent to a code with generator matrix

$$G = \begin{bmatrix} I_{k_1} & A & B_1 + uB_2 \\ 0 & uI_{k_2} & uD \end{bmatrix},$$

where A, B_1, B_2, and D are matrices over $\mathbb{Z}_2$.

We can map linear codes over R to linear codes over $\mathbb{Z}_2$ by using the following Gray map.

Let $a = (x_0 + uy_0, \ldots, x_{n-1} + u_{n-1}y_{n-1}) \in R^n$. Define the Gray mapping

$$\begin{gathered} \phi : R^n \to \mathbb{Z}_2^{2n} \\ \phi(a) = (y_0, \ldots y_{n-1}, x_0 \oplus y_0, \ldots, x_{n-1} \oplus y_{n-1}) \end{gathered} \tag{2.1}$$

where $x_i \oplus y_i = x_i + y_i \bmod 2$, $0 \leq i \leq n - 1$. The map ϕ is an isometry, which transforms the Lee distance in R^n to the Hamming distance in $\mathbb{Z}_2^{2n}$. The Hamming weight of any codeword is defined as the number of its nonzero entries. The Hamming distance between two codewords is the Hamming weight of their difference.

Furthermore, the Gray image $\phi(C)$ of C is a binary linear code as well. This property is not valid for the codes over $\mathbb{Z}_4$ in general. We naturally define the Lee weight of a codeword $v = (v_0, \ldots, v_{n-1}) \in R^n$ as

$$wt(v) = \sum_{i=0}^{n-1} wt_L(v_i)$$

where $wt_L(v_i)$ is the Lee weight of the coordinate of $v_i \in R$, and the Lee weight of a coordinate $v_i \in R$ is defined by $wt_L(v_i) = 2$ if $v_i = u$, $wt_L(v_i) = 1$ if $v_i \in \{1, 1 + u\}$ and zero otherwise. We can also extend the above map to $R^r \times R^s$ for $a = (x_0 + uy_0, \ldots, x_{r-1} + uy_{r-1}) \in R^r,\ b = (p_0 + uq_0, \ldots, p_{s-1} + uq_{s-1}) \in R^s$ as follows:

$$\begin{aligned}&\Phi : R^r \times R^s \rightarrow \mathbb{Z}_2^{2n}\\ &(a, b) \rightarrow (y_0, \ldots y_{r-1}, x_0 \oplus y_0, \ldots, x_{r-1} \oplus y_{r-1}, q_0, \ldots, q_{s-1}, p_0 \oplus q_0, \ldots, p_{s-1} \oplus q_{s-1})\end{aligned}$$

where $x_i \oplus y_i = x_i + y_i \mod 2,\ 0 \leq i \leq r-1,\ p_j \oplus q_j = p_j + q_j \mod 2,\ 0 \leq j \leq s-1$, and $n = r + s$.

Now, consider the polynomial ring $R[x]/(x^n - 1)$. A cyclic code of length n over R is an ideal in the ring $R[x]/(x^n - 1)$. Next, we introduce the definition of double cyclic codes over R, which is a natural extension of the classical definition of cyclic codes.

Definition 2.1. *Let C be a linear code over R of length $n = r + s$. The code C will be called an R-double cyclic if*

$$c = (u_0, u_1, \ldots, u_{r-2}, u_{r-1} | v_0, v_1, \ldots, v_{s-2}, v_{s-1}) \in C$$

implies

$$T(c) = (u_{r-1}, u_0, u_1, \ldots, u_{r-2} | v_{s-1}, v_0, v_1, \ldots, v_{s-2}) \in C.$$

For any codeword $c = (u_0, u_1, \ldots, u_{r-2}, u_{r-1} | v_0, v_1, \ldots, v_{s-2}, v_{s-1}) \in R^n$ and any $i \in \mathbb{Z}$, we define the ith shift of the codeword c to be

$$T^i(c) = \left(u_{(0-i) mod\ r}, u_{(1-i) mod\ r}, \ldots, u_{(r-1-i) mod\ r} | v_{(0-i) mod\ s}, \ldots, v_{(s-1-i) mod\ s}\right).$$

In this paper, we always take r and s as odd positive integers. Let us denote the set $R[x]/(x^r - 1) \times R[x]/(x^s - 1)$ by $\mathcal{R}_{r,s}$. If $C \subseteq R^r \times R^s$, then any element

$$c = (u_0, u_1, \ldots, u_{r-1} | v_0, v_1, \ldots, v_{s-1}) \in C$$

can be identified with an element of $\mathcal{R}_{r,s}$ as follows:

$$c(x) = (u_0 + u_1 x + \cdots + u_{r-1} x^{r-1} | v_0 + v_1 x + \cdots + v_{s-1} x^{s-1}) = (u(x), v(x)).$$

This is a one-to-one correspondence between $R^r \times R^s$ and $\mathcal{R}_{r,s}$. Moreover, for any $h(x) \in R[x]$ and any $(f(x), g(x)) \in \mathcal{R}_{r,s}$, define the multiplication

$$h(x) * (f(x), g(x)) = (h(x) f(x), h(x) g(x)).$$

This multiplication is well-defined and the ring $\mathcal{R}_{r,s}$ is an $R[x]$-module. Furthermore, any R-double cyclic code C is an $R[x]$-sub-module of $\mathcal{R}_{r,s}$.

The inner product between two elements

$$v = (a_0, \ldots, a_{r-1}, b_0, \ldots, b_{s-1}), w = (d_0, \ldots, d_{r-1}, e_0, \ldots, e_{s-1}) \in R^r \times R^s,$$

is defined by

$$\langle v, w \rangle = \left(\sum_{i=0}^{r-1} a_i d_i + \sum_{j=0}^{s-1} b_j e_j \right) \in \mathbb{Z}_2 + u\mathbb{Z}_2.$$

By using this inner product, we can define the dual code of an R-double cyclic code C.

Definition 2.2. *Let C be an R-double cyclic code. The dual of C is defined in the usual way as follows:*

$$C^{\perp} = \{w \in R^{r} \times R^{s} | \ \langle v, w \rangle = 0 \ \forall v \in C\} .$$

Using this definition of the dual, we have the following Lemma 2.1. We skip the details for the proof of Lemma 2.1 since we obtain these results with a similar approach to that in [5].

Lemma 2.1. *If C is an R-double cyclic code, then $C^{\perp}$ is also an R-double cyclic code.*

In the sequel, we determine the generator polynomials of an R-double cyclic code C.

Theorem 2.1. *Let C be an R-double cyclic of length $n = r + s$, then*

$$C = \langle (g_1(x) + ua_1(x), 0) , (\ell(x), g_2(x) + ua_2(x)) \rangle ,$$

where $a_1(x)|g_1(x)| (x^{r} - 1) , a_2(x)|g_2(x)| (x^{s} - 1)$ over R and $\ell(x)$ is a polynomial over R.

Proof. Let C be an R-double cyclic code. Since both C and $R[x]/(x^{s} - 1)$ are $R[x]$-modules, we can define the following map:

$$\chi : C \to R[x]/(x^{s} - 1)$$
$$\chi\, (f_1(x), f_2(x)) = f_2(x).$$

It is clear that χ is an R-module homomorphism whose image is an $R[x]$-sub-module (indeed an ideal) of $R[x]/(x^{s} - 1)$ and $\ker(\chi)$ is a sub-module of C. Furthermore, we can easily show that Image(χ) is an ideal in $R[x]/(x^{s} - 1)$. The reader can find more detailed information about the structure of cyclic codes over $R[x]/(x^{s} - 1)$ in [2]. Since s is an odd integer and Image(χ) is an ideal in $R[x]/(x^{s} - 1)$, from [2] we have

$$\chi(C) = \langle g_2(x) + ua_2(x) \rangle$$

where $g_2(x)$ and $a_2(x)$ are polynomials in $R[x]$ satisfying $a_2(x)|g_2(x)|x^{s} - 1$. We also note that

$$\ker(\chi) = \{(f(x), 0) \in C \mid f(x) \in R[x]/(x^{r} - 1)\}.$$

Now, let us define the set

$$\mathcal{A} = \{f(x) \in R[x]/(x^{r} - 1) \mid (f(x), 0) \in \ker(\chi)\}.$$

It is clear that $\mathcal{A}$ is an ideal in $R[x]/(x^{r} - 1)$. So, we can write $\mathcal{A} = \langle g_1(x) + ua_1(x) \rangle$ with $g_1(x), a_1(x) \in R[x]/(x^{r} - 1)$ and $a_1(x)|g_1(x)|x^{r} - 1$. It follows from here that for any element $(j(x), 0) \in \ker(\chi)$, we have $j(x) \in \mathcal{A}$, then $j(x) = m_1(x)\, (g_1(x) + ua_1(x))$ for the polynomial $m_1(x) \in R[x]$. Hence,

$$(f(x), 0) = m_1(x) * (g_1(x) + ua_1(x))$$

which implies that $\ker(\chi)$ is a sub-module of C generated by the element of the form $(g_1(x) + ua_1(x))$. By the first isomorphism theorem, we have

$$C/ \ker(\chi) \cong (g_2(x) + ua_2(x)) .$$

Finally, we need to prove the uniqueness of the generators. Note that since $(g_1(x) + ua_1(x))$ and $(g_2(x) + ua_2(x))$ are cyclic codes over R, this proves the uniqueness of the polynomials $g_1(x)$, $a_1(x)$, and $g_2(x)$, $a_2(x)$. Now, suppose that

$$\begin{aligned} C &= \langle (g_1(x) + ua_1(x), 0), (\ell_1(x), g_2(x) + ua_2(x)) \rangle \\ &= \langle (g_1(x) + ua_1(x), 0), (\ell_2(x), g_2(x) + ua_2(x)) \rangle. \end{aligned}$$

Therefore, $(\ell_1(x) - \ell_2(x), 0) \in \ker(\chi) = \langle g_1(x) + ua_1(x), 0 \rangle$. This implies that

$$\ell_1(x) - \ell_2(x) = (g_1(x) + ua_1(x))\mu(x)$$

for some polynomial $\mu(x) \in R[x]$. Since $\deg(\ell_1(x) - \ell_2(x)) \leq \deg \ell_1(x) < \deg(g_1(x) + ua_1(x))$, then $\mu(x) = 0$, and we have $\ell_1(x) = \ell_2(x)$. This completes the proof. □

Lemma 2.2. *If* $C = \langle (g_1(x) + ua_1(x), 0), (\ell(x), g_2(x) + ua_2(x)) \rangle$ *is an* R*-double cyclic code, then we may assume that* $\deg \ell(x) < \deg(g_1(x) + ua_1(x))$.

Proof. See Lemma 9 in [1]. □

Lemma 2.3. *If* $C = \langle (g_1(x) + ua_1(x), 0), (\ell(x), g_2(x) + ua_2(x)) \rangle$ *is an* R*-double cyclic code, then* $(g_1(x) + ua_1(x)) | \left(\frac{x^s - 1}{a_2(x)} \right) \ell(x)$.

Proof. Consider

$$\chi \left(\frac{x^s - 1}{a_2(x)} * (\ell(x), g_2(x) + ua_2(x)) \right) = \chi \left(\frac{x^s - 1}{a_2(x)} \ell(x), 0 \right) = 0.$$

It means that $\left(\frac{x^s - 1}{a_2(x)} \ell(x), 0 \right) \in \ker(\chi)$, and we have $(g_1(x) + ua_1(x)) | \left(\frac{x^s - 1}{a_2(x)} \right) \ell(x)$. □

Remark 1. *From the above discussion, if* $(\ell(x), g_2(x) + ua_2(x)) \in C$ *for any* R*-double cyclic code, then* $\left(\frac{x^s - 1}{a_2(x)} \ell(x), 0 \right) \in C$. *This implies that if* R*-double cyclic code* C *is generated by* $(\ell(x), g_2(x) + ua_2(x))$, *then we must have* $(x^r - 1) \Big| \frac{x^s - 1}{a_2(x)} \ell(x)$.

We summarize all the discussions about the generators of R-double cyclic codes with the following theorem.

Theorem 2.2. *Let* C *be a double cyclic code in* $\mathcal{R}_{r,s}$, *then* C *can be identified as*

(1) $C = \langle (g_1(x) + ua_1(x), 0) \rangle$, *where* $a_1(x) | g_1(x) | (x^r - 1)$, *or*

(2) $C = \langle (\ell(x), g_2(x) + ua_2(x)) \rangle$, *where* $(x^r - 1) \Big| \frac{x^s - 1}{a_2(x)} \ell(x)$ *and* $a_2(x) | g_2(x) | (x^s - 1)$, *or*

(3) $C = \langle (g_1(x) + ua_1(x), 0), (\ell(x), g_2(x) + ua_2(x)) \rangle$, *where* $a_1(x) | g_1(x) | (x^r - 1)$, $a_2(x) | g_2(x) | (x^s - 1)$, $(g_1(x) + ua_1(x)) | \left(\frac{x^s - 1}{a_2(x)} \right) \ell(x)$, *and* $\deg \ell(x) < \deg(g_1(x) + ua_1(x))$.

Definition 2.3. *Let* M *be an* R*-module. A linearly independent subset* N *of* M *that spans* M *is called a basis of* M. *If an* R*-module has a basis, then it is called a free* R*-module.*

It is important to note that if C is a double cyclic code of the form $C = \langle (g_1(x) + ua_1(x), 0), (\ell(x), g_2(x) + ua_2(x))\rangle$ with $(g_1(x) + ua_1(x))|(x^r - 1)$ and $(g_2(x) + ua_2(x))|(x^s - 1)$, then C is a free R-module [2]. If C is not of this form, then it is not a free R-module. Still, one can present a minimal spanning set for the code. In the following theorem, we present a spanning minimal set for double cyclic codes viewed as R-sub-modules.

Theorem 2.3. *Let $C = \langle (g_1(x) + ua_1(x), 0), (\ell(x), g_2(x) + ua_2(x))\rangle$ be an R-double cyclic code in $\mathcal{R}_{r,s}$ with all generator polynomials $g_1(x)$, $a_1(x)$, $g_2(x)$, $a_2(x)$, and $\ell(x)$ as in Theorem 2.1 and $g_1(x)h_1(x) = x^r - 1$, $g_2(x)h_2(x) = x^s - 1$. Furthermore, let* $\deg(g_1(x)) = t_1$, $\deg(a_1(x)) = t_2$, $\deg(g_2(x)) = k_1$, *and* $\deg(a_2(x)) = k_2$. *Consider the following sets:*

$$S_1 = \bigcup_{i=0}^{r-t_1-1} \left\{x^i * (g_1(x) + ua_1(x), 0)\right\}$$

$$S_2 = \bigcup_{i=0}^{t_1-t_2-1} \left\{x^i * (uh_1(x)a_1(x), 0)\right\}$$

$$S_3 = \bigcup_{i=0}^{s-k_1-1} \left\{x^i * (\ell(x), g_2(x) + ua_2(x))\right\}$$

$$S_4 = \bigcup_{i=0}^{k_1-k_2-1} \left\{x^i * (h_2(x)\ell(x), uh_2(x)a_2(x))\right\},$$

then

$$S = S_1 \cup S_2 \cup S_3 \cup S_4$$

forms a minimal spanning set for C as an R-module. Moreover, C has $4^{r+s-t_1-k_1}2^{t_1+k_1-t_2-k_2}$ codewords.

Proof. Let

$$c(x) = m(x) * (g_1(x) + ua_1(x), 0) + n(x) * (\ell(x), g_2(x) + ua_2(x)) \in \mathcal{R}_{r,s}$$

correspond to a codeword in C, where $m(x)$ and $n(x)$ are polynomials in $R[x]$. If $\deg(m(x)) \le r - t_1 - 1$, then $m(x) * (g_1(x) + ua_1(x), 0) \in \text{Span}(S_1)$. Otherwise, by using the division algorithm, we have $m(x) = h_1(x)q_1(x) + r_1(x)$, where $q_1(x), r_1(x) \in R[x]$ and $0 \le \deg((r_1(x))) < r - t_1 - 1$. It follows from here that

$$\begin{aligned} m(x) * (g_1(x) + ua_1(x), 0) &= (h_1(x)q_1(x) + r_1(x)) * (g_1(x) + ua_1(x), 0) \\ &= q_1(x) * (uh_1(x)a_1(x), 0) + r_1(x) * (g_1(x) + ua_1(x), 0). \end{aligned}$$

If $\deg(q_1(x)) \le t_1 - t_2 - 1$, then we get that $q_1(x) * (uh_1(x)a_1(x), 0) \in \text{Span}(S_2)$. Otherwise, by using the division algorithm again, we have

$$q_1(x) = \frac{x^r - 1}{h_1(x)a_1(x)} q_2(x) + r_2(x)$$

where $q_2(x)$ and $r_2(x)$ are polynomials in $R[x]$ with $0 \le \deg(r_2(x)) \le t_1 - t_2 - 1$. Therefore,

$$q_1(x) * (uh_1(x)a_1(x), 0) = \left(\frac{x^r - 1}{h_1(x)a_1(x)} q_2(x) + r_2(x)\right) * (uh_1(x)a_1(x), 0)$$

$$= \; r_2(x) * (uh_1(x)a_1(x), 0) \in \mathrm{Span}(S_2).$$

So, we have shown that $m(x) * (g_1(x) + ua_1(x), 0) \in \mathrm{Span}(S_1 \cup S_2)$.

Now, if $\deg(n(x)) \leq s - k_1 - 1$, then $n(x) * (\ell(x), g_2(x) + ua_2(x) \in \mathrm{Span}(S_3)$. Otherwise, by the division algorithm,

$$n(x) = q_3(x)h_2(x) + r_3(x) \text{ with } 0 \leq \deg(r_3(x)) \leq s - k_1 - 1.$$

Hence,

$$\begin{aligned} n(x) * (\ell(x), g_2(x) + ua_2(x) &= (q_3(x)h_2(x) + r_3(x)) * (\ell(x), g_2(x) + ua_2(x)) \\ &= q_3(x) * (h_2(x)\ell(x), uh_2(x)a_2(x)) + r_3(x) * (\ell(x), g_2(x) + ua_2(x)). \end{aligned}$$

Since $0 \leq \deg(r_3(x)) \leq s - k_1 - 1$, then $r_3(x) * (\ell(x), g_2(x) + ua_2(x)) \in \mathrm{Span}(S_3)$. So, the only remaining part is to prove that

$$q_3(x) * (h_2(x)\ell(x), uh_2(x)a_2(x)) \in \mathrm{Span}(S).$$

We know that $(g_1(x) + ua_1(x)) | \left(\frac{x^s - 1}{a_2(x)}\right)\ell(x)$. Therefore, we can find a polynomial $\lambda(x) \in R[x]$ such that $\frac{x^s - 1}{a_2(x)}\ell(x) = \lambda(x)(g_1(x) + ua_1(x))$. Again, if $\deg(q_3(x)) \leq k_1 - k_2 - 1$, then $q_3(x) * (h_2(x)\ell(x), uh_2(x)a_2(x)) \in \mathrm{Span}(S_4)$. Otherwise, we have

$$q_3(x) = \frac{x^s - 1}{h_2(x)a_2(x)} q_4(x) + r_4(x)$$

for the polynomials $q_4(x), r_4(x) \in R[x]$ with $0 \leq deg(r_4(x)) \leq k_1 - k_2 - 1$. Therefore,

$$q_3(x) * (h_2(x)\ell(x), uh_2(x)a_2(x)) = q_4(x) * \left(\frac{x^s - 1}{a_2(x)}\ell(x), 0\right) + r_4(x) * (h_2(x)\ell(x), uh_2(x)a_2(x)).$$

Since $\frac{x^s - 1}{a_2(x)}\ell(x) = \lambda(x)(g_1(x) + ua_1(x))$, then $q_4(x) * \left(\frac{x^s - 1}{a_2(x)}\ell(x), 0\right) \in \mathrm{Span}(S_1 \cup S_2)$. Also, it is clear that $r_4(x) * (h_2(x)\ell(x), uh_2(x)a_2(x)) \in \mathrm{Span}(S_4)$. Therefore, $S = S_1 \cup S_2 \cup S_3 \cup S_4$ is a spanning set for C. Finally, it is clear that the set S is a minimal generating set in the sense that there is no element in S linearly dependent with the other elements. So, C has $4^{r+s-t_1-k_1}2^{t_1+k_1-t_2-k_2}$ codewords. □

Example 2.1. *Consider the double cyclic code C in $R[x]/(x^{15} - 1) \times R[x]/(x^7 - 1)$ generated by $((g_1(x) + ua_1(x), 0), (\ell(x), g_2(x) + ua_2(x)))$, where*

$$\begin{aligned} g_1(x) = a_1(x) &= (1 + x)(1 + x + x^4)(1 + x^3 + x^4) = 1 + x^2 + x^3 + x^6 + x^7 + x^9, \\ g_2(x) &= (1 + x)(1 + x + x^3) = 1 + x^2 + x^3 + x^4, \\ a_2(x) &= 1 + x + x^3, \\ \ell(x) &= (1 + u)(1 + x + x^4)(1 + x^3 + x^4) = (1 + u)(1 + x + x^3 + x^4 + x^5 + x^7 + x^8). \end{aligned}$$

We note that the polynomials above are obtained from the factorizations of $(x^{15} - 1)$ and $(x^7 - 1)$ in $R[x]$. One can make use of the factorization in $\mathbb{Z}_2[x]$ since this also holds over R. Moreover, we can calculate the following polynomials:

$$g_1(x)h_1(x) = x^{15} - 1 \Rightarrow h_1(x) = 1 + x^2 + x^3 + x^4 + x^6,$$

$$g_2(x)h_2(x) \;=\; x^7 - 1 \Rightarrow h_2(x) = 1 + x^2 + x^3.$$

Hence, using the spanning sets in Theorem 2.3, we have the generator matrix for C as

$$G = \begin{bmatrix}
u{+}1 & 0 & u{+}1 & u{+}1 & 0 & 0 & u{+}1 & u{+}1 & 0 & u{+}1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & u{+}1 & 0 & u{+}1 & u{+}1 & 0 & 0 & u{+}1 & u{+}1 & 0 & u{+}1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & u{+}1 & 0 & u{+}1 & u{+}1 & 0 & 0 & u{+}1 & u{+}1 & 0 & u{+}1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & u{+}1 & 0 & u{+}1 & u{+}1 & 0 & 0 & u{+}1 & u{+}1 & 0 & u{+}1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & u{+}1 & 0 & u{+}1 & u{+}1 & 0 & 0 & u{+}1 & u{+}1 & 0 & u{+}1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & u{+}1 & 0 & u{+}1 & u{+}1 & 0 & 0 & u{+}1 & u{+}1 & 0 & u{+}1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
u{+}1 & u{+}1 & 0 & u{+}1 & u{+}1 & u{+}1 & 0 & u{+}1 & u{+}1 & 0 & 0 & 0 & 0 & 0 & 0 & u{+}1 & u & 1 & u{+}1 & 1 & 0 & 0 \\
0 & u{+}1 & u{+}1 & 0 & u{+}1 & u{+}1 & u{+}1 & 0 & u{+}1 & u{+}1 & 0 & 0 & 0 & 0 & 0 & 0 & u{+}1 & u & 1 & u{+}1 & 1 & 0 \\
0 & 0 & u{+}1 & u{+}1 & 0 & u{+}1 & u{+}1 & u{+}1 & 0 & u{+}1 & u{+}1 & 0 & 0 & 0 & 0 & 0 & 0 & u{+}1 & u & 1 & u{+}1 & 1 \\
u{+}1 & u{+}1 & u{+}1 & u{+}1 & 0 & 0 & 0 & u{+}1 & 0 & u{+}1 & 0 & u{+}1 & 0 & 0 & 0 & u & u & u & u & u & u & u
\end{bmatrix}.$$

Furthermore, the Gray image $\Phi(C)$ of C is a binary linear code with parameters $[44, 19, 6]$.

3. The structure of the dual double-cyclic codes

In this section, we study the structure of the dual of free R-double cyclic codes with using the similar approach given in [5,10]. Let $f(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$ be any element in the ring $R[x]/\left(x^n - 1\right)$. Note that in this description, a_i might equal 0 for any $i = 0, 1, \ldots, n-1$. From now on, the polynomial $f^*(x)$ will denote $f^*(x) = x^{n-1}f(1/x) = a_{n-1} + a_{n-2}x + \ldots a_0x^{n-1}$, i.e., if $a_{n-1} \neq 0$, then $f^*(x)$ is the reciprocal of $f(x)$. By definition, we note that $f^{**}(x) = f(x)$.

Let $(a_0, a_1, \ldots, a_{r-1}, b_0, b_1 \ldots, b_{s-1}) \in R^r \times R^s$ and the cyclic shift of this codeword be $T(a, b) = (a_{r-1}, a_0, \ldots, a_{r-2}, b_{s-1}, b_0, \ldots, b_{s-2})$. It is clear that the set $\{(a, b), T(a, b), T^2(a, b), \ldots, T^{m-1}(a, b)\}$ produces all the cyclic shifts of (a, b), where $m = lcm(r, s)$.

We will give the relation between the inner product and the polynomial product, which relies on the cyclic shifts in $R^r \times R^s$. This approach was originally introduced in [5]. Let $V = (a_0, a_1, \ldots, a_{r-1}, b_0, b_1, \ldots, b_{s-1})$, $W = (d_0, d_1, \ldots, d_{r-1}, e_0, e_1, \ldots, e_{s-1}) \in R^r \times R^s$, and, without loss of generality, suppose $r \leq s$, then

$$\begin{aligned}
\langle V, T(W)\rangle &= \underbrace{a_0d_{r-1} + a_1d_0 + \ldots + a_{r-1}d_{r-2}}_{\omega_0} + \underbrace{b_0e_{s-1} + b_1e_0 + \ldots + b_{s-1}e_{s-2}}_{\sigma_0} \\
&= \omega_0 + \sigma_0.
\end{aligned}$$

In general,

$$\begin{aligned}
\langle V, T^i(W)\rangle &= a_0d_{r-i} + a_1d_{r-i+1} + \ldots + a_{r-1}d_{r-i-1} + b_0e_{s-i} + \ldots + b_{s-1}e_{s-i-1} \\
&= \omega_{(i-1) \bmod r} + \sigma_{(i-1) \bmod s},
\end{aligned}$$

for all $i = 1, 2, \ldots, m$ where $m = lcm\,(r, s)$. Now, construct the polynomial

$$\begin{aligned}
Z(x) &= (\omega_0 + \sigma_0) + (\omega_1 + \sigma_1)\,x + \cdots + \left(\omega_{(r-1) \bmod r} + \sigma_{(r-1) \bmod s}\right) x^{r-1} \\
&\quad + \left(\omega_{r \bmod r} + \sigma_{r \bmod s}\right) x^r + \cdots + \left(\omega_{(s-1) \bmod r} + \sigma_{(s-1) \bmod s}\right) x^{r-1} \\
&\quad + \left(\omega_{s \bmod r} + \sigma_{s \bmod s}\right) x^s + \cdots + \left(\omega_{(m-1) \bmod r} + \sigma_{(m-1) \bmod s}\right) x^{m-1}.
\end{aligned}$$

Simplifying $Z(x)$, we have

$$Z(x) = \left(a(x)d^*(x) \bmod (x^r - 1)\left(\frac{x^m - 1}{x^r - 1}\right) + b(x)e^*(x) \bmod (x^s - 1)\left(\frac{x^m - 1}{x^s - 1}\right)\right).$$

So, we can give the following proved theorem.

Theorem 3.1. *Let $V = (a_{0,}a_1, \ldots, a_{r-1}, b_0, b_1, \ldots, b_{s-1})$, $W = (d_0, d_1, \ldots, d_{r-1}, e_0, e_1, \ldots, e_{s-1}) \in R^r \times R^s$, then V is orthogonal to W and all its cyclic shifts if, and only if,*

$$\begin{aligned} Z(x) &= [a(x)d^*(x) \bmod (x^r-1)]\left(\frac{x^m-1}{x^r-1}\right) + [b(x)e^*(x) \bmod (x^s-1)]\left(\frac{x^m-1}{x^s-1}\right) \\ &= 0 \bmod (x^m-1). \end{aligned}$$

This equation can be written as

$$Z(x) = [a(x)d^*(x)]\left(\frac{x^m-1}{x^r-1}\right) + [b(x)e^*(x)]\left(\frac{x^m-1}{x^s-1}\right) = 0 \bmod (x^m-1).$$

Let us consider the free double cyclic code $C = \langle (g_1(x) + ua_1(x), 0), (\ell(x), g_2(x) + ua_2(x)) \rangle$ in $\mathcal{R}_{r,s}$. Since C is free, it is clear that $a_1(x) = a_2(x) = 0$.

Let $d(x) = \gcd(g_1(x), \ell(x))$. Since $g_1(x) | \frac{x^s-1}{g_2(x)}\ell(x)$, we can write $\left(\frac{x^s-1}{g_2(x)}\ell(x)\right) = g_1(x)\beta(x)$. Since $d(x) = \gcd(g_1(x), \ell(x))$, we have $\alpha_1(x)\ell(x) + \alpha_2(x)g_1(x) = d(x)$, $g_1(x) = d(x)d_1(x)$, $\ell(x) = d(x)d_2(x)$, $\frac{x^s-1}{g_2(x)}\ell(x) = g_1(x)\beta(x) = d(x)d_1(x)\beta(x)$.

Now, since C is a free double cyclic code, we have $g_1(x) | (x^r-1)$ and also $g_1(x) = d(x)d_1(x)$, then $x^r - 1 = g_1(x)h_1(x) = d(x)d_1(x)h_1(x)$. Therefore,

$$\begin{aligned} \frac{x^s-1}{g_2(x)}d(x) &= \frac{x^s-1}{g_2(x)}[\alpha_1(x)\ell(x) + \alpha_2(x)g_1(x)] \\ &= \alpha_1(x)g_1(x)\beta(x) + \alpha_2(x)\frac{x^s-1}{g_2(x)}g_1(x) \\ &= g_1(x)\underbrace{\left[\alpha_1(x)\beta(x) + \alpha_2(x)\frac{x^s-1}{g_2(x)}\right]}_{\theta(x)}. \end{aligned}$$

So, we have

$$\begin{aligned} \frac{x^s-1}{g_2(x)}d(x) &= g_1(x)\theta(x) \\ (x^s-1)\,d(x) &= g_2(x)g_1(x)\theta(x) = g_2(x)d(x)d_2(x)\theta(x). \end{aligned}$$

Therefore, $x^s - 1 = g_2(x)d_2(x)\theta(x)$ and $\theta(x)$ is a factor of $x^s - 1$.

Lemma 3.1. *Let $C = \langle (g_1(x), 0), (\ell(x), g_2(x)) \rangle$ be a free double cyclic code in $\mathcal{R}_{r,s}$, then the code C is orthogonal to the code*

$$\mathcal{D} = \left\langle \left(\left(\frac{x^r-1}{d(x)}\right)^*, 0\right), \left(\left(\alpha_1(x)\frac{x^r-1}{g_1(x)}\right)^*, (\theta(x))^*\right) \right\rangle$$

where $d(x), \alpha_1(x)$, and $\theta(x)$ are defined above.

Proof. Let $C = \langle (g_1(x), 0), (\ell(x), g_2(x)) \rangle$ be a free R-double cyclic code and $g_1(x)h_1(x) = x^r - 1$, then by using polynomial multiplication $Z(x)$ defined before, we have

$$(g_1(x), 0) \cdot \left(\frac{x^r-1}{d(x)}, 0\right)^* = \left(g_1(x)\frac{x^r-1}{d(x)} \bmod (x^r-1)\right)\frac{x^m-1}{x^r-1}$$

$$\begin{aligned}
&= \left(d(x)d_1(x)\frac{x^r-1}{d(x)} \bmod (x^r-1)\right)\frac{x^m-1}{x^r-1}\\
&= 0 \bmod (x^m-1)
\end{aligned}$$

$$\begin{aligned}
(\ell(x), g_2(x)) \cdot \left(\frac{x^r-1}{d(x)}, 0\right)^* &= \left(\ell(x)\frac{x^r-1}{d(x)} \bmod (x^r-1)\right)\frac{x^m-1}{x^r-1}\\
&= \left(d(x)d_2(x)\frac{x^r-1}{d(x)} \bmod (x^r-1)\right)\frac{x^m-1}{x^r-1}\\
&= 0 \bmod (x^m-1)
\end{aligned}$$

$$\begin{aligned}
(g_1(x), 0) \cdot \left(\alpha_1(x)\frac{x^r-1}{g_1(x)}, \theta(x)\right)^* &= g_1(x)\left(\alpha_1(x)\frac{x^r-1}{g_1(x)} \bmod (x^r-1)\right)\frac{x^m-1}{x^r-1}\\
&= 0 \bmod (x^m-1)\,.
\end{aligned}$$

Now, we will find the product of the last generator polynomials.

$$\begin{aligned}
(\ell(x), g_2(x)) \cdot \left(\alpha_1(x)\frac{x^r-1}{g_1(x)}, \theta(x)\right)^* &= \left(\ell(x)\alpha_1(x)\frac{x^r-1}{g_1(x)} \bmod (x^r-1)\right)\left(\frac{x^m-1}{x^r-1}\right)\\
&\quad + (g_2(x)\theta(x) \bmod (x^s-1))\left(\frac{x^m-1}{x^s-1}\right)\\
&= \underbrace{(d(x)+\alpha_2(x)g_1(x))}_{\alpha_1(x)\ell(x)}\frac{x^r-1}{g_1(x)}\left(\frac{x^m-1}{x^r-1}\right)\\
&\quad + g_2(x)\left(\frac{x^s-1}{d_2(x)g_2(x)}\right)\left(\frac{x^m-1}{x^s-1}\right)\\
&= d(x)\frac{x^r-1}{g_1(x)}\left(\frac{x^m-1}{x^r-1}\right) + \frac{x^s-1}{d_2(x)}\left(\frac{x^m-1}{x^s-1}\right)\\
&= d(x)\frac{x^r-1}{g_1(x)}\left(\frac{x^m-1}{x^r-1}\right) + \frac{x^s-1}{d_2(x)}\frac{d(x)h_1(x)}{d(x)h_1(x)}\left(\frac{x^m-1}{x^s-1}\right)\\
&= d(x)\frac{x^r-1}{g_1(x)}\left(\frac{x^m-1}{x^r-1}\right) + \frac{x^s-1}{x^r-1}d(x)h_1(x)\left(\frac{x^m-1}{x^s-1}\right)\\
&= d(x)\frac{x^r-1}{g_1(x)}\left(\frac{x^m-1}{x^r-1}\right) + d(x)\frac{x^r-1}{g_1(x)}\left(\frac{x^m-1}{x^r-1}\right)\\
&= 0 \bmod (x^m-1)\,.
\end{aligned}$$

Hence, we have

$$(\ell(x), g_2(x)) \cdot \left(\alpha_1(x)\frac{x^r-1}{g_1(x)}, \theta(x)\right)^* = 0 \bmod (x^m-1)\,.$$

Consequently, the code C is orthogonal to the code $\mathcal{D}$. □

Lemma 3.2. *Let* $C = \langle (g_1(x), 0), (\ell(x), g_2(x))\rangle$ *be a free double cyclic code in* $\mathcal{R}_{r,s}$. *Let* $\mathcal{D} = \left\langle \left(\left(\frac{x^r-1}{d(x)}\right), 0\right), (M(x), \theta(x))\right\rangle$ *with the generators as above, where* $M(x) = \alpha_1(x)\frac{x^r-1}{g_1(x)}$, *then*

(1) $\left(\dfrac{x^r-1}{d(x)}\right)$ *is a factor of* (x^r-1), $\theta(x)$ *is a factor of* (x^s-1).

(2) $\left(\dfrac{x^r-1}{d(x)}\right) \mid \left(\left(\dfrac{x^s-1}{\theta(x)}\right)M(x)\right)$.

Proof. See the proof of Lemma 5 in [5]. □

Lemma 3.3. *Let* $C = \langle (g_1(x), 0), (\ell(x), g_2(x)) \rangle$ *be a free double cyclic code in* $\mathcal{R}_{r,s}$. *Let* $\mathcal{D} = \left\langle \left(\left(\dfrac{x^r-1}{d(x)}\right), 0\right), (M(x), \theta(x)) \right\rangle$, *then* $\mathcal{D}$ *has* $4^{\deg d}4^{(s-\deg\theta)}$ *codewords.*

Proof. Since the generators of $\mathcal{D}$ have the same properties as the generators of C in Theorem 2.3, the result follows from Theorem 2.3. □

Lemma 3.4. *Let* $C = \langle (g_1(x), 0), (\ell(x), g_2(x)) \rangle$ *be a free double cyclic code in* $\mathcal{R}_{r,s}$. *Let* $\mathcal{D} = \left\langle \left(\left(\dfrac{x^r-1}{d(x)}\right), 0\right), (M(x), \theta(x)) \right\rangle$, *then* $|C|\,|\mathcal{D}| = 4^n$.

Proof. We know that $|C| = 4^{r-\deg g_1}4^{s-\deg g_2}$ and $|\mathcal{D}| = 4^{\deg d}4^{(s-\deg\theta)}$. Since $\dfrac{x^s-1}{g_2(x)}d(x) = g_1(x)\theta(x)$, we have

$$\begin{aligned} s-\deg\theta &= s-(s+\deg d-\deg g_2-\deg g_1) \\ &= \deg g_2+\deg g_1-\deg d. \end{aligned}$$

Therefore, $|C|\,|\mathcal{D}| = 4^q$, where

$$\begin{aligned} q &= r-\deg g_1+s-\deg g_2+\deg d+\deg g_2+\deg g_1-\deg d \\ &= r+s=n. \end{aligned}$$

So, $|C|\,|\mathcal{D}| = 4^n$. □

Finally, we will give the following theorem that determines the generators of a dual of a free double cyclic code C.

Theorem 3.2. *If* $C = \langle (g_1(x), 0), (\ell(x), g_2(x)) \rangle$ *is a free double cyclic code in* $\mathcal{R}_{r,s}$, *then*

$$C^{\perp} = \left\langle \left(\left(\frac{x^r-1}{d(x)}\right)^*, 0\right), \left(\left(\alpha_1(x)\frac{x^r-1}{g_1(x)}\right)^*, (\theta(x))^*\right) \right\rangle.$$

Example 3.1. *Let* C *be a double cyclic code in* $R[x]/(x^7-1) \times R[x]/(x^7-1)$ *generated by* $((g_1(x)+ua_1(x), 0), (\ell(x), g_2(x)+ua_2(x)))$, *where*

$$\begin{aligned} g_1(x) &= (1+x+x^3)(1+x^2+x^3) = 1+x+x^2+x^3+x^4+x^5+x^6,\ a_1(x) = x^7-1, \\ g_2(x) &= 1+x+x^3,\ a_2(x) = x^7-1, \\ \ell(x) &= 1+x+x^3. \end{aligned}$$

Furthermore, we can calculate the following polynomials:

$$g_1(x)h_1(x) = x^7-1 \Rightarrow h_1(x) = 1+x,$$

$$g_2(x)h_2(x) \;=\; x^7-1 \Rightarrow h_2(x) = 1+x+x^2+x^4.$$

Hence, using the spanning sets in Theorem 2.3, we have the generator matrix for C as

$$G=\begin{bmatrix} 1&1&1&1&1&1&1&0&0&0&0&0&0&0\\ 1&1&0&1&0&0&0&1&1&0&1&0&0&0\\ 0&1&1&0&1&0&0&0&1&1&0&1&0&0\\ 0&0&1&1&0&1&0&0&0&1&1&0&1&0\\ 0&0&0&1&1&0&1&0&0&0&1&1&0&1 \end{bmatrix}.$$

Furthermore, the Gray image $\Phi(C)$ of C is a binary linear code with parameters $[28,10,6]$.

Now, let us find the generator matrix of the dual cyclic code $C^\perp$ by considering Theorem 3.2 as follows. First, we will determine the generator polynomials of the dual code.

$$\begin{aligned} d(x) &= \gcd(\ell(x), g_1(x)) = 1+x+x^3,\\ h_2(x)\ell(x) &= g_1(x)\beta(x) \Rightarrow \beta(x) = 1+x,\\ \alpha_1(x)\ell(x)+\alpha_2(x)g_1(x) &= d(x) \Rightarrow \alpha_1(x)=1, \alpha_2(x)=0,\\ \theta(x) &= \alpha_1(x)\beta(x)+\alpha_2(x)h_2(x) = 1+x,\\ M(x) &= \alpha_1(x)h_1(x) = 1+x. \end{aligned}$$

Therefore, $C^\perp = \left\langle \left(\left(1+x+x^2+x^4\right)^*, 0\right), \left((1+x)^*, (1+x)^*\right) \right\rangle$ *and the the parity-check matrix of C is*

$$H=\begin{bmatrix} 0&0&1&0&1&1&1&0&0&0&0&0&0&0\\ 1&0&0&1&0&1&1&0&0&0&0&0&0&0\\ 1&1&0&0&1&0&1&0&0&0&0&0&0&0\\ 0&0&0&0&0&1&1&0&0&0&0&0&1&1\\ 1&0&0&0&0&0&1&1&0&0&0&0&0&1\\ 1&1&0&0&0&0&0&1&1&0&0&0&0&0\\ 0&1&1&0&0&0&0&0&1&1&0&0&0&0\\ 0&0&1&1&0&0&0&0&0&1&1&0&0&0\\ 0&0&0&1&1&0&0&0&0&0&1&1&0&0 \end{bmatrix}.$$

Moreover, $\Phi(C^\perp)$ *has the parameters* $[28,18,4]$ *which are very close to the optimal parameters* $[28,18,5]$.

Let $C = \langle (g_1(x), 0), (\ell(x), g_2(x)) \rangle$ be a self-dual free double cyclic code in $\mathcal{R}_{r,s}$, then $C = C^\perp$, so we have the following results.

(1) $\left(\dfrac{x^r-1}{d(x)}\right)^* = g_1(x) \implies x^r - 1 = g_1(x)(d(x))^*.$

(2) $\left(\alpha_1(x)\beta(x)+\alpha_2(x)\dfrac{x^s-1}{g_2(x)}\right)^* = g_2(x)$

$$\begin{aligned} &\implies \alpha_1(x)\beta(x)+\alpha_2(x)\frac{x^s-1}{g_2(x)} = (g_2(x))^*\\ &\implies \alpha_2(x)\frac{x^s-1}{g_2(x)} = \alpha_1(x)\beta(x)+(g_2(x))^*\\ &\implies x^s-1 = \frac{g_2(x)}{\alpha_2(x)}(\alpha_1(x)\beta(x)+(g_2(x))^*). \end{aligned}$$

(3) $((M(x))^*, (\theta(x))^*) = k_1(x)(g_1(x), 0) + k_2(x)(\ell(x), g_2(x))$, then $(M(x))^* = k_1(x)g_1(x) + k_2(x)\ell(x)$. We also know from Theorem 3.2 that $(M(x))^* = \left(\frac{x^r - 1}{g_1(x)}\alpha_1(x)\right)^*$ and also from (1) that we have $x^r - 1 = g_1(x)(d(x))^*$, so

$$x^r - 1 = g_1(x)(d(x))^* \implies \left(\frac{x^r - 1}{g_1(x)}\right)^* = d(x).$$

Therefore, $d(x)(\alpha(x))^* = k_1(x)g_1(x) + k_2(x)\ell(x)$, and we have

$$(\alpha(x))^* = k_1(x)\frac{g_1(x)}{d(x)} + k_2(x)\frac{\ell(x)}{d(x)}.$$

Since $\gcd\left(\frac{g_1(x)}{d(x)}, \frac{\ell(x)}{d(x)}\right) = 1$, we have $(\alpha_1(x))^* = 1$ and $\alpha_1(x) = 1$.

Example 3.2. *Let C be a free R-double cyclic code in $R^7 \times R^7$ with $C = \langle((g_1(x), 0), (\ell(x), g_2(x)))\rangle$, where*

$$g_1(x) = 1 + x^2 + x^3 + x^4,\ \ell(x) = 1 + x + x^3 = g_2(x).$$

Therefore, C has the following generator matrix

$$G = \begin{bmatrix} 1&0&1&1&1&0&0&0&0&0&0&0&0&0\\ 0&1&0&1&1&1&0&0&0&0&0&0&0&0\\ 0&0&1&0&1&1&1&0&0&0&0&0&0&0\\ 1&1&0&1&0&0&0&1&1&0&1&0&0&0\\ 0&1&1&0&1&0&0&0&1&1&0&1&0&0\\ 0&0&1&1&0&1&0&0&0&1&1&0&1&0\\ 0&0&0&1&1&0&1&0&0&0&1&1&0&1 \end{bmatrix}.$$

Furthermore, the dual code is $C^\perp = \langle(\bar{g_1}(x), 0), (\bar{\ell}(x), \bar{g_2}(x))\rangle$ with

$$\bar{g_1}(x) = x^2 + x^4 + x^5 + x^6,\ \bar{\ell}(x) = x^3 + x^4 + x^6 = \bar{g_2}(x)$$

and has the generator matrix of the form

$$H = \begin{bmatrix} 0&0&1&0&1&1&1&0&0&0&0&0&0&0\\ 1&0&0&1&0&1&1&0&0&0&0&0&0&0\\ 1&1&0&0&1&0&1&0&0&0&0&0&0&0\\ 0&0&0&1&1&0&1&0&0&0&1&1&0&1\\ 1&0&0&0&1&1&0&1&0&0&0&1&1&0\\ 0&1&0&0&0&1&1&0&1&0&0&0&1&1\\ 1&0&1&0&0&0&1&1&0&1&0&0&0&1 \end{bmatrix}.$$

Since $GH^T = 0$ and the dimensions of C and $C^\perp$ are the same, C is a self-dual R-double cyclic code with the parameters $[28, 14, 4]$ of $\Phi(C)$.

In Table 1, we present several examples of optimal binary linear codes, which are actually the Gray images of R-double cyclic codes. We use the table of codes in reference [11] that contains a database of optimal linear codes with respect to the Hamming distance according to their lengths and dimensions. We obtain these optimal codes by direct construction with no puncturing or shortening.

Table 1. Table of optimal parameter binary linear codes derived from R-double cyclic codes.

Generators	$[r, s]$-type	Parameter
$g_1(x) = 1 + x,\ a_1(x) = x^3 - 1$ $g_2(x) = 1 = \ell(x),\ a_2(x) = x^3 - 1$	$[3, 3]$	$[12, 10, 2]$
$g_1(x) = x^3 - 1 = a_1(x)$ $g_2(x) = x^7 - 1,\ a_2(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$ $\ell(x) = u\left(x^2 + x + 1\right)$	$[3, 7]$	$[20, 1, 20]$
$g_1(x) = 1 + x + x^2,\ a_1(x) = x^3 - 1$ $g_2(x) = 1,\ a_2(x) = x^9 - 1$ $\ell(x) = 1 + x$	$[3, 9]$	$[24, 20, 2]$
$g_1(x) = 1 + x + x^2,\ a_1(x) = x^3 - 1$ $g_2(x) = 1,\ a_2(x) = x^{15} - 1$ $\ell(x) = 1 + x$	$[3, 15]$	$[36, 32, 2]$
$g_1(x) = x^7 - 1 = a_1(x)$ $g_2(x) = x^7 - 1,\ a_2(x) = 1 + x^2 + x^3 + x^4$ $\ell(x) = u(1 + x^2 + x^3 + x^4)$	$[7, 7]$	$[28, 3, 16]$
$g_1(x) = x^9 - 1 = a_1(x)$ $g_2(x) = x^9 - 1,\ a_2(x) = 1 + x + x^3 + x^4 + x^6 + x^7$ $\ell(x) = u(1 + x^2 + x^3 + x^5 + x^6 + x^8)$	$[9, 9]$	$[36, 2, 24]$
$g_1(x) = x^{11} - 1 = a_1(x)$ $g_2(x) = x^7 - 1,\ a_2(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$ $\ell(x) = u\left(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\right)$	$[11, 7]$	$[36, 1, 36]$
$g_1(x) = x^{11} - 1 = a_1(x) = g_2(x)$ $a_2(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ $\ell(x) = u\left(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\right)$	$[11, 11]$	$[44, 1, 44]$
$g_1(x) = x^{15} - 1 = a_1(x)$ $g_2(x) = x^{15} - 1,\ a_2(x) = x^{11} + x^{10} + x^9 + x^8 + x^6 + x^4 + x^3 + 1$ $\ell(x) = u\left(x^{11} + x^{10} + x^9 + x^8 + x^6 + x^4 + x^3 + 1\right)$	$[15, 15]$	$[60, 4, 32]$
$g_1(x) = x^{15} - 1 = a_1(x)$ $g_2(x) = x^{15} - 1,\ a_2(x) = x^{13} + x^{12} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^3 + x + 1$ $\ell(x) = u\left(x^{13} + x^{12} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^3 + x + 1\right)$	$[15, 15]$	$[60, 2, 40]$

4. Gray images of R-double cyclic codes

We have defined the below Gray map in the first part of the paper. Now, we will talk about the Gray images of R-double cyclic codes. We know that the Gray map Φ is linear and the images of R-double cyclic codes under this map are binary linear codes. For $a = (x_0 + uy_0, \ldots, x_{r-1} + uy_{r-1}) \in R^r$, $b =$

$(p_0 + uq_0, \dots, p_{s-1} + uq_{s-1}) \in R^s$, we have

$$\Phi : R^r \times R^s \to \mathbb{Z}_2^{2n}$$
$$(a, b) \to (y_0, \dots y_{r-1}, x_0 \oplus y_0, \dots, x_{r-1} \oplus y_{r-1}, q_0, \dots, q_{s-1}, p_0 \oplus q_0, \dots, p_{s-1} \oplus q_{s-1})$$

where $x_i \oplus y_i = x_i + y_i \bmod 2,\ 0 \le i \le r-1,\ p_j \oplus q_j = p_j + q_j \bmod 2,\ 0 \le j \le s-1$, and $n = r + s$.

Theorem 4.1. *Let C be a double cyclic code in $\mathcal{R}_{r,s}$.*

(1) If $r = s$, then $\Phi(C)$ is a binary QC-code of index 4.
(2) If $r \neq s$, then $\Phi(C)$ is a binary GQC-code ([13]) of index 4.

Proof. The proof of this theorem is similar to the proof of Theorem 9 in [5]. □

5. Conclusions

In this paper, we studied the algebraic structure of R-double cyclic codes and their duals where $R = \mathbb{Z}_2 + u\mathbb{Z}_2 = \{0, 1, u, 1 + u\}$ is the ring with four elements and $u^2 = 0$. We gave the generator polynomials of both the R-double cyclic code C and its dual code $C^{\perp}$. We also presented examples of optimal parameter binary linear codes that are Gray images of R-double cyclic codes. In the present paper, we have chosen the lengths r and s as odd integers, since $R[x]/(x^n - 1)$ is a principal ideal ring for an odd integer n. In our case, cyclic codes over R can be generated using only one generator. However, when n is not odd, $R[x]/(x^n - 1)$ is not a principal ideal ring, and cyclic codes over R can be generated by two generators [2]. Therefore, exploring double cyclic codes over R with even lengths for future research could be interesting.

Use of AI tools declaration

The author declares he has not used Artificial Intelligence (AI) tools in the creation of this article.

Conflict of interest

The author declares no conflict of interest.

References

1. T. Abualrub, I. Siap, N. Aydin, $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, *IEEE Trans. Inform. Theory*, **60** (2014), 1508–1514. http://dx.doi.org/10.1109/TIT.2014.2299791

2. T. Abualrub, I. Siap, Cyclic codes over the cings $\mathbb{Z}_2+u\mathbb{Z}_2$ and $\mathbb{Z}_2+u\mathbb{Z}_2+u^2\mathbb{Z}_2$, *Des. Codes Cryptogr.*, **42** (2007), 273–287. http://dx.doi.org/10.1007/s10623-006-9034-5

3. M. Al-Ashker, M. Hamoudeh, Cyclic codes over $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2 + \cdots + u^{k-1}\mathbb{Z}_2$, *Turk. J. Math.*, **35** (2011), 737–749. http://dx.doi.org/10.3906/mat-1001-71

4. I. Aydogdu, Codes over $\mathbb{Z}_p[u]/\langle u^r\rangle \times \mathbb{Z}_p[u]/\langle u^s\rangle$, *J. Algebra Comb. Discrete Appl.*, **6** (2019), 39–51. http://dx.doi.org/10.13069/jacodesmath.514339

5. I. Aydogdu, T. Abualrub, I. Siap, $\mathbb{Z}_2\mathbb{Z}_2[u]$-cyclic and constacyclic codes, *IEEE Trans. Inform. Theory*, **63** (2017), 4883–4893. http://dx.doi.org/10.1109/TIT.2016.2632163

6. A. Bonnecaze, P. Udaya, Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$, *IEEE Trans. Inform. Theory*, **45** (1999), 1250–1255. http://dx.doi.org/10.1109/18.761278

7. T. Bag, H. Islam, O. Prakash, A. K. Upadhyay, A note on constacyclic and skew constacyclic codes over the ring $\mathbb{Z}_p[u,v]/\left\langle u^2-u, v^2-v, uv-vu\right\rangle$, *J. Algebra Comb. Discrete Appl.*, **6** (2019), 163–172. http://dx.doi.org/10.13069/jacodesmath.617244

8. J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, M. Villanueva, $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality, *Des. Codes Cryptogr.*, **54** (2010), 167–179. http://dx.doi.org/10.1007/s10623-009-9316-9

9. J. Borges, C. Fernández-Córdoba, R. Ten-Valls, $\mathbb{Z}_2$-double cyclic codes, *Des. Codes Cryptogr.*, **86** (2018), 463–479. http://dx.doi.org/10.1007/s10623-017-0334-8

10. J. Gao, M. J. Shi, T. T. Wu, F. W. Fu, On double cyclic codes over $\mathbb{Z}_4$, *Finite Fields Appl.*, **39** (2016), 233–250. http://dx.doi.org/10.1016/j.ffa.2016.02.003

11. M. Grassl, *Table of Bounds on Linear Codes*, 2024. Available from: `http://www.codetables.de/`.

12. O. Prakash, S. Patel, A note on two-dimensional cyclic and constacyclic codes, *J. Algebra Comb. Discrete Appl.*, **9** (2022), 161–174.

13. I. Siap, N. Kulhan, The structure of generalized quasi-cyclic codes, *Appl. Math. E-Notes*, **5** (2005), 24–30.